A New Fair Trade Model for Online Shopping

Kuo-Zhe Chiou[2], Chin-Ta Lin[1], Hsi-Chung Lin[2], Jheng-Hong Tu[2], and Sung-Ming Yen[2]

[1] Networks and Multimedia Institute Technology Service Center, Institute for Information Industry, Taipei 106, Taiwan, R.O.C.
cheetah@nmi.iii.org.tw
[2] Laboratory of Cryptography and Information Security (LCIS), Dept of Computer Science and Information Engineering, National Central University, Chung-Li 320, Taiwan, R.O.C.
{kzchiou, hclin, 945202043, yensm}@csie.ncu.edu.tw
http://www.csie.ncu.edu.tw/~yensm/

摘要

隨著網際網路的發達，許多網路平台業者，如 Yahoo 和 eBay 等，在網路上架設網頁平台以提供賣方提供商品資訊，方便買方透過網路瀏覽商品資訊。致使網路購物成為時下最熱門的購物方式之一。但是其所採用的交易模式卻難以達到交易公平性。

本篇提出一個新的網路購物交易方式，結合具備 RFID 讀取能力的 3G 行動手機和電子錢包，可以讓買方輕鬆地透過手機瀏覽在網路上的商品資訊，使用電子錢包來進行付款外，此交易方式亦可以確實地讓網路平台業者收取交易的服務費用，以及確保買賣雙方交易的公平性。

關鍵詞：第三代行動通訊，近距離無線通訊，行動商務，同步生效簽章，線上購物。

Abstract

Recently, online shopping has become a popular trade model. Merchants can put their goods information on a website built by the Internet platforms, such as Yahoo and eBay. This trade model facilitates customers to browse what goods the merchants sell. But the employed types of payment are not fair.

In this paper, a new trade model for online shopping is proposed. This model adopts 3G mobile phone with RFID reader and electronic wallet to facilitate customers to browse goods information and pay for the goods by using electronic wallet. Moreover, this model not only can let Internet platforms charge the successful transaction but also guarantee that the transaction is fair.

Keywords: 3G mobile communication, Near Field Communication, Mobile commerce, Concurrent Signature, Online shopping.

1. Introduction

The main problem of conventional trade is that how does a merchant let customers know what goods and at where he sells? Accordingly, the market such as convenience store and wholesale has become an important transaction mechanism where merchants can provide their goods and customers come here to look for what he wants. Nowadays, along with the tremendous development of Internet, undoubtedly online shopping is an important trend. Some Internet platforms, such as Yahoo[16] and eBay[13], provide this kind of service that merchants can put their goods information on the website of the platform so that customers can browse these goods by IE.

Moreover, due to the introduction of third generation (3G) networks and the adoption of USIM card, mobile phone facilitates users to obtain valuable information by connecting with the wireless World Wide Web (wWWW) and make fast and efficient commercial transactions. By means of 3G mobile phone, customers can go online shopping at any where and any time.

However, instead of paying face to face in conventional payment, there are two main payment types. One is cash against documents (C.A.D) and the other is cash on delivery (C.O.D.). The former is that the customer transfers money to the merchant's account in advance, then the merchant delivers the goods. But this payment type may lead to the result that customer has paid money but does not receive goods. The latter is that the customer will pay cash when the goods arrived. This payment type is unfavorable to the merchant because he does not know whether the customer has sufficient money to pay. Therefore, these two payment types are not fair.

In this paper, a new fair trade model for online shopping is proposed. This model adopts 3G mobile phone with RFID reader and electronic wallet to facilitate customers to browse goods information and pay by using electronic wallet. Moreover, we propose a new concurrent signature slightly modified from Chen et al.'s current signature [1] and employs Kim et al.'s proxy signature [2] so that Internet platforms can charge for providing online shopping service, and transaction can be guaranteed fairness.

The rest of this paper is organized as follows. In Section 2, the related works is given. The introduction to the proposed trade model including overview, security analysis and dispute settling are provided in the Section 3. Finally, the discussion and the conclusions are given in Section 4 and Section 5, respectively.

2. Related Works

Yahoo and eBay are two well-known Internet platforms which provide online shopping service. Instead of payment face to face in the real world, C.A.D, and C.O.D. are two main e-payment ways for online shopping. However, these two payment ways and goods delivery are always processed outside the platforms, so the platforms always can not solve transaction disputes effectively and effectively. In other words, they can not guarantee transaction fairness that *merchants can get money and customers can receive what they want. Otherwise, both parties get nothing*.

