Fair Trading Protocol With Off-line Anonymous Credit Card Payment

Weiliang Zhao[1], Vijay Varadharajan[1,2], and George Bryan[1]

[1] Center for Advanced Systems Engineering
University of Western Sydney,
Locked Bag 1797
Penrith South DC, NSW 1797, Australia

[2] Department of Computing,
Macquarie University,
NSW 2109, Australia

Abstract. A fair trading protocol with off-line anonymous credit card payment is proposed in this paper. The fair trading protocol provides an overall solution for a trading process with off-line anonymous credit card payment. The fairness is achieved for both the involved client and merchant. The client information about credit card is anonymous in the protocol. The proposed protocol is based on the general optimistic protocols for fair exchange with an off-line Trusted Third Party (TTP). The financial institution for credit card service can be off-line in the fair trading protocol. The TTP and the financial institution for the credit card service are not involved in normal transactions and the running cost will be reduced.

1 Introduction

With the exploding growth of electronic commerce on the Internet, the issue of fairness [1, 2] is becoming increasingly more important. Fair exchange protocols have already been broadly used for applications such as electronic transactions [3, 4], electronic mails [5, 6], and contract signing [7]. The fairness is one of critical issues in on-line transactions and related electronic payment systems. Many electronic payment systems have been proposed for providing different levels of security to financial transactions, such as iKP [8], SET [9], NetBill[10] and NetCheque [11]. In a normal electronic commerce transaction, there is always a payer and a payee to exchange money for goods or services with each other. At least one financial institution, normally a bank, should be present in the payment system. The financial institution will play the role of issuer for the payer and the role of acquirer for the payee. An electronic payment system must enable an honest payer to convince the payee of a legitimate payment and prevent a dishonest payer from making other unsuitable behaviors. At the same time, some additional security requirements may be addressed based on the nature of trading processes and trust assumptions of the system. Payer, payee and the financial institution have different interests and the trust between two parties should be as little as possible. In electronic commerce, the payment happens over an open network, such as the Internet, the issue

Zhao W., Varadharajan V. and Bryan G. (2004).
Fair Trading Protocol With Off-line Anonymous Credit Card Payment.
In *Proceedings of the 2nd International Workshop on Security in Information Systems*, pages 186-195
DOI: 10.5220/0002673801860195

of fairness must be carefully addressed. There is no fairness for involved parties in the existing popular payment protocols. One target of this paper is to address the fairness issue in the credit card payment process. In the existing credit card protocols, the financial institution that provides the credit card service plays a role of on-line authority and will be actively involved in a payment. To avoid the involvement of financial institution in normal transactions and reduce running costs, some credit card based schemes with off-line financial authority has been proposed [12]. Another target of this paper is to avoid the on-line financial institution for credit card service in the normal transactions.

In this paper, we propose a fair trading protocol with off-line anonymous credit card payment. The protocol addresses the fairness and privacy of the trading process and its associated payment. The credit card is anonymous and an on-line credit card service from a financial institution is not necessary during the processing of a payment. The TTP and financial institution for credit card can be both off-line, the proposed protocol has better availability and reliability and is more efficient than other solutions with more on-line components. The technique of proof of equivalence of discrete logarithm to discrete log-logarithm [13] is the essential tool in the constructing of our fair trading protocol. In section 2, the electronic payment with off-line anonymous credit card is discussed. In section 3, we propose a fair exchange protocol with off-line anonymous credit card based payment. Finally, section 4 concludes the paper with some final remarks.

2 Electronic Payment With Anonymous Off-line Credit Card

Credit card payment is currently the most popular of all on-line payment methods. There are at least three parties involved in this kind of payments: Client, Merchant and Bank. The client is the buyer or service user who will make the payment. The merchant is the goods or service provider who will receive the payment. The bank is the financial institution that provides credit card service and guarantees the transfer of money value from the client to the merchant. The bank acts as the issuer of credit cards to clients and acquirer of payment records from merchants. For one payment, the issuer and acquirer can be same or different, clearing between the issuer and the acquirer will be done using existing financial networks. There is an on-line financial authority in the existing electronic credit card protocols [8–11]. The authors in [12] have proposed a credit based payment scheme in which the financial institution is not necessary on-line. Merchant can ensure the authenticity of the credit cards without the help of an on-line authority organization. Firstly, the client applies for a digital credit card from the bank. After the credit check, if the client is approved to have it, the digital credit card is delivered to the client through a secure channel. The credit information of the client is anonymous with the technique of no-interactive equality proof [16].

