To Pay or Not To Pay:
Resolving Frauds in Auction with Mobile Payment

Kuen-Liang Sue and Ya-Chun Hsiao
Department of Information Management, National Central University
Jhongli City, Taoyuan County, Taiwan
Tel.+886-3-4267270
klsue@mgt.ncu.edu.tw, u1403065@cc.ncu.edu.tw

ABSTRACT

With the growing popularity of the Internet, online auctions have been the efficient way of transaction. Online auctions break region restriction and reducing transaction cost. However, there are more risks in online auction, because it lacks contact face to face. Online auction frauds occur more and more, which cause buyers suffer many losses. Therefore, it's urgent to construct a safer and more convenient payment scheme for avoiding frauds.

This paper designs a mobile payment scheme in which the buyers purchase goods on the online auction website. Our mechanism can prevent frauds by taking advantages of multiple authentications by mediators. We will explain our payment processes in detail, discussing the security and why our model avoids frauds. Our mobile payment system can not only satisfy security criteria but also provide transaction privacy to buyers.

1: Introduction

Online auctions offer an electronic implementation of the bidding mechanism from traditional auctions. With the features of the Internet, online auctions have been the efficient way of transaction. Online auctions eliminate the limitation of geographic scope, reducing the time spending in transaction, lowering the cost during transaction and are easily accessible to buyers. With the benefits of online auctions, the users are a lot and growing stably.

Although buyers and sellers don't need to contact face to face in online auctions, risks are much more than traditional transaction. Most of the current online auctions provide their trade security by the feedback rating system, which is hard to prevent frauds.

Nowadays buyers have to make the payment before getting the goods purchased on the online auction websites. The most common online auction fraud is the failure to deliver the purchased item. Non-delivery is that the seller placing an item up for bid, but the seller never ship the goods after the buyer makes the purchases and actually transfer the payment to him. The other kind of frauds is misrepresentation, which means that the goods sent by the seller are different from that described on the website. Another kind is that after the buyer bids the items, a cheater who is not the seller pretend to be the real seller defrauds the buyer to transfer the payment to the cheater. The fraudulent methods may be sending email as a payment reminder and claiming himself as the seller. Yahoo! and eBay in Taiwan haven't provided an effective solution for those kinds of frauds yet. Those two website ask users be careful themselves and give compensation if frauds really happen.

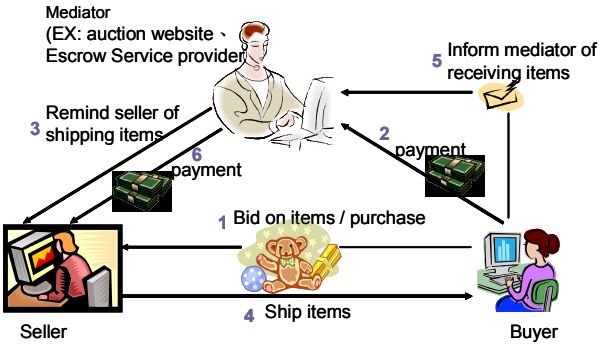

Fig.1. First method of avoiding frauds

It is unfair to buyers who lost a lot in frauds. In this paper, we propose a mobile payment model which uses cell phone as the main payment media when buyers make transactions in online auctions. The buyer could prevent the risk of not receiving the goods or be fooled by cheaters, because buyers don't need to transfer the payment to sellers before receiving the goods.

The paper is organized as follows. In Section 2, we introduce some of the existing resolution to prevent auction frauds. In Section 3, we will go into detail about our payment mechanism for avoiding frauds. In Section 4, we will discuss why our model avoids frauds and the security of our model. Conclusions are finally presented in Section 5.

2: Related Works

First of all, two existing resolutions are discussed to prevent buyer from not receiving the goods.

