

A Survey on Fair Exchange E-commerce Protocols

Indrajit Ray and Indrakshi Ray
Department of Computer and Information Science
University of Michigan-Dearborn

Performing business over the internet where the parties cannot be trusted has necessitated the development of fair exchange protocols. These protocols are proposed in a variety of contexts (electronic mails, digital signatures, contract signing) where two parties want to exchange each other's items. The main objective of these protocol is: either both the parties obtain each other's items or none do. Sometimes it is not possible to meet the above objective and researchers have aimed for a weaker objective: gather evidence during protocol execution using which an honest party can prove his case. Protocols which meet any of the two objectives are termed fair exchange protocols. In this paper we review some of the work done on fair exchange.

1. INTRODUCTION

Fair exchange is often a requirement in secure electronic commerce protocols. In particular it is needed under scenarios where there is no established trust relation between the parties involved - be it B2B or B2C. A fair exchange protocol ensures that no party can gain an advantage over the other party by misbehaving, misrepresenting or by prematurely aborting the protocol.

Fair exchange protocols has been variously studied in the context of exchange of electronic mails, exchange of digital signatures, exchange of documents (where the consistency of the documents need to be verified before the exchange) and in the context of electronic payment for services. In electronic payment systems, fair-exchange is often referred to as "goods atomicity" – a merchant receives payment if and only if the customer receives the product.

Researchers have coined the word "true fair-exchange" to denote protocols that ensures that either both parties receive each other's item or none do. However, many a times true fair exchange is difficult to achieve. Instead some protocols rely on gathering evidence during the protocol execution, that can be used later for dispute resolution in a court of law. A human judge looks at the evidence and delivers his judgement. Researchers call such protocols "weak fair-exchange" protocols. There is also a set of protocols that emphasizes dispute avoidance rather than dispute resolution. Their opinion is that in e-commerce it may not be always feasible to take a erring party to a court of law - particularly when e-commerce may transcend geographical boundaries.

In this paper we review some of the more important fair exchange protocols that have been proposed within the last five or six years. The paper is organized as follows: Section 2 mentions some gradual exchange protocols. Section 3 describes some fair exchange protocols based on using a trusted online third party. Section 4 describes a protocol in which the third party can be trusted to lesser extent. Section 5 describes some protocols that involve the trusted third party only when some problem occurs. Section 6 concludes the paper.

2. GRADUAL EXCHANGE PROTOCOLS

Previous work on fair exchange schemes can be classified under two categories: (i) gradual exchange protocols and (ii) third party protocols. Gradual exchange protocols [Bahreman and Tygar 1994; Blum 1983; Even et al. 1985] gradually increase the probability of fair exchange over several rounds of message exchanges; these protocols have extensive communication requirements and assume that both the parties have equal computational power.

3. PROTOCOLS USING AN ON-LINE TRUSTED THIRD PARTY

The third party protocols [Cox et al. 1995; Deng et al. 1996; Franklin and Reiter 1997; Zhou and Gollmann 1996] make use of a trusted on-line third party. The idea of using a trusted on-line third party to obtain non-repudiation of origin and delivery of a mail message was proposed by Deng et al. [Deng et al. 1996] and Zhou and Gollmann [Zhou and Gollmann 1996]. These protocols are essentially similar. They differ in what information is exchanged and how the information gets transferred from one party to the other. The basic idea is as follows. When A wants to send a message to B, A encrypts the message with a key, and sends B the encrypted message and a trusted third party the key. B after submitting his proof of delivery can get the key and read the message. Dispute resolution is outside the scope of these protocols; however, the protocols do specify what evidence must be stored for the dispute to be resolved in a fair manner.

The use of fair exchange to sell and deliver low-priced network goods is advocated in the NetBill system [Cox et al. 1995]. The NetBill system uses a trusted third party called the NetBill server which maintains accounts for both the customer and the merchants, and is linked with conventional financial institutions. In this protocol the customer requests the merchant for a good. The merchant sends the good encrypted with a key. Upon receipt of this encrypted good, the customer supplies the merchant with a signed electronic purchase order. The electronic purchase order contains a segment that has payment information. This portion is readable only by the NetBill server. The merchant endorses the electronic purchase order, and forwards it to the NetBill server together with the decrypting key. The NetBill server debits the customer's account and credits the merchant's account and then sends a signed message to the merchant that includes the result of the transaction and an encrypted receipt intended for the customer. The encrypted receipt contains the decrypting key, and the status of the customer's account after the transaction. The receipt can be read only by the customer. The merchant forwards the encrypted message to the customer to complete the transaction. If, for some reason, the merchant does not deliver the receipt, the customer gets it from the NetBill server.