The digital credit card contains at least the following information:

- client's ID
- $h_i = g_i^x \bmod q$, $i = 1, 2, \ldots, l$, where $g_i \in Z_p^*$ are the common generators, x contains the credit card number, PIN number, other confidential information and salt.
- credit amount A

– expiry date E

The digital credit card token is of the form $\mathcal{C} = \ < C, h_1, h_2, \cdots, h_l, E, A >_{skb}$. It has the signature of the bank. If a client sends his digital credit card to a merchant, the merchant can know the credit amount, the expiry date and can check the signature of the bank but can not know the credit card number and PIN number. The client must prove to the merchant that he knows the secret (credit card number, PIN number and other confidential information in the credit card) without revealing the secret to the merchant. Using the technology of equality proof of knowledge, the client chooses a random number r, $r \in Z_p^*$ to compute $a_i = g_i^r \bmod p$ for all $i = 1, 2, \ldots, l$. The pair $\{c, z\}$ is calculated as:

$$c = H(g_1||g_2||\cdots||g_l||a_1||a_2||\cdots||a_l||h_1||h_2||\cdots||h_l),$$
$$z = cx + r \bmod p.$$

The client will send $\{c, z, p, g_1, \ldots, g_l, a_1, \ldots, a_l, h_1, \ldots, h_l\}$ to the merchant and the merchant can use the following equation to check the validity of the digital credit card.

$$g_i^z \stackrel{?}{=} h_i^c a_i \bmod p.$$

In any case, the merchant has the option to get confirmation from the authority organization for higher level of assurance. The credit card is anonymous and the financial authority is normally off-line.

3 Fair Trading Protocol with Off-line Anonymous Credit Card Payment

Based on the well-known optimistic protocol for fair exchange[14, 15, 17], we will propose a generic fair trading protocol with off-line anonymous credit card payment. The proposed protocol is an overall solution with the off-line TTP and off-line financial institution for credit card service. The credit information of the client is anonymous in the protocol.

3.1 Notations

Here we give the general notations which will be used in the description of the fair trading protocol.

(1) Parties:

- C: Client
- M: Merchant
- TTP: Trusted Third Party
- B: Bank (Financial Institute for Credit Authority)

(2) Public Key Cryptosystems:

- PKX: Public key of user X.
- SKX: Private key of user X.
- $P_{enc}(PKX, m)$: Encryption of message *m* with public key PKX.
- $P_{dec}(SKX, c)$: Decryption of ciphertext *c* with private key SKX.

(3) Digital Signature Schemes:

- pkx: Verifying key of user X.
- skx: Signing key of user X.
- $< m >_{skx}$: Creation of signature of *m* under signing key skx.
- $S_{veri}(pkx, < m >_{skx}, m)$: Verification of signature $< m >_{skx}$ on message *m*, *true* for valid and *false* for invalid.

(4) Other items:

- t_x : Timestamp generated by party X.
- $H(m)$: Hash function on message *m*.

3.2 System Setup

There are four parties in our protocol, they are Client, Merchant, TTP and Bank. Client has a pair of public and private keys: PKC and SKC, and a pair of signing and verifying keys: skc and pkc. Merchant has a pair of public and private keys: PKM and SKM and a pair of signing and verifying keys: skm and pkm. TTP has a pair of public and private keys: PKT and SKT. We will employ the technique of proof of equivalence of discrete logarithm to discrete log-logarithm. The above key pairs must follow some overall rule of the whole system. This means that these key pairs must be setup based on the same set of algorithms and parameters. If necessary, the signature scheme of TTP, public key cryptosystem of bank and signature scheme of bank can be defined independently. They need not follow the same set of algorithms and parameters.