PayPal [14] is a famous e-payment system based on credit card system. If any parties would like take advantage of this system to do transaction, they have to register their PayPal account first. When ordering the goods, the customer will transfer his e-money from his PayPal account to the merchant's. This action is made by PayPal and let the merchant know that the customer can pay for the goods, so he delivers the goods.

On the other hand, PayPal provides a chargeback mechanism for protecting customers. If the transaction disputes happen (the goods not received or the goods significantly different), the customer can apply this mechanism that his credit card bank asks PayPal to withdraw back e-money. Beside, PayPal will notice the merchant about this dispute. The merchant has to provide related evidences to prove he is honest. The judge will be made by PayPal and both parties' credit card bank. Briefly speaking, the transaction fairness is reached because PayPal manages two parties' PayPal account. Moreover, any disputes can be solved by following the disputes settling solution of credit card system. However the solution is complicated and always takes many days.

Proxy signature, first introduced by Mambo et al.[7], allows a designated person, called a proxy signer, to sign on behalf of an original signer. There are three types of delegation including full delegation, partial delegation, and delegation by warrant. However, in consideration of security, it is bad to adopt full delegation type because proxy signer will know the private key of original signer. Although the proxy signature using partial delegation has lower computational cost than the proxy signature using delegation with warrant, the latter can restrict documents to be signed (e.g. warrant states the valid period) but the former does not have such property. This paper employed Kim et al.'s proxy signature [2] which provides a new type of delegation called partial delegation with warrant. This new types have both of the advantages of partial delegation and delegation with warrant.

Due to the work of Chen et al.[1], concurrent signature becomes an important research topic about how to fairly exchange two signatures between two parties without the assistance of a trusted third party and without the assumption of the same computing power between two parties. Therefore, the concurrent signature is applicable for the proposed model because the mobile phone is used by the customer. In concurrent signatures, two parties, namely initial signer and matching signer, are involved in the protocol. The initial signer who launches the concurrent signature protocol first will randomly selects a secret number, namely keystone, and then both parties exchanged their signatures with the same keystone. The concurrent signature is based on ring signature [9] that provides the property of signer-ambiguous. Therefore, from any third party's point of view, the two signatures exchanged between two parties are ambiguous with respect to the identity of two parties. However, after the keystone is released by the initial signer, the signatures will be simultaneously bound to their real signer and become valid signatures concurrently. From then on, some concurrent signatures have been proposed [5][8][11]. Although the fairness of concurrent signature is weaker than that of fair exchange system [3][4], it is satisfying with the requirement in the proposed trade model.

RFID (Radio-Frequency IDentification) [6][15] is a technology for identifying the identification of objects. Usually, RFID is viewed as a means of explicitly labeling objects to facilitate their perception by computing devices. An RFID device, called an RFID tags, is a small and wireless devices. It is generally attached to an antenna in a package that resembles an ordinary adhesive sticker. Therefore, people can use RFID reader to easily identify the identification of object by reading the attached RFID tags.

3. The Proposed Trade Model

3.1 Overview of the proposed trade model

In this paper, we proposed a new trade model (see Figure 1).

There are three parties including the Internet platform (P), the merchant (M), and the customer (C). The following provides the security issues and assumptions.

- Internet platform:

The platform provides a website space for merchants so that merchants can put their goods information on the Internet and customers browse these goods information and pay to the merchant by the assistance of the platform. Therefore, we have to

believe that the platform does not modify the goods information provided by merchants and honestly keeps and transfers e-money. Moreover, the platform will charge when the merchant and the customer carry a transaction out successfully.

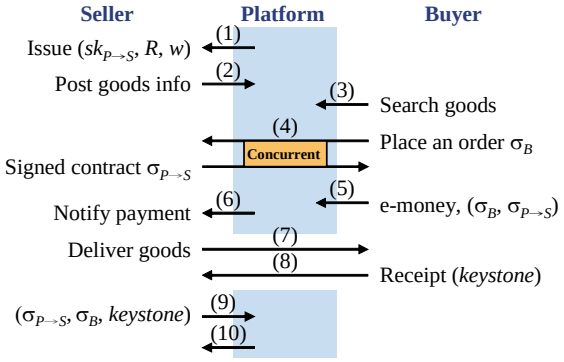

Figure 1: The trade model

■ The merchant:

All the goods information on the platform is provided by the merchant. When receiving the order from the platform, the merchant sends the goods by the deliveryman who is the employee of the trusted delivery party such as DHL [12]. Moreover, the merchant will prepare a RFID tag in which has related transaction data including the goods information, the date, the price, the digital signature, and any information related the transaction. Then this tag is attached to the goods. By means of the RFID tag, the deliveryman and the customer can read the transaction information by using their mobile device embedded RFID reader. Take advantage of RFID tag in case the deliveryman takes a lot of transaction data. The deliveryman will bring back the keystone such that the merchant can use it to redeem from the platform.