The first method is to add a mediator as a trusted third party beyond buyer and seller. The process is shown as Fig. 1. The mediator can be exactly the

auction website or Escrow Service provider. The buyer can transfer the payment to the mediator after making purchases on the auction website. The mediator notifies the seller to ship the items when the mediator receives the payment. The buyer notifies the mediator when the merchandise is receiving and is satisfactory. The mediator will then release the payment to the seller. eBay in America and one auction website in China are using this method and eBay cooperates with Escrow Service provider[1].

This method is useful for large sales, but is not convenient for low value transactions. In addition, it will take a longer time to finish a transaction [2].

The second method is like Sotheby's auction. There is also a mediator, who is assumed to be trustworthy. The mediator is commissioned by the seller to auction the items. First, the seller ships the items to the mediator. If a buyer wants to make purchases, he/she has to transfer the payment to the mediator. The mediator will ship the items to the buyer and transfer the payment to the seller then. The mediator would charge commissions.

Those two resolutions seem to solve the online auction frauds, but users might still suffer loss if they link to a fake website taking the wrong information about making payment such as the account to accept payment. Phishing and Pharming are techniques which make the users enter forged webpages. Phishing is a kind of frauds, which combines the internet technology and soft engineering to tempt users to enter the fraudulent website. For examples, sending mails tempting users to click the fake links [3] [4]. Pharming is harder to be identified, because it directly attack DNS server by some network technologies. Even though users key in correct URL, they will still enter the fake website, which provide the false account for making a payment. The methods of frauds could be much more than what mentioned above, so a securer mechanism is necessary to ensure the security of online auction.

3: Solution with Mobile Payment

We propose a mobile payment mechanism to solve the frauds more effectively. There are two trustworthy mediators beside sellers and buyers in our mechanism. The operator and the banks are the mediators, who take charge of the verification of seller and buyer and the transaction. The operator verifies the buyer through the cell phone number and the password of transaction. The bank also verifies the buyer through his/her financial account. Additionally, the bank manages the account of the buyer, so the greatest benefit of our model is that the buyer could transfer the payment by his/her bank after receiving the goods. This benefit makes our mechanism different form current payment ways of online auctions. Security of our payment mechanism is enhanced by asymmetric encryption and one-way hash function. The participators are hard to be faked.

Beside security, our model also provides transaction privacy to buyers. The mediator, the operator and the bank, only know the total amount in the transaction instead of the actual items.

There are two assumptions in the mechanism:

- The operator and banks are trustworthy and will not disclose the sensitive information of the users.
- The buyer has surely become the winning bidder of certain items.

The detail of our payment mechanism is illustrated in next paragraph, and the abbreviations of the relevant data used in the payment system are shown in Table 1.

Table 1. Abbreviations of the data used in the proposed mobile payment system

Abbreviation	Description
PhoneNo	The buyer's phone number.
BK_R	The bank's private key.
BK_U	The bank's public key.
OK_R	The operator's private key.
OK_U	The operator's public key.
$Passwd_{Trans}$	The transaction password known only by the buyer and the operator.
$Passwd_{Acct}$	The account password which is only known by the buyer and the bank.
RandNo	A random number.
TransNo	The transaction number only created legally by the buyer.
Price	The total amount of money of the goods.
SerialNo	A serial number created by the seller.
Date-Time	The date and time of the transaction.
TransData	The transaction data summarized by the seller.
Digest	The message digest created by one way hash function. The inputs of the hash function are *TransData* and $Passwd_{Acct}$.
TransList	The detailed data of the transaction.
TransRe	The transaction receipt.
$Account_B$	The financial account of the buyer.
$Account_S$	The financial account of the seller.
$Certificate_S$	The certificate of the seller.
ID_O	The identity of the operator.
Record	The record of transferring accounts.
PaymentRe	The payment receipt.
SendNoti	The message sent by the bank to notify seller to ship goods.
RecQuery	The message sent by the bank to confirm whether the buyer has received the goods.

3.1: Overview of the Payment Process

The participators in our payment mechanism include: buyers, sellers, the operator, and banks.