At first, we choose three primes to set up the system. The three primes are p, q and q', which are of the form $p = 2q + 1$ and $q = 2q' + 1$. We will use ElGamal cryptosystem for encryption and decryption and a DSA-like scheme for signature.

Public Key Cryptosystems q is the prime number for the ElGamal cryptosystem. Z_q^* is a intractable multiplicative group with order $q - 1$. G is a generator of Z_q^*. SKX is the private key and PKX is the public key. $PKX = G^{SKX}$ mod q and $SKX \in \{1, 2, \ldots, q - 2\}$. The ciphertext of m under PKX is:

$$cx = P_{enc}(PKX, m) = (W, V)$$

where $W = G^w \text{mod } q$ and $V = m(PKX)^w \text{mod } q$, w is randomly chosen from $\{1, 2, \ldots, q - 2\}$. The message after decryption is:

$$m = V \cdot W^{-SKX} \text{mod } q$$

Digital Signature Scheme p is the prime number for the DSA-like digital signature scheme. Z_p^* is a intractable multiplicative group with order $p-1$. g is a generator of Z_p^*. skx is the signing key and pkx is the verifying key. $pkx = g^{skx}$ mod p and $skx \in \{1, 2, \ldots, q-2\}$. The signature of m under pkx is :

$$< m >_{skx} = (r, s)$$

where $r = g^k \text{mod}\, p$ and $s = k^{-1}(h(m) + r \cdot skx)\text{mod}\, q$. k is randomly chosen from $\{1, 2, \ldots, q-2\}$ and $h(\ldots)$ is the hash function.

For verification of signature, $S_{veri}(pkx, < \text{m} >_{skx}, \text{m})$ is to check

$$r^s \overset{?}{=} g^{h(m)} \cdot (pkx)^r \text{mod}\, p$$

Construction of Important Tokens In this section, we will give details of digital tokens used in our fair exchange protocol with credit card based payment.

(1) Credit Card
The token for credit card is of the form

$$\mathcal{C} = \; < C, l, h_1, h_2, \cdots, h_l, E, A >_{skb}$$

The credit token contains the client's identity C, the confidence level l, the expiry date E, maximum credit amount A and $h_i = g_i^x$ mod p, where $g_i \in Z_p^*$ are common generators for $i = 1, 2, \cdots, l$, where x is the concatenation of PIN number, credit card number and salt. The credit token is signed by the bank using its private key skb.

(2) Payment Slip
The data in the payment slip is

$$SlipData = \mathcal{C}, M, O, \$, tc,\; H(\mathcal{C}, M, O, \$, tc),$$

where M is ID of merchant, O is the order, $ is the amount of money and currency type and t_c is the timestamp generated by the client C.

The payment slip token has the form

$$Slip = < SlipData >_{skc},$$

The payment slip is signed by the client with private key skc.

(3) Encrypted Payment Slip
The encrypted payment slip token is

$$C_S = P_{enc}(PKT, Slip).$$

The client's payment slip is encrypted under the TTP's public key PKT. If necessary, TTP can open it with its private key SKT.

(4) Certificate of Encrypted Payment Slip
$C_S Cert$ is the token to prove C_S is a ciphertext of S without disclosing the signature.

Here, we will give all the details of construction C_S and $C_S Cert$. p and q are the two prime numbers used in our system. The client has a pair of signing key and verifying key $\{skc, pkc\}$, g is a generator of Z_p^* and $pkc = g^{skc}$mod p. The TTP has public key and private key $\{PKT, SKT\}$, G is a generator of Z_q^* and $PKT = G^{SKT}$mod q.

For encryption of message m, we have the following:

$$P_{enc}(PKT, m) = (W, V) \bmod q,$$

where $W = G^w$ and $V = m(PKT)^w$, $w \in \{1, 2, \cdots, q-2\}$ is a randomly chosen number.

