Trends in Mathematics
Information Center for Mathematical Sciences
Volume 8, Number 1, June, 2005, Pages 87–92

ON FAIRNESS IN ONLINE PURCHASE OF PHYSICAL GOODS (EXTENDED ABSTRACT)

JUN-BUM SHIN

ABSTRACT. A lot of on-line purchase systems are used for electronic commerce. But the omission of the face-to-face contract between buyer and seller can raise some problems, called disputes. In this paper, we study the fairness issues in online purchase of physical goods and propose a corresponding dispute-free payment system.

Keywords: electronic commerce, fairness, cryptography

1. INTRODUCTION

In our daily life, we use many kinds of payment systems like money, credit card, etc. and a lot of online payment systems are in use for internet shopping mall, internet bookstore, etc [5]. But the omission of the face-to-face contract between buyer and seller can raise many problems, called disputes. In payment systems, a dispute may arise if one participant does not follow the rule. For example, consider the following situation:

- Alice paid to Bob for the purchase of a product (item). However, Alice did not receive the item from Bob.

We say that a system is fair if it does not discriminate against a correctly behaving player (or an honest player). In this paper, we study the fairness issues in online purchase of physical goods and propose a corresponding dispute-free payment system. We assume that physical goods are delivered by third-party shipping company, and the model is shown in Figure 1. The purpose of our research is to develop a fair purchase system with this setting.

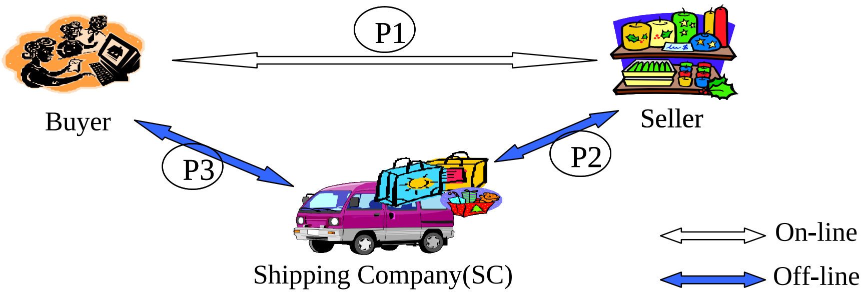

FIGURE 1. Online payment and offline delivery model

A lot of research has been done for fair electronic commerce A lot of work has been done in this area[11, 12, 6, 7, 9, 8], and in late-90s, Asokan et. al.s proposed a fair exchange model in which real payment systems (including credit card number transfer over SSL, 3D-Secure [1] and SET [3]) can be used for fair online purchase of digital goods. However this technique cannot be applied for the purchase of physical goods.

2. Our Approach

2.1. **Idea sketch and assumptions.** For handling a dispute, one of the most important properties is that the protocols should produce sufficient and proper evidence-tokens indicating how many steps have been completed [13].

In our approach, we apply the notion of fairness in each exchange phase, develop a dispute resolution rule from the meanings of evidence tokens, and verify its correctness:

- Step 1. Design an exchange phase s.t. each step can be distinguished by meaningful evidence tokens.
    - We suppose that the phase P1(buyer ↔ seller) in Figure 1 is the fair exchange of payment and receipt. In this case, it is easy to see that the payment happens if and only if a buyer holds a corresponding receipt, so we can consider the receipt as the evidence token of P1 in Figure 1. Similarly, for off-line exchange P2 and P3, we can get similar evidence token if we make each transaction be an exchange of physical goods and receipt.
- Step 2. Develop a dispute resolution phase based on the meanings of evidence tokens.
    - This step is intuitive if the system can produce meaningful evidence tokens. For example, consider the case that both buyer and seller hold the receipts, but the shipping company (SC) does not. This implies that SC receives the product from seller, but does not deliver it to the buyer. So the dispute can be resolved if we can let a TTP (Trusted Third Party) enforce SC to deliver the product to buyer.
- Step 3. Verify whether the rule can handle the dispute in a reasonable manner
    - This step is required to verify the soundness of dispute resolution rule developed in Step 2. When there is a problem, we should go to Step 2.

In our model, we assume the followings:

- A1(Security). Both digital signature and paper signature are secure.
- A2(Uniqueness). We can construct a label L uniquely identifies the exchange between buyer and seller
    - The uniqueness condition is satisfied if we let L contains two random numbers generated by buyer and seller.

- A3(Product Representation). There is a function desc s.t. anyone can check whether desc(L) = product(L).
- A4(Fairness-online). There exists a fair online exchange system for the exchange of payment and receipt
  - We can use classical fair online purchase system for digital goods. Note that we can let the receipt be the product because in online phase, the form of receipt is digital.
- A5(Fairness-offline). There exists a fair offline exchange system for the exchange of product and receipt
  - This is satisfied if two players exchange after verifying the product. However, it is unrealistic in some cases because of the privacy problem.