1) **Buyer:** To make a transaction with the seller, the buyer needs to apply to the operator for the mobile payment service.
2) **Seller:** The seller provides auction goods to buyers.

3) **Operator:** The operator has to confirm the transaction with the buyer. The operator has to check whether the buyer is a legal subscriber of the mobile payment service.
4) **Bank:** The bank is responsible for the verification of buyers and sellers and settlement of accounts.

There are three phases in our payment scheme: initiation phase, transaction phase, and settlement phase.

initiation phase

This phase includes the required preparations of each participant before the payment mechanism performs.

transaction phase and settlement phase

As an illustration, the steps in transaction phase and settlement phase is shown in Fig. 2.

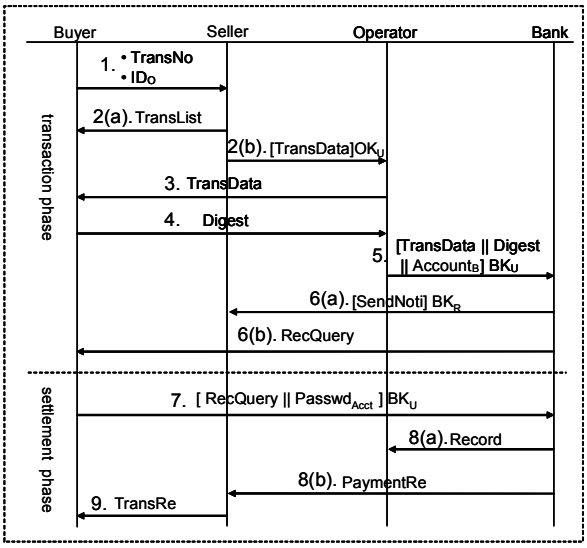

Fig.2. Data flow of transaction procedure

3.2: Interactions between the Participators

We now describe the interactions between the participants for each phase.

1) Initiation phase.

- **Buyer:** First, the buyer should have the mobile device, such as cell phone or PDA which the telecommunication module is embedded in. The mobile device must have the capability of data storage and cryptographic computing. The buyer applies for the mobile payment service and transfers his financial account ($Account_B$) to the operator. Then, the operator issues a personal transaction password and the public key of the operator (OK_U) to the buyer and stores the key in the SIM card of the cell phone.

  To reduce the waiting time of transaction, the buyer could generate the transaction number in advance before the transaction. The transaction number is created by using the operator's public key to encrypt the consumer's phone number, transaction password, and a random number.

- **Seller:** Seller can communicate with the operator or the bank through the Internet. For the security concern, the seller need to apply for a digital certificate to prove his identity to the bank and download the certificate of the operator and the bank issued from the trusted certificate authority (CA). The certificate of the operator/bank includes the public key of the operator/bank, which is needed in our mechanism.
- **Operator:** As for the operator, they have to maintain additional data in the database, such as the transaction passwords, the corresponding phone number and the identities of the bank of the buyers who has applied for the mobile payment service. The operator also applies for its digital certificate and downloads all cooperative banks' certificates from CA. The operator has asymmetric keys for data encryption, includes the public keys of all cooperative bank.
- **Bank:** The bank also has to store additional data in the database, such as the account password ($Passwd_{Acct}$) of the consumer which is different from the password of the cash card. Besides, the bank needs to maintain the transaction record for future inquiries. The same with the operator, the bank need to apply for its certificate, too.

2) Transaction phase.

In step 1), the buyer transfers the transaction number (TransNo) and the identity of the operator (ID_O) to the seller. The transaction number is a ciphertext encrypted by using the public key of the operator. As mentioned in initiation phase, the transaction number is generated by using the operator's public key to encrypt the consumer's phone number (PhoneNo), transaction password ($Passwd_{Trans}$), and a random number (RandNo). The random number is generated by the cell phone and used to make the transaction number dynamic. The operator could verify the buyer by the data in the transaction number. The transaction number could only be decrypted by the operator's private key.