A fair exchange protocol ensuring the consistency of the document but requiring the active participation of a trusted third party has been proposed by Ketchpel [Ketchpel 1995]. The merchant and the customer after agreeing upon the product and the price sign a contract which is forwarded to the third party. Each party then sends his item to the third party. The third party verifies that the items satisfy the contract, and then forwards them to the respective parties. The customer sends the payment to the third party and the merchant sends the required product to the

third party. The third party verifies that the product and payment satisfy the terms of the contract and then forwards the product to the customer and the payment to the merchant.

Another protocol that uses an online trusted third party as an escrow agent has been proposed by Ray et al. [Ray et al. 2000]. This protocol aims at dispute avoidance. A merchant has several products to sell. The merchant places a description of each product on an on-line catalog service with the trusted third party together with an encrypted copy of the product. If the customer is interested in a product, he downloads the encrypted product from the third party and then sends a purchase order to the merchant. Note that the customer cannot use the product unless he has decrypted it. The merchant does not send the decrypting key unless the merchant receives payment. The customer does not pay unless he is sure that he is getting the right product. This is handled as follows: the merchant sends the product encrypted with a second key, K_2 , such that K_2 bears a particular mathematical relation with the key, K_1 , where K_1 is the key the merchant used when uploading the encrypted product on the trusted third party. Additionally, the merchant escrows the decryption key, \hat{K} , corresponding to K_2 , with the trusted third party. The mathematical relation between the keys K_1 and K_2 , is the basis for the theory of cross validation that has been proposed. Briefly the theory of cross validation states that the encrypted messages compare if and only if the unencrypted messages compare. Thus, by comparing the encrypted product received from the merchant with the encrypted product that the customer downloaded from the trusted third party, the customer can be sure that the product he is about to pay for is indeed the product he wanted. At this stage the customer is yet to obtain the actual product because he does not have the key, \hat{K} , to decrypt the encrypted product. Once the customer is satisfied with his comparison, he sends his payment token to the third party. The third party verifies the customer's financial information and forwards the decrypting key to the customer and the payment token to the merchant.

4. PROTOCOLS REQUIRING A SEMI-TRUSTED THIRD PARTY

Franklin and Reiter [Franklin and Reiter 1997] propose a set of fair exchange protocols that verify the consistency of a document before the exchange takes place. These protocols require a semi-trusted third party. A semi-trusted third party is one that can misbehave on its own but will not collude with any of the participating parties. The protocols use a one-way function f which has the property that there exists another efficiently computable function F such that $F(x, (f(y))) = f(xy)$. The function, f , is known by both the parties, and F is known by the third party. The authors suggest three ways how such a function f can be constructed: (i) construction based on factoring, (ii) construction based on discrete logarithms and (iii) construction based on graph isomorphism. The basic protocol is as follows. Suppose X and Y wish to exchange some secret information K_X and K_Y . Before the protocol is initiated, it is assumed that X and Y know $f(K_Y)$ and $f(K_X)$ respectively. The first step involves X sending a random number x_1 to Y, and Y sending y_1 to X. In the second step X sends the following to the third party: $f(K_X)$, $f(K_Y)$, $K_X x_1^{-1}$, and $f(y_1)$; Y also sends the corresponding components to the third party. The third party makes some comparisons to ascertain that each is sending the correct components, and then forwards $K_X x_1^{-1}$ to Y and $K_Y y_1^{-1}$

to X. Y and X can multiply these by x_1 and y_1 respectively to get the items.