■ The customer

In the model, the customer must have a device which can connect to Internet and has high transmission speed. Moreover, a temper-proof device, such as SIM card, is required to manage electronic wallet securely. Therefore, 3G mobile phone is suitable for the proposed model. By means of 3G mobile phone, the customer can browse website easily and the embedded USIM card can manage electronic wallet and customer's public key pair securely. Moreover, the mobile phone must have RFID reader for reading any transaction data which is attached to the goods.

The transaction flow can be roughly separated into four phases including delegation phase, payment phase, goods delivery phase, and redeeming phase. The detailed introduction is provided as follows:

■ Delegation phase:

Delegation phase contains (1) and (2) steps. Before (1), the merchant has to tell the platform what goods he wants to sell, then a proxy signature protocol will be launched for getting a triple ($sk_{P->M}$, R, w) via secure channel in (1), where $sk_{P->M}$ is the proxy key, R is the proxy public key and w is a warrant. Finally, the merchant can put the goods information on the website in (2).

■ Payment phase:

The step (3), (4), (5), and (6) involve in this phase. Simply speaking, the customer uses his mobile phone to browse the goods information in the website. If the customer wants to purchase, the mobile phone will ask him to input PIN Code for checking his identity. Then, the customer selects a random number as keystone and launches modified concurrent signature protocol to fairly exchange the signatures σ_C and $\sigma_{P->M}$, with the merchant. Finally the customer sends e-money and the two signatures to the platform and then the platform sends a notice to ask the merchant to deliver the goods.

■ Goods delivery phase:

The main purpose of in this phase is to deliver the goods to the customer. When receiving a notice from the platform, the merchant delivers the goods to the customer by the deliveryman who has mobile device such as PDA embedded with RFID reader in (7). After checking the goods is fine, the customer gives the keystone to the deliveryman. Then the deliveryman uses the keystone to check the validity of concurrent signature. If it is valid then stores the keystone in the PDA and gives it to the merchant. Otherwise, reject to give goods to the customer. This procedure is done in step (8).

■ Redeeming phase:

Eventually, there are two steps, (9) and (10) in the redeeming phase. In these two steps, the merchant sends the keystone to the platform for redeeming e-money. When receiving the redeeming request, the platform will verify the concurrent signature σ_C and $\sigma_{P->M}$ with the keystone. If the verification is acceptance, the platform deducts the charge from e-money and sends remaining e-money to the merchant.

3.2 The concrete protocol

The system setting is given in the following. Two big primes, p and q, such that $q|(p-1)$, and g is a generator of the subgroup of order q in Z_p^*. The message space M is the same as the keystone space K $=\{0,1\}^*$, and the signature space S is the same as the keystone fix space $F = Z_q^*$. Three different public hash functions $H_1(): K \rightarrow F$, and $H()$, $H_2(): \{0,1\} \rightarrow Z_q^*$ are selected. The private key of each party is labeled as sk_i which is selected randomly. The corresponding public key is $pk_i = g^{sk_i} \bmod p$. The public system parameters are (p, q, g, $H()$, $H_1()$, $H_2()$).

In the delegation phase, the merchant has to communicate with the platform to register some information including what the goods will sell, the identity of merchant, and related information. Then the platform give a proxy key pair to the merchant by doing the following calculation:

$$R = g^r \bmod p$$
$$e = H(w||R)$$
$$s = (r + e \times sk_P) \bmod q$$

where r is randomly selected in Z_q^*. The proxy key $sk_{P->M}$ is s and the corresponding proxy public key can be obtained by computing $pk_{P->M} = R \times pk_P^{H(w||R)}$. The content of the warrant w could contain goods information, the identity of the merchant and platform, and the expired date. Then the platform sends the triple ($sk_{P->M}$, R, w) to the merchant. Then the merchant puts goods information on the website.