In step 2a), the seller summarizes the required information into the transaction data list (TransList), and sends it to the buyer as a verification of this transaction. All details about this transaction such as the transaction number, the transaction date, the serial number, the item name, unit price and total amount of money are included in this transaction data list. The buyer could view the list on the browser.

In step 2b), the seller summarizes the required information into the transaction data (TransData), and encrypts the transaction data by using the operator's public key. The seller transmits the transaction data to the operator according to the ID_O of the buyer for the further confirmation. The transaction data includes the transaction number, the transaction date, the serial number, seller's financial account, seller's digital certificate and total amount of money. The transaction data would not contain the details of the goods to ensure the transaction privacy of the consumer. Only the seller

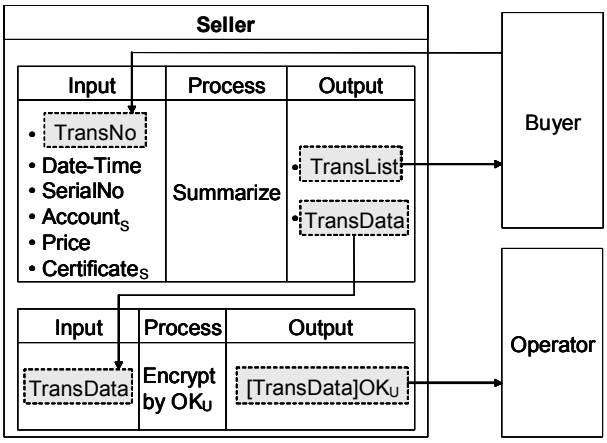

Fig.3.Step 2 in transaction phase

knows the goods the buyer bids. The transaction data in step 2a and step 2b are shown in Fig. 3.

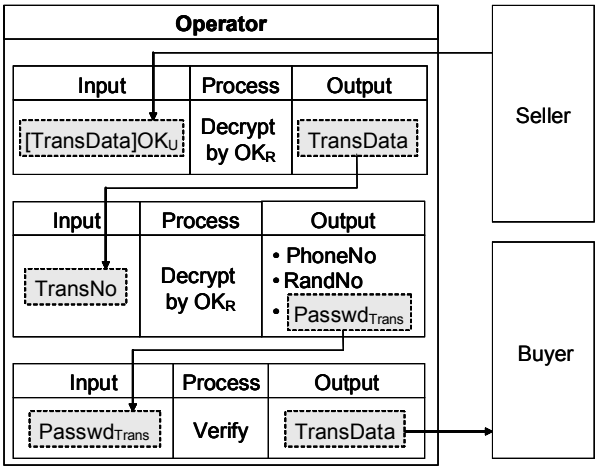

Fig.4. Step 3 in transaction phase

In step 3), the operator takes charge of the verification of the buyer and the transaction. After the operator receives the transaction data (TransData) from the seller, it decrypts the transaction data with its private key (OK_R) to get the transaction number. The operator further decrypts the transaction number and verifies the buyer's transaction password ($Passd_{Trans}$). If no error occurs in the verification, the operator will transfer the transaction data to the buyer through USSD connection for further check and waits for the consumer's response as depicted in Fig. 4. Making the buyer check the transaction data prevents the seller from interpolating the transaction content and fabricating the transaction transferred to the operator.

In step 4), the buyer has to confirm the transaction data delivered by the operator. If the transaction information is correct, the consumer has to input the account password ($Passwd_{Acct}$) as a confirmation of his identification. The cell phone will hash the transaction data and the account password by a hash function. After the hash function being performed, it will create a message digest (Digest). Finally, the consumer

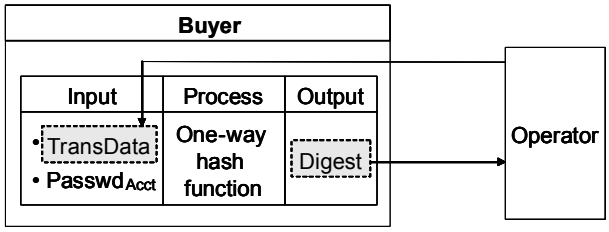

Fig.5. Step 4 in transaction phase

transmits the message digest back to the operator to finish the transaction confirmation as depicted in Fig. 5. The operator will transmit the message digest to the bank for further verify. Using one-way hash function to produce the message instead of encryption with the public key of the bank is because of the speed of one-way hash function is faster than that of the encryption.