One contribution of this paper is that the trusted party will not be revealed the informations which X and Y are trying to exchange. Note that the protocol will be compromised if X can find a $\hat{K}_X \neq K_X$ such that $f(\hat{K}_X) = f(K_X)$. In that case, X will have received the worthy information K_Y from Y and will have given the worthless information \hat{K}_X to Y. To counter this problem, the authors suggest that f be a function of the document encrypted with K_X , and make it difficult to determine a \hat{K}_X such that $f(\hat{K}_X) = f(K_X)$. The authors argue that this is possible because the protocol does not require the same f to be used by X and Y. However, not using the same f for X and Y and making f a function of the encrypted document involves additional communication overhead. Suppose X uses f and Y does not use f but uses g , then f and g must be communicated to Y and X respectively. In such a case the third party, in addition to knowing F , must also know G which is a function such that $G(x, g(y)) = g(xy)$. In short, making f a function of the document encrypted with K_X makes the protocol cumbersome and involves additional communication overhead.

A second solution to this problem is to require f to be collision-free. If the construction of f is based on discrete logarithms, f is collision free; however this construction is more computation intensive than the other two. The construction based on graph isomorphism is not collision free. For constructions based on factoring trivial collisions can be found; however the protocol must be extended to include mechanisms for detecting and overcoming such collisions.

5. OPTIMISTIC PROTOCOLS

Three fair exchange protocols that do not require the involvement of the third party unless there is a problem, have been proposed by Bao et al. [Bao et al. 1998]. The first one exchanges digital signatures on some document, the second one exchange signatures on two documents, and the third one exchanges a document and a signature on the document. The important contribution of this paper is that the authors provide a theory based on which each party is able to verify that the signature he is about to receive is indeed the correct signature, before actually receiving the signature. Asokan et al. [Asokan et al. 1998] also provide an optimistic protocol for the fair exchange of digital signatures.

A more general optimistic protocol that allows exchange of any two digital items has been proposed by Asokan et al. [Asokan et al. 1997]. This protocol does not involve the third party unless one of the parties behaves unfairly or aborts. The basic protocol is as follows. The two parties, termed originator and recipient, wish to exchange two items. The protocol begins by the two parties promising each other an exchange of items. If they agree on the terms of the exchange, the exchange takes place. The items as well as non-repudiation tokens are exchanged. When each party receives an item, the item is checked to see if it matches the description. In case of any failure or any party misbehaving, the recovery phase which involves the third party is initiated. The authors assume there is a reliable communication channel between each party and the third party. Hence, all the messages exchanged in the recovery phase uses these reliable channels via the third party. When any party misbehaves, the third party can issue an affidavit which can be used in a court of law in case of a dispute. Non-repudiation of origin and non-repudiation of

receipt is guaranteed by these protocols. The protocol always guarantees that an honest party can prove his case in case of a dispute. However, a dishonest recipient after receiving the exchange item can simply disappear without sending the item he promised. The authors state under what conditions fair-exchange can be ensured: (i) the item sent by the originator is revocable or (ii) the item sent by the recipient is generatable. Generability or revocability can be obtained by depositing the items with a third party, who can take the proper steps when presented with an affidavit. Thus to ensure fair-exchange the protocol must actively use a third party.

Another protocol that does not require the involvement of the trusted third party unless a problem occurs has been proposed by Ray et al. [Ray and Ray 2000]. A merchant who wishes to sell some electronic products registers itself with the third party. The merchant sends the products, their description which includes the cost, and a key K_{M_1} to the third party. The third party encrypts all the products with the key and advertises them on the web. A customer interested in buying a product must have an account with some bank. Each customer has a key K_{C_1} that is known by both the bank and the customer. The protocol begins by the customer downloading an encrypted product from the third party. The customer gets a payment token signed by the bank. The value of the payment token is the cost of the item. The customer sends a purchase order to the merchant together with the payment token signed by the bank and encrypted with a key denoted by $K_{C_1} \times K_{C_2}$. This key has a mathematical relation with the K_{C_1} . The merchant sends the product encrypted with key $K_{M_1} \times K_{M_2}$. Using the theory of cross-validation, the customer is able to verify that the product he is about to receive is the one he will be paying for. If the customer is satisfied, he sends the merchant the keys necessary to decrypt the payment token. If the merchant is satisfied with the payment token, he sends the key required for decrypting the product to the customer. If the merchant does not send the product, the third party is contacted who can send the product to the customer. Thus, fairness is ensured by this protocol. Although the protocol is described in the context of purchase of electronic goods using electronic currency, it can be used for the exchange of any two digital items.