The signature scheme works as follows: Choose a random $k \in Z_q^*$, the signature has the form

$$Slip = < SlipData >_{skc} \ \equiv \ (r, s)$$

where $r = g^k$ mod p and $s = k^{-1}(H(m) + r \times skc)$ mod q and $pkc = g^{skc}$ mod p. $Slip$ is the payment slip.

Encrypting the above payment slip $Slip$ with PKT, we have, $P_{enc}(PKT, Slip) = (W, V)$. The encrypted payment slip with signature is then given as follows:

$$C_S = \{r, W, V\},$$

where $W = G^w$ mod q, $V = s(PKT)^w$ mod q.

With transformation $x = G$, $y = W^{-1}$ mod q, $z = PKT$, $X = r^V$ mod p, $Y = g^{H(S)}(pkc)^r$ mod p and $\alpha = -w$, choose $w_i \in \{1, 2, \cdots, q-2\}$, then

$$t(x_i) = x^{w_i} \bmod q,\ t(X_i) = X^{z^{w_i}} \bmod p$$

and

$$\begin{array}{l} c = H_l(x||y||z||X||Y||t(x_1)||t(X_1)|| \cdots ||t(x_l)||t(X_l)) \\ c = c_1 c_2 \cdots c_l \\ r_i = w_i - c_i \alpha \bmod q-1 \end{array}$$

(R, c) is the certificate $C_S Cert$ for C_S.

The process of verification is to check,

$$c = H_l((x||y||z||X||Y||u_1||U_1|| \cdots ||u_l||U_l)$$

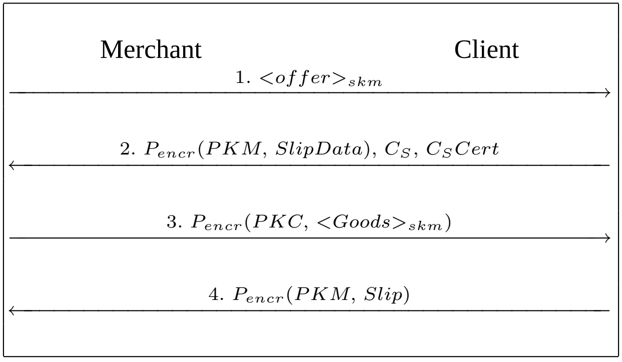
where $u_i = x^{r_i} y^{c_i}$ mod q, and

$$U_i = \begin{cases} X^{z^{r_i}} \bmod p\ if\ \ c_i = 0 \\ Y^{z^{r_i}} \bmod p\ if\ \ c_i = 1 \end{cases}$$

3.3 Fair Trading Protocol

Based on the tokens defined in the last subsection, our fair trading protocol is constructed. The fairness of the trading between a client and a merchant is guaranteed.

Fair Trading Protocol


Merchant
Client
1. $<offer>_{skm}$
2. $P_{encr}(PKM,\ SlipData),\ C_S,\ C_SCert$
3. $P_{encr}(PKC,\ <Goods>_{skm})$
4. $P_{encr}(PKM,\ Slip)$

For the above protocol, if both the client and the merchant perform properly, the TTP will not be involved. The details of the protocol are as follows:

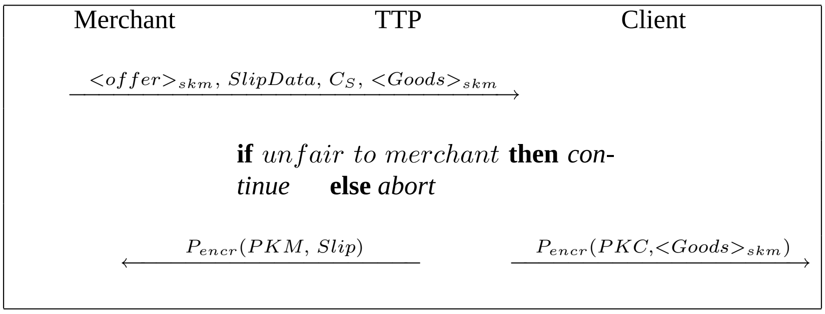
1. In step one, the merchant sends his signed $offer$ to the client. The $offer$ should contain the description of the $Goods$ and related trading information, such as price, valid date etc. The client checks the $offer$, and if client is not satisfied with the $offer$, he can quit the protocol, and therefore it is fair for both parties.
2. In step two, the client sends the merchant his credit card C, order information O, amount of money and currency type \$ and time stamp t_c, encrypted payment slip C_S and the certificate C_SCert. The encrypted payment slip C_S is encrypted with TTP's public key. The merchant checks the validity of the above data, and especially, the credit information and encrypted payment slip.