But if the buyer rejects the payment or enters the wrong $Passwd_{Acct}$ three times, the operator will transfer a message to inform the seller about the breach of the transaction.

In step 5), the operator has to forward relative data to the bank for further check. The operator will receive the message digest from the buyer if the transaction exists and the transaction data is confirmed by the buyer. The operator encrypts the transaction data, the message digest, and the buyer's bank account ($Account_B$) with the bank's public key (BK_U) and transfers these data to the cooperative bank for verifying the buyer and recording the transaction.

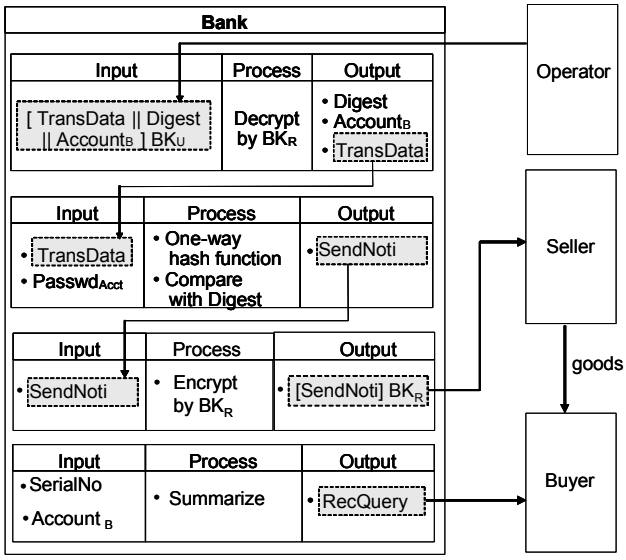

Fig.6. Step 6 in transaction phase

In step 6a), as shown in Fig. 6, when the bank receives the encrypted data from the operator, it uses its private key (BK_R) to decrypt the ciphertext getting the buyer's digest, the buyer's financial account and transaction data. The bank authenticates the seller by verifying its certificate contained in the transaction data. The bank can find the account password of the buyer by

the corresponding financial account. Then the bank calculates the hash function over the concatenation of the transaction data and the account password of the buyer. If the comparison between the output of the hash function and the message digest from the operator is the same, which means the buyer doesn't interpolate the TransData, the bank will further check the buyer's credit line and transmit a message, which is encrypted by its private key (BK_R) ([SendNoti]BK_R), notifying the seller to deliver the goods to the buyer. The SendNoti is truly sent by the bank if the seller can decrypt that cipher text by using the bank's public key (BK_U). The seller can send the goods according to the serial number involved in that notification.

In step 6b), the bank sends a query (RecQuery) to ask whether the buyer receive the goods. The query contains the serial number for the buyer to identify the transaction. The bank will complete account settlement after receiving the reply from the buyer. The process in step 6b is shown in Fig. 6.

3) Settlement phase.

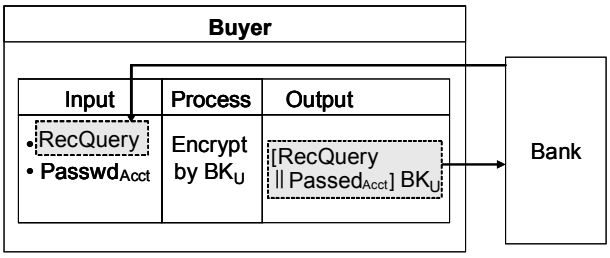

Fig.7. Step 7 in settlement phase

In step 7), after the buyer receives the query, he/she identifies the transaction according to the serial number. When receiving the goods, the buyer input the account password ($Passwd_{Acct}$). The cell phone encrypts the account password and the query with the bank's public key to create a cipher text as a reply and send it to the bank as shown in Fig. 7. The bank will start the account settlement when noticing that the buyer has received the goods.