2.2. **Proposed System.** Our model assumes online payment but offline delivery settings. We assume that there are four participants, buyer, seller, shipping company(SC), and a TTP(Trusted Third Party for dispute resolution).
Purchase phase. Our model consists of four phases:

- P0. buyer ←(L:L)→seller
  - online negotiation of a label L.
  - L contains the purchase information (e.g. product type, value,).
- P1. buyer←(payment(L):NRR1(L))→seller
  - online exchange between payment(L) of buyer and NRR1(L) of seller.
  - NRR1(L): digital signature of seller on a message containing L.
- P2. seller⇐(product(L):NRR2(L))⇒SC
  - offline exchange between product(L) of seller and NRR2(L) of SC.
  - NRR2(L): paper signature of SC.
- P3. SC⇐(product(L):NRR3(L))⇒buyer
  - offline exchange between product(L) of SC and NRR3(L) of buyer.
  - NRR3(L): paper signature of buyer.

The system is summarized in Figure 2. Note that our model is similar to the basic model shown in Figure 2 except Phase 0, which is required to negotiate the product to purchase.

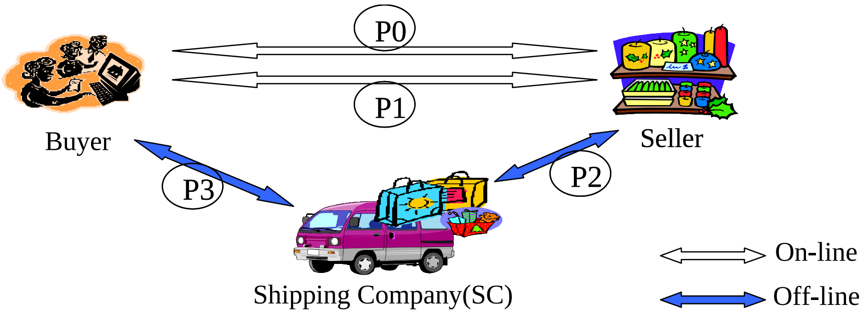

Figure 2. Proposed system

As mentioned in Section 2.1, we assume P1, P2, and P3 are fair exchange, so we let NRR1(L), NRR2(L), and NRR3(L) be evidence tokens: The meanings of them are summarized in Table 1.

Table 1. The holder of evidence tokens

	L	NRR1(L)	NRR2(L)	NRR3(L)
End of P0	Buyer, Seller			
End of P1	Buyer, Seller	Buyer		
End of P2	ALL	Buyer	Seller	
End of P3	ALL	Buyer	Seller	SC

Dispute Resolution Phase. In dispute resolution phase, each party can raise a dispute to TTP, by presenting a label L. TTP enforces each party to present his/her evidence tokens, and TTP makes a judgment using the dispute resolution role from the collected evidence tokens.

Note that the existence of NRR1(L) implies that P1 is completed, so the value is transferred from buyer to seller. Similarly that of NRR2(L) (resp. NRR3(L)) implies that P2 (resp P3) is completed, so the value is transferred from seller (resp. SC) to SC (resp. buyer).

We suppose that no one holds NRR1(L). This implies that there is no value transfer, so there is no reason for dispute. In this case, TTP can either ignore the case or charge the dispute raiser as calumny. On the other hands, consider the case that seller holds NRR2(L) but SC does not holds NRR3(L). This happens when SC holds the product but it does not deliver that to the buyer. In this case, it is reasonable for TTP to enforce SC to deliver the product to buyer.

Based on this observation, After P2, TTP verifies each evidence tokens and then makes the decision according to the last valid token: The judgment in each case is summarized in table 2, where

- $FORCE_0$: Ignore or charge the dispute raiser as calumny.
- $FORCE_1$: Enforce a seller to send the product to the seller.
- $FORCE_2$: Enforce SC to deliver the product to the seller.
- $FORCE_3$: Enforce buyer to receive the product from SC.

2.3. **Analysis.** We adopt the notion of fairness proposed by Wong [10].

> "A payment system is fair if for any participant, its interest is satisfied."

To simplify our discussion, we assume that the value of product does not change over time and there is no penalty due to the late delivery. Each player's interest can be expressed as follows:

- Buyer's interest: $+(L, payment) \Rightarrow \#(+(L, payment)) = 1 \wedge -product(L)$
  - Suppose that a buyer pays a payment ($+(L, payment)$). Then (i) this event does not happens more than once, ($\#(+(L, payment)) = 1$), and (ii) a buyer can receive the ordered product ($-product(L)$).