In the payment phase, the customer uses mobile phone to search what goods he wants first. Once he decides to buy an item, he launches the following modified concurrent signature protocol:

Customer → Merchant:

1. Selects a random number as *keystone* and calculates keystone fix $f = H_1(keystone)$.
2. Obtains the proxy public key of the merchant by computing $pk_{P->M} = R \times pk_p^{H(w||R)}$.
3. Calculates a signature σ_C on the message m_C by the following computation:
$$h = H_2((g^{r_C} pk_{P->M}^{\ f} \bmod p) \| m_C)$$
$$h_C = (h - f) \bmod q$$
$$s_C = (r_C - h_C sk_C) \bmod q$$
return $\sigma_C = (s_C, h_C, f)$
4. Sends σ_C and m_C to the merchant.

Merchant→Customer

1. When receiving σ_C and m_C, the merchant checks if the σ_C is valid by the following equation:
$$h_C + f = H_2((g^{s_C} pk_C^{\ h_C} pk_{P->M}^{\ f} \bmod p) \| m_C)$$
2. Generates the signature σ_M on message m_M by doing the following calculation:
$$h' = H_2((g^{r_M} pk_C^{\ f} \bmod p) \| m_M)$$
$$h_M = (h' - f) \bmod q$$
$$s_M = (r_M - h_M sk_{p->M}) \bmod q$$
return $\sigma_M = (s_M, h_M, f)$
3. Sends σ_M and m_M to the customer.

To the end, the customer has to check if the σ_M is valid by the following equation:

$$h_M + f = H_2((g^{s_M} pk_{P->M}^{\ h_M} pk_C^{\ f} \bmod p) \| m_M)$$

If the checking is valid, then the customer sends a triple (*payment*, σ_C, σ_M) to the platform, where the *payment* is a signature generated by USIM card. The *payment* indicates that the customer will pay the price of goods to the merchant. Therefore, the amount in the USIM card will be deducted. After receiving the triple (*payment*, σ_C, σ_M), the platform will keep the triple for a few days, usually one weak, and asks the merchant to send goods. If the merchant does not launch redeeming phase after one week, the customer will get *payment* back from the platform.

In the goods delivery phase, the merchant sends the goods by commissioning a deliveryman. When the goods arrived and the customer checks the goods is correct, then transmits the *keystone* from his mobile phone to the mobile device of deliveryman. The deliveryman has to check whether the keystone can validate the signature σ_C and σ_M by doing the following procedures:

1. Derives keystone fix f from *keystone*: $f = H_1(keystone)$.
2. Verify the validity of σ_C by the following verification. If it is valid, returns ACCEPT, otherwise, returns REJECT.
$$h_C + f = H_2((g^{s_C} pk_C^{\ h_C} pk_{P->M}^{\ f} \bmod p) \| m_C)$$
3. Verify the validity of σ_M by the following verification. If it is valid, returns ACCEPT, otherwise, returns REJECT.
$$h_M + f = H_2((g^{s_M} pk_{P->M}^{\ h_M} pk_C^{\ f} \bmod p) \| m_M)$$

Both of the results of the above procedure 2 and 3 are ACCEPT, the deliveryman give the goods to the customer, otherwise, deliveryman will reject this transaction. Finally, the deliveryman brings the keystone to the merchant.

In the redeeming phase, the merchant will redeem e-money from the platform by sending the *keystone*. Once receiving the redeem request from the merchant, the platform will verify if *keystone* can validate the signatures, σ_C and σ_M. The procedure of verification is the same as what deliveryman does. If the verification results are ACCEPT, then the platform deducts the charge from e-money and sends remaining e-money to the merchant.

3.3 Security analysis

It is implicit that the security issues of the proposed trade model satisfy transaction fairness, and the signature unforgeable and signer-ambiguous.

- Signature unforgeable: Similar to [1], the modified concurrent signature presented in this paper is also derived from Schnorr signature [10] which is based on discrete logarithms problem (DLP). In other words, it is computational infeasible to derive private key sk_i from the corresponding public key pk_i by computing $sk_i = \log_g(pk_i)$ even the keystone is released.
- Signer-ambiguous: Before the keystone is released, both signatures are ambiguous. The modified concurrent signature is also based on ring signature [9] that the signer-ambiguous is provided. In other words, in the modified concurrent signature, the two exchanged signatures are signer-ambiguous from any third party's point of view. However, once the keystone is released, the two exchanged signatures become valid and any one can identify who has actually signed the message.