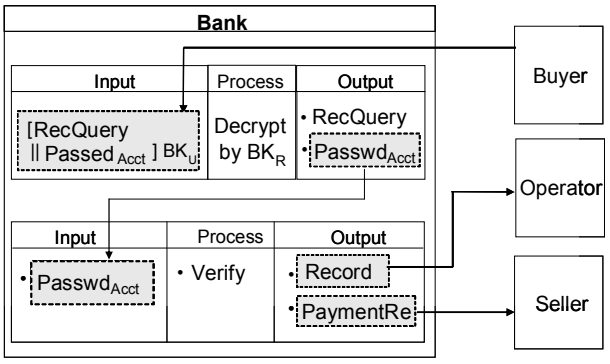

Fig.8. Step 8 in settlement phase

The bank will receive a reply from the buyer if the buyer actually receives the goods. The bank can get the buy's password of the account and the query which includes the serial number by decrypt the reply. The bank can find the account password of the buyer by the corresponding financial account recorded in the transaction records. If the password is correct, the bank will complete the account settlement. Then the bank transmits the transaction record to the operator for avoiding the possible dispute (step 8a) and also transfers the payment receipt (PaymentRe) to the seller (step 8b) as shown in Fig. 8. The seller could show the transaction receipt (TransRe) on the browser for the consumer to check and print.

Every transaction has to go through the transaction phase and settlement phase.

4: Discussion

1) Our mechanism can avoid fraud, because the bank will perform the account settlement after the goods really received by the buyer who is verified by the operator and the bank. If the seller does not ship the items in purpose, the buyer will not reply the bank for completing the account settlement. In respect of another situation, if someone pretends to be the seller sending mail includes fake remitting information, the buyer will not be fooled, for buyer need not make the payment before get the goods and the seller actually would not contact with the buyer by mail in our mechanism.

2) Our mechanism can prevent buyers duping from phishing and pharming, for buyers do not need to make the payment before getting the goods. Even the buyer enters fake website bidding something and the cheater imitate the process to transact with the buyer, the fraud will still fails since the buyer will not notify the bank to make the account settlement without receiving the items.

3) Our mechanism protects buyers' transaction privacy. The operator and the bank cannot acquire the detail of the merchandise purchased by the buyer except the total amount of the merchandise. Although only the seller knows what the buyer purchases, the seller can't ship the good which isn't meeting the item description outlined on the website, or the seller won't receive the payment. Besides, the transferred data with encryption of the asymmetric cryptography is hard to be broken [5].

4) Beside privacy, our mechanism also meets security criteria which includes confidentiality, authentication, integrity, and non-repudiation.

- Confidentiality. As for data storage, the sensitive data of transaction and the encryption keys are stored in the SIM card which is a tamper-resist device. The verification of the PIN and the $Passwd_{Acct}$ prevent the cell phone from misusing by someone else.

  As for data transmission, the data between the seller and the operator or between the operator and the bank can be transferred through the wired network such as ADSL, which use SSL

transaction protocol to ensure the security of data. In our payment scheme, the data transferred in the wired network is protected by the public-key based algorithm which can prevent the confidential attack effectively [6].

Besides, the secure connection of USSD between the operator and buyer is provided by the signal protection mechanisms of GSM/UMTS [7].

- Authentication. The buyer is authenticated three times in our payment mechanism:
  a) The cell phone verifies the PIN of the buyer.
  b) The operator verifies the $Passwd_{Trans}$.
  c) The bank verifies the $Passwd_{Acct}$ of the buyer.

  With those tree authentications, the risk of counterfeit is reduced to the minimum.