Table 2. Dispute Resolution Rules

The last valid token	Possible dispute raiser	Dispute	Decision by TTP
L	All	All	$FORCE_0$
NRR1(L)	Buyer	Delivery	$FORCE_1$
	Other	Other	$FORCE_0$
NRR2(L)	Seller	Delivery	$FORCE_2$
	SC	Delivery	$FORCE_3$
	Other	Other	$FORCE_0$
NRR3(L)	All	All	$FORCE_0$

- Seller's interest $+(L, product) \Rightarrow \#(+(L, product)) = 1 \wedge -payment(L)$
  - Suppose that a seller sends a product ($+(L, product)$). Then (i) the event happens only once ($\#(+(L, payment)) = 1$), and (ii) a seller can receive the intended payment ($-payment(L)$).
- SC's interest $+(L, NRR2(L)) \Rightarrow -NRR3(L)$
  - Suppose that SC receives the product $+(L, NRR2(L))$. Then SC can deliver the product to buyer ($-NRR3(L)$)

Below, we will show the fairness of proposed system, i.e., the proposed system satisfies every player's interest.

Lemma 1. *The proposed system satisfies buyer's interest.*

Proof Sketch: We suppose that a buyer pays a payment ($+(L, payment)$). From our assumption A1 and A2. ($\#(+(L, payment)) = 1$) is guaranteed, because (i) the signature for payment is unforgeable by A1, and (ii) L uniquely identifies each transaction by A2. We suppose that $+(L, payment)$ happens but the buyer does not receive the product. In this case a buyer can raise a dispute to TTP, and then the buyer can receive the product by $FORCE_1$ or $FORCE_2$. Finally, the product is the indented one by A3. □

Lemma 2. *The proposed system satisfies seller's interest.*

Lemma 3. *The proposed system satisfies shipping company(SC)'s interest.*

Their proofs are similar to that of Lemma 1, and this shows the fairness of proposed system.

3. Conclusion

In this paper, we proposed a fair online purchase system of physical product, and shows that our system is fair in the sense of Wong [10]

One weakness of proposed system is that our system does not satisfy the strong fairness: the system is not secure against the criminal that a dishonest seller intentionally runs away after receiving the payment without delivering the product. The problem can be fixed using payment escrow service, and the analysis of that system will be considered for the further research.

References

[1] Visa Authenticated Payment Program, 3-D Secure homepage.
Avialable at http://international.visa.com/fb/paytech/secure/main.jsp

[2] B. Cox, M. Sirbu, and J. D. Tygar. NetBill: An Internet Commerce System. In *IEEE COMPCON*, 1995.

[3] SET(Secure Electronic Transaction) homepage.
Available at http://www.setco.org.

[4] N. Asokan, Michael Steiner, and Els Van Herreweghen. Towards a Framework for Handling Disputes in Payment Systems. In *Proceedings of 3rd USENIX Workshop on Electronic Commerce*, 1998.

[5] N. Asokan, P. Janson, M. Steiner, and M. Waidner. State of the art in electronic payment systems. *IEEE Computer*, 30(9):28–35, 1997.

[6] N. Asokan, M. Schunter, and M. Waidner. Optimistic protocols for fair exchange. In *Proceedings of 4th ACM Conference on Computer and Communication Security*, 1997.

[7] N. Asokan, V. Shoup, and M. Waidner. Asynchronous Protocols for Optimistic Fair Exchange IEEE Security and Privacy, 1998

[8] O. Markowitch, D. Gollmann, and S. Kremer. On fairness in exchange protocols, ICISC 2002, LNCS 2587

[9] Indrakshi Ray and Indrajit Ray, An Optimistic Fair-Exchange E-Commerce Protocol with Automated Dispute Resolution, Proceedings of the First International Conference on Electronic Commerce and Web Technologies, Greenwich, U.K., LNCS 1875, 2000.

[10] H. C. Wong. Protecting Individual's Interests in Electronic Commerce Protocols. *PhD Thesis, School of Computer Science, CMU*, 2000.

[11] J. Zhou and D. Gollmann. A fair non-repudiation protocol. In *Proceedings of 1996 IEEE Symposium on Security and Privacy*, pages 55–61, 1996.

[12] J. Zhou and D. Gollmann. An efficient non-repudiation protocol. In *Proceedings of 1997 IEEE Computer Security Foundations Workshop*, pages 126–132, 1997.

[13] J. Zhou and D. Gollmann. Evidence and non-repudiation. *Journal of Network and Computer Applications*, 20:267–281, 1997.

Softforum Co., LTD., 6-8th FL, Mirae B/D. 545-7, Dokog-Dong, Gangnam-Gu, Seoul, 135-270, Korea

E-mail address: jbshin@softforum.co.kr