   (1) The merchant checks credit information with equality proof of knowledge (see section 2).

   (2) The merchant uses C_SCert to check C_S is the ciphertext of the payment slip $Slip$ signed by the client (see section 3.2).

   If the merchant finds anything wrong in the above verification, he will quit the protocol, and the protocol will be fair for both parties.
3. In step three, the merchant sends $P_{encr}(PKC, < Goods >_{skm})$ to the client. If the $Goods$ is consistent with the $offer$, the client will continue the protocol. If the $Goods$ is inconsistent with the $offer$, the client quits the protocol. If the merchant believes that it is not fair, he needs to require TTP to run the resolve protocol.
4. In step four, the client sends $P_{encr}(PKM, Slip)$ to the merchant. If the merchant can not get the payment, the merchant will ask TTP to run resolve protocol.

If the merchant can not get the payment, the merchant will ask TTP to run the following resolve protocol:


Merchant
TTP
Client
$<offer>_{skm}$, $SlipData$, C_S, $<Goods>_{skm}$
if $unfair\ to\ merchant$ **then** *continue* **else** *abort*
$P_{encr}(PKM, Slip)$
$P_{encr}(PKC, <Goods>_{skm})$

In the completion of the resolve protocol, the merchant has the payment and the client has the goods.

3.4 Properties of Fair Trading Protocol

Some general properties of cryptographic protocols such as integrity and confidentiality are not included in this section, even our fair trading protocol have these properties and can satisfy the related security requirements. Our discussions here only focus on the properties we have emphasized in the design and construction of the fair trading protocol. The fair trading protocol has perfect fairness and high efficiency and provides good availability & reliability of the involved services. The sensitive information (credit card) has untraceability & privacy in the fair trading protocol.

(1) Fairness

If both the merchant and the client behave according to the fair trading protocol, when protocol has completed, client has received the goods and merchant has received the payment. For the client, if something is wrong, he can quit the trading protocol after step three and the whole protocol is fair. For the merchant, if something is wrong after step three, he can bring $offer$, $SlipData$, C_S, $Goods$ to TTP. TTP will check the status. If it is really unfair to merchant, TTP will send the $Goods$ to the client and send the $Slip$ to the merchant. The protocol is fair against cheating attempts by either merchant or client. The protocol is fair in case of system failures as well. The fair trading protocol and the associate resolve protocol can guarantee the trading protocol to be fair in any case.

(2) Efficiency

In normal case, the TTP is off-line and the credit card service from a financial institution is off-line as well. The TTP is only involved when one party misbehaves or system failure happens. The protocol is more efficient than protocols with more on-line components. Computation and communication overheads are reduced to the minimum.

(3) Availability and Reliability

We compare two protocols A and B. If protocol A has one more on-line component than protocol B and all other parts of the two protocols are the same, the on-line component of protocol A has some chance to be unavailable or unreliable because of network problem, system failure or evil behaviors from involved parties or other attackers. Protocol A has less availability and reliability than protocol B. In the fair trading protocol in this paper, TTP and credit card service from a financial institution are off-line in normal case, the protocol is more available and reliable than other protocols with more on-line components (TTP is on-line, the credit card service is on-line or both of them are on-line).

(4) Untraceability and Privacy

The client uses the credit card to pay on the Internet in the fair trading protocol. Untraceability of the credit holder is a necessary or desirable characteristic of this kind of trading protocols. In our fair trading protocol, the credit card is anonymous, the untraceability and privacy of the card holder is achieved.