  As for the seller, the bank authenticates the seller by verifying its certificate. The certificate of the seller is issued from the trusted third party which could be the governmental institution.
- Integrity. The seller summarizes the TransList to the buyer and show TransRe to the consumer after the account settlement. The operator forwards TransData to the buyer for checking. The bank transfers a PaymentRe to the buyer after the account settlement. These data can be combined through the SerialNo of the transaction. The buyer can ensure the integrity of the transaction by comparing these data.
- Non-repudiation. After the buyer confirms the transaction, he has to enter the $Passwd_{Acct}$ for the calculation of message digest. Then, the bank authenticates the buyer by verifying the message digest. Only the legal buyer and the bank can calculate the same Digest because the $Passwd_{Acct}$ is only known by them. The transaction is confirmed if the Digest was correctly verified, and the buyer cannot deny the transaction.

5: Conclusion

Many people purchase goods by online auctions and online auction fraud is gradually prevalent nowadays. We propose a mobile payment mechanism to protect numerous customers from auction fraud.

The participators in our payment mechanism include: buyers, sellers, the operator, and banks. The operator and the banks are mediator, verifying seller, buyer and the transaction. The bank also acts like an Escrow Service provider mentioned above. Even if the buyer receives the items without replying the bank, the seller still can ask the bank to transfer the payment by some other process, for the bank manages the account of the buyer.

The process is that after the operator and the bank verify the buyer by some data transferred between the four participators, the bank will notify the buyer to ship the items. Then the bank will complete the account settlement after the buyer receives the items and send the reply to the bank.

Our payment mechanism provides many advantages:

1) **Security:** Our payment scheme meets security criteria, which includes integrity, confidentiality, authentication, and non-repudiation. Besides, the risk can be minimized when the consumer loses the cell phone or the cell phone is forged because our method provides multiple authentications. Besides, auction fraud, Phishing and pharming can be resolved, for our unique designation. Buyers can make the actual payment after receiving the goods.
2) **Transaction privacy:** The operator and the bank cannot acquire the detail of the merchandise purchased by the consumer except the total amount of price.
3) **Convenience:** The time of the transaction is shortened because the buyer needs not to send remittance to the mediator compared with the method mentioned in the section 2. Beside the time-saving, the cost of the transaction can be lower.
4) **Low computational load of the mobile phone:** The operation of the consumer in the transaction phase can be only a one-way hash function. The speed of one-way hash function is about 100 times faster than that of the encryption/decryption of the secret-key system and the speed of the encryption/decryption of the secret-key system is about 100 times faster than that of the signature/verification of the public key system [8].
5) **Feasibility:** The participators can adopt our payment scheme into their business model without additional cost of hardware. And it is implemented based on the existing network environment.

References

[1] eBay, http://pages.ebay.com/help/tp/payment-escrow.html

[2] Sulin Ba , Andrew B. Whinston , Han Zhang, "Building trust in online auction markets through an economic incentive mechanism", Decision Support Systems, v.35 n.3, p.273-286, June 2003

[3] Wenyin Liu, et al, "Phishing Web page detection", Document Analysis and Recognition, 2005. Proceedings. Eighth International Conference on, Vol. 2, p.560-564, Sept. 2005.

[4] E. Kirda, C. Kruegel, "Protecting users against phishing attacks with AntiPhish", Computer Software and Applications Conference, 2005. COMPSAC 2005. 29th Annual International, Vol. 2, p.517-524, July 2005

[5] David Pointcheval, "Asymmetric cryptography and practical security", Journal of Telecommunications and Information Technology, no. 4, p. 41–56, April 2002.

[6] William Stallings, Network Security Essentials, Prentice Hall, 2000.

[7] S. Schwiderski Grosche and H. Knospe, "Secure mobile commerce", Electronics & Communication Engineering Journal, p.228- 238, October 2002.

[8] Wei-Bin Lee, Chang-Kuo Yeh, "A New Delegation-Based Authentication Protocol for Use in Portable Communication Systems", IEEE Transactions on Wireless Communications, Vol. 4, No. 1, p. 57- 64, Jsanuary 2005