– Transaction fairness: Because of the properties of signer-unforgeable and signer-ambiguous, for all signatures that are generated with the same keystone will not be forged and be binding concurrently when the keystone is released. Therefore, in the proposed trade model, before the keystone is given to the merchant, it is impossible for the merchant to get e-money. Moreover, since the customer has to send the payment to the platform in advance, so, if obtaining the keystone, the merchant can gain the e-money.

4. Discussion

Similar to PayPal, the platform in the proposed trade model is a trusted party and manages the payment flow between the customer and the merchant. However, the transaction dispute settling in the proposed model is easier than that in the PayPal. To simply speaking, the basis for settling the disputes is keystone. Because the platform has the payment sent from the customer, once the merchant provides the keystone, then the merchant can gain the e-money. On the other hand, if the customer does not receive the goods, he can ask platform to cancel the transaction and the payment will transfer the customer's bank. But this requirement will not be done until after one week. Therefore, the platform can easily solve the transaction dispute depending on the condition that if the merchant can provide the keystone.

In the proposed trade model, the "proxy-protected" proxy signature [2] could be employed, and the platform could be "semi-trusted" in the sense that he does not escrow the proxy key and he can not obtain the keystone before the merchant does.

5. Conclusions

Online shopping has become a trend for transaction in digital form. Moreover, because of the capability of 3G mobile device, the customer can use it to browse website and make a payment easily.

In this paper, a new fair trade model for online shopping is proposed by means of it. Employing Kim et al.'s proxy signature and the modified concurrent signature, the proposed model satisfies transaction fairness, signature unforgeable, and signer-ambiguous. Moreover, from the customer's point of view, the steps for transaction are simple and easy that only orders the goods and receives it. The computation of the protocol can be done by the mobile device automatically.

Acknowledgment

This work was supported by the Institute for Information Industry, R.O.C.

References

[1] L. Chen, C. Kudla, and K.G. Paterson, "Concurrent Signatures," in *Advances in Cryptology — EUROCRYPT* 2004, LNCS, Vol. 3027, pp. 287-305, Springer-Verlag, 2004.

[2] S. Kim, S. Park, and D. Won, "Proxy Signatures, Revisited," *Proc. of Information and Communications Security — ICICS*'97, LNCS, Vol. 1334, pp. 223-232, Springer-Verlag, 1997.

[3] N. Asokan, V. Shoup, M. Waidner, "Optimistic Fair Exchange of Digital Signatures," in *Advances in Cryptology — EUROCRYPT* '98, LNCS Vol. 1403, pp. 591-606, Springer-Verlag, 1998.

[4] E.F. Brickell, D. Chaum, I.B. Damgård, and J. van de Graaf, "Gradual and Verifiable Release of a Secret," in *Advances in Cryptology — CRYPTO* '87, pp. 156-166.

[5] Y.C. Chen and S.M. Yen, "Balanced Concurrent Signature," Technical report of LCIS, Department of computer science and information engineering, National Central University, Taiwan.

[6] Ari Juels, "RFID Security and Privacy: A Research Survey," RSA Laboratory, available at http://www.rsa.com/rsalabs/node.asp?id=2937

[7] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures for Delegating Signing Operation," *Proc. of the 3rd ACM Conference on Computer and Communications Security* (*ACM CCS'96*), ACM Press, pp. 48-57, 1996.

[8] K. Nguyen, "Asymmetric Concurrent Signatures," *Proc. of Information and Communications Security — ICICS* 2005, LNCS Vol. 3783, pp. 181-193, Springer-Verlag, 2005.

[9] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a Secret", in *Advances in Cryptology — ASIACRYPT* 2001, LNCS Vol. 2248, pp. 552-565, Springer-Verlag, 2001.

[10] C.P. Schnorr, "Efficient Identification and Signature for Smart Card," in *Advances in Cryptology — CRYPTO* '89, LNCS Vol. 435, pp. 239-252, Springer-Verlag, 1990.

[11] W. Susilo, Y. Mu, and F. Zhang, "Perfect Concurrent Signature Schemes," *Proc. of Information and Communications Security — ICICS* 2004, LNCS Vol. 3269, pp. 14-26, Springer-Verlag, 2004.

[12] DHL, available at : http://www.dhl-usa.com/home/home.asp

[13] eBay, available at: http://www.ebay.com/.

[14] PayPal, available at: http://www.paypal.com

[15] RFID Journal, available at: http://www.rfidjournal.com

[16] Yahoo, available at: http://www.yahoo.com