4 Concluding Remarks

We have introduced our fair trading protocol with off-line anonymous credit card payment over the Internet. The fairness for involved client and merchant is achieved in the protocol and the client is anonymous in the credit card payment. The TTP is off-line and the financial institution for credit service can be off-line as well. The details of digital constructions for credit card payment and fair trading process are provided in this paper. The technique of proof of equivalence of discrete logarithm to discrete log-logarithm is employed as the main building block to construct the protocol. The protocol provides a generic overall solution for fair on-line trading with credit card payment. The involvement of TTP and the on-line financial institution for the credit card service is reduced to the minimum. Our protocol has better efficiency and availability than protocols with more on-line components. The protocol can be used as the starting point to build some complicated protocols in on-line environment, such as on-line gambling protocols.

References

1. F. C. Gartner, H. Pagnia and H. Vogt, “Approaching a formal definition of fairness in electronic commerce”, In Proceedings of the International Workshop on Electronic Commerce (WELCOM’99), Lausanne, Switzerland, Oct. 1999.
2. V. Shmatikov and J. C. Mitchell, “Analysis of a fair exchange protocol”, Proceedings of the 1999 FLoC Workshop on Formal Methods and Security Protocols, 1999.
3. B.Cox, J.D.Tygar and M.Sirbu, “NetBill security and transaction protocol”, Proc. 1st USENIX Workshop on Electronic Commerce, pp. 77-88, 1995.
4. S.Ketchpel, “Transaction Protection for Information Buyers and Sellers”, Proceedings of the Dartmouth Institute for Advanced Graduate Studies ’95: Electronic Publishing and Information Highway, 1995.
5. A.Bahreman and J.D.Tygar, “Certified electronic mail”, Proc. Internet Society Symposium on Network and Distributed Systems Security, pp. 3-19, 1994.

6. R.H.Deng, Li Gong, A.A.Lazar and Weiguo Wang, “Practical protocols for certificated electronic mail”, J.Network and Systems Management, 4(3) pp. 279-297, 1996.
7. N.Asokan, V.Shop and M. Waidner, “Asynchronous protocols for optimistic fair exchange”, Proc. IEEE Symposium on Research in Security and Privacy, pp. 86-99, 1998.
8. R. Hauser, M. Steiner and M. Waidner, “Micro-payments based on iKP”, Technical Report 2791 (No. 89269), June 1996.
9. “SET Secure Electronic Transaction 1.0”, Technical Report, Mastercard, May 1997.
10. M. Sirbu and J. D. Tygar, “Netbill: An Internet commerce system optimized or network delivered services”. ¡http://www.ini.cmu.edu/netbill¿.
11. B. C. Neuman and G. Medvinsky,“Requirements for network payment: The netcheque perspective”, Proceedings of IEEE CompCon’95, March 1995.
12. Y. Mu and V. Varadharajan, “A new scheme of credit based payment for electronic commerce”, the Proceedings of 23rd Local Area Networks Conference, IEEE Computer Society, October, Boston, pp.278-284, 1998.
13. M. Stadler, “Publicly verifiable secret sharing”, Proceeding of Eurocrypto’ 96, LNCS 1070, Springer-Verlag, pp.190-199, 1996.
14. N. Asokan, M. Schunter and M. Waidner, “Optimistic protocols for fair exchange”, Proceedings of 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, pp.6-17, pp.6-17, 1997.
15. F. Bao, R. Deng and W. Mao, “Efficient and Practical Fair Exchange Protocols with Off-line TTP”, 1998 IEEE Symposium on Security and Privacy, pp.77-85, 1998.
16. J. Camenisch, “Efficient and generalized group signatures”, Advances in cryptology - EUROCRYPT’97, Lecture Notes in Computer Science 1233, Spring-Verlag, Berlin, pp.465-479, 1997.
17. Indrakshi Ray and Indrajit Ray, “An Optimistic Fair Exchange E-commerce Protocol with Automated Dispute Resolution”, EC-Web, pp. 84-93, 2000. http://citeseer.nj.nec.com/462055.html.