6. CONCLUSION

In this paper we have reviewed some of the more important fair-exchange e-commerce protocols. Fair-exchange protocols are necessary to ensure that no party involved in an e-commerce transaction, gains an unfair advantage over the other party by misbehaving, misrepresenting or by prematurely aborting the transaction. A majority of the works attempts to ensure only “weak fair-exchange” where the emphasis is on gathering evidence that can be used at the protocol conclusion to ensure justice. However there are quite a few that attempt to ensure “true fair-exchange” and some protocols that emphasize dispute avoidance.

Protocols that rely on trusted third party for mediating the fair-exchange often require the third party to be on-line. This is serious drawback as the third party is a source bottleneck. Optimistic protocols tries to minimize the use of a third party. Typically they do not approach the third party unless a problem occurs. Thus the third party can be off-line which is a major advantage. However, having a third party – on-line or off-line – has serious implications for anonymous fair-exchange

protocol. On the other hand, protocols that do not require a third party seem promising for anonymous exchanges, although they have not been well investigated. Such protocols often require complex cryptographic computation that may not be widely available.

Summarizing, we believe that two areas appear good candidates for research – fair exchange protocols that do not rely on third party and yet are computationally simple and anonymous fair-exchange protocols.

REFERENCES

- ASOKAN, N., SCHUNTER, M., AND WAIDNER, M. 1997. Optimistic Protocols for Fair Exchange. In T. MATSUMOTO Ed., *Proceedings of the 4th ACM Conference on Computer and Communications Security* (Zurich, Switzerland, April 1997), pp. 7–17.
- ASOKAN, N., SHOUP, V., AND WAIDNER, M. 1998. Optimistic Fair Exchange of Digital Signatures. In *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Eurocrypt '98* (Helsinki, Finland, June 1998), pp. 591–606.
- BAHREMAN, A. AND TYGAR, J. D. 1994. Certified Electronic Mail. In *Proceedings of the Internet Society Symposium on Network and Distributed Systems Security* (February 1994), pp. 3–19.
- BAO, F., DENG, R. H., AND MAO, W. 1998. Efficient and Practical Fair Exchange Protocols with Off-line TTP. In *Proceedings of the IEEE Symposium on Security and Privacy* (Oakland, California, May 1998).
- BLUM, M. 1983. How to Exchange (Secret) Keys. *ACM Transactions on Computer Systems* 1, 175–193.
- COX, B., TYGAR, J. D., AND SIRBU, M. 1995. NetBill Security and Transaction Protocol. In *Proceedings of the 1st USENIX Workshop in Electronic Commerce* (July 1995), pp. 77–88.
- DENG, R. H., GONG, L., LAZAR, A. A., AND WANG, W. 1996. Practical Protocols for Certified Electronic Mail. *Journal of Network and System Management* 4, 3.
- EVEN, S., GOLDREICH, O., AND LEMPEL, A. 1985. A Randomized Protocol for Signing Contracts. *Communications of the ACM* 28, 6 (June), 637–647.
- FRANKLIN, M. K. AND REITER, M. K. 1997. Fair Exchange with a semi-trusted Third Party. In T. MATSUMOTO Ed., *Proceedings of the 4th ACM Conference on Computer and Communications Security* (Zurich, Switzerland, April 1997), pp. 1–6.
- KETCHPEL, S. 1995. Transaction Protection for Information Buyers and Sellers. In *Proceedings of the Dartmouth Institute for Advanced Graduate Studies '95: Electronic Publishing and the Information Superhighway* (1995).
- RAY, I. AND RAY, I. 2000. An Optimistic Fair Exchange E-commerce Protocol with Automated Dispute Resolution. In *Proceedings of the 1st International Conference on Electronic Commerce and Web Technologies* (London, U. K., Sept. 2000).
- RAY, I., RAY, I., AND NARASIMHAMURTHI, N. 2000. A Fair-Exchange Protocol with Automated Dispute Resolution. In *Proceedings of the 14th Annual IFIP WG 11.3 Working Conference on Database Security* (Schoorl, The Netherlands, Aug. 2000).
- ZHOU, J. AND GOLLMANN, D. 1996. A Fair Non-repudiation Protocol. In *Proceedings of the IEEE Symposium on Security and Privacy* (Oakland, California, May 1996), pp. 55–61.