Fair Exchange in E-commerce

INDRAJIT RAY and INDRAKSHI RAY
Department of Computer Science
Colorado State University

Many business transactions over the Internet involve the exchange of digital products between two parties – electronic mails, digital audio and video, electronic contract signing and digital signatures, to name a few. Often these transactions occur between players that do not trust each other. To facilitate such transactions, a number of secure protocols have been proposed. The main objective of these protocols 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 collectively termed fair exchange protocols. In this paper we review some of the work done on such fair exchange protocols and identify areas that still need to be addressed.

Categories and Subject Descriptors: H.4.m [**Information Systems Applications**]: Miscellaneous

Additional Key Words and Phrases: electronic commerce, fair-exchange, security, protocols

1. INTRODUCTION

Electronic commerce transactions, specially those that involve the exchange of digital products between the transacting parties, have additional requirements as compared to classical brick-and-mortar transactions. In the classical business environment, a transaction essentially involves fulfillment of some obligation by two parties; a contract describes the penalties if either party fails to meet its obligation. For example, a purchase of products involve the merchant delivering the product and, simultaneously, a customer paying for it. Since each transacting party has an identifiable place of doing business, if any party behaves unfairly in the transaction, that party can be physically approached and held accountable for its unfair behavior, according to the terms of the contract. In an electronic commerce environment, on the other hand, a party does not always have a physically identifiable place of doing business. After behaving unfairly in the electronic commerce transaction, a party can simply vanish without trace. In such a case, it may be next to impossible to enforce the penalties of the contract. Consequently, in an electronic commerce environment the two parties are reluctant to trust each other.

Owing to this lack of trust, electronic commerce protocols need to be carefully designed to prevent unfair business dealings by any player involved. However, it is not a simple proposition. Consider the following transaction. A customer C contacts an on-line mer-

Authors' address: Department of Computer Science, Colorado State University. 601 South Howes Street, Fort Collins, CO 80523.
Email: \{indrajit,iray\}@cs.colostate.edu

chant M for a product P. The product is an electronic database. Now the customer is not willing to pay for the product without being sure it is the right database sent by the merchant. A merchant is not willing to give the database unless he is sure that he will receive the proper payment. If the merchant delivers the product prior to receiving the payment, the fraudulent customer may simply disappear after getting the product, causing loss for the merchant. If, on the other hand, the customer pays before receiving the product, the merchant may not deliver it or may deliver some wrong product.

Fairness is thus often a stronger requirement in secure electronic commerce protocols. Fairness is achieved in the transaction if at the end of it, either each player fulfills its obligation and receives the item it expects, or neither receives any portion of the other's item. A fair exchange protocol can then be defined as *a protocol that ensures that no player in an electronic commerce transaction can gain an advantage over the other player by misbehaving, misrepresenting or by prematurely aborting the protocol*.

Note that the problem of fair exchange is not just limited to information goods. We always assume that fairness is ensured in any business transaction. In an electronic commerce transaction where the product is not a piece of information, but rather something more tangible, we automatically have the same set of safeguards that ensure fair exchange in conventional transactions. However, if the product is a piece of information that is transmitted electronically over an inherently insecure medium such as the Internet, with the destination address possibly not bound to any physical address, fair exchange is more difficult to achieve. Thus the problem of fair exchange for information goods have received the widest attention lately and the term is now mostly used to denote such protocols.

Further, the problem is not always primarily a cryptographic problem. For example, we can achieve fair exchange by utilizing an escrow agent in the transaction. The escrow agent receives the item to be exchanged from each player and performs the exchange. Assuming that there is a reliable communication mechanism (in the sense that it does not produce errors or it cannot be tapped into and so on) between the escrow agent and each player, such a protocol can be implemented without recourse to any cryptographic protocols. Over the Internet reliable communication can be achieved only by utilizing cryptographic techniques. It is no surprise, therefore, that fair exchange electronic commerce protocols have received the maximum attention from researchers in cryptography.

Fair exchange protocols have 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.

Majority of the fair exchange protocols *rely on gathering evidence during the protocol execution, that can be used later for dispute resolution in a court of law*. The dispute resolution phase is not a part of the protocol. After the protocol is completed, a human judge looks at the evidence and delivers his judgment. Researchers call such protocols "*weak fair-exchange*" protocols. These protocols try to emulate conventional business transactions. However, in the electronic commerce world such after-the-fact dispute resolution may not always be possible, for example when the transaction transcends geographical boundaries. Researchers have also proposed a number of other fair exchange protocols that try to avoid disputes and ensure that if disputes arise they are resolved within the scope of the transaction without requiring human judges. These protocols, called "*true fair-exchange*" or "*strong fair-exchange*"protocols, achieve fair exchange by *ensuring that either both players receive each other's item or none do.*

In this paper we review some of the more important fair exchange protocols that have been proposed within the last few years. We use the following terms in our categorization of fair exchange protocols.

Trusted third party. This is a player in the fair exchange protocol that acts like an escrow agent. The parties that exchange goods rely on this player to ensure that fairness is achieved at the end of the protocol. It is assumed that the trusted third party will not misbehave or collude with one of the transacting parties.

Semi trusted third party. The requirements on the third party is less stringent. The third party still acts like an escrow agent but it can now misbehave. However, it cannot collude with any of the transacting parties.

Online trusted/semi-trusted third party. The third party (trusted or semi-trusted) will always be available during the entire duration of the electronic transaction. It cannot fail.

Fair exchange protocol. An electronic commerce protocol that ensures that no player gains an unfair advantage over the other player by misbehaving misrepresenting or prematurely aborting the protocol.

True fair exchange protocol. An fair exchange protocol that ensures that either both players receive each other's item or none do so.

Weak fair exchange protocol. An fair exchange protocol that gathers evidence during protocol execution so that a misbehaving party is identified in case of a dispute and (somehow) made to pay for its misdeeds. These protocols assume that the misbehaving parties can be brought to justice.

Gradual exchange protocol. A fair exchange protocol that gradually increases the probability of fairness being achieved over several rounds of message exchanges between the players. Typically these protocols are complex and make use of advanced cryptographic techniques. However, the protocols do use any third party.

Optimistic protocol. A fair exchange protocol that relies on a trusted / semi-trusted third party but does not require the third party to be online and the third party does not behave like an escrow agent. These protocols assume that most of the time the players will not misbehave. Only when something wrong happens, is the third party contacted to resolve the dispute.

We characterize the set of protocols into four types: (i) Gradual exchange protocols, (ii) Protocols using online trusted third party, (iii) Protocols using online semi-trusted third party and (iv) Optimistic protocols that use off-line third parties. The rest 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 a lesser extent. Section 5 describes some optimistic protocols. Section 6 concludes the paper by identifying areas that require further research.

2. GRADUAL EXCHANGE PROTOCOLS

Most of the earlier works in fair-exchange protocols have been gradual exchange protocols [Blum 1983; Even et al. 1985; Ben-Or et al. 1990; Sandholm and Lesser 1996]. These protocols 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.

The protocol presented by Blum [1983] provides a mechanism by which two players can exchange secrets. The secrets are such that they are prime factors of the players' publicly announced composite numbers. The two players exchange their respective secrets bit by bit, alternately. For each bit provided to the adversary, a player has to prove that the bit is good, that is, it is part of the secret. The protocol assumes that both players have equal computational capability and an equal knowledge of algorithms. The author shows how the protocol can be used in conjunction with digital signatures to sign contracts and send certified emails.

Even et al. [1985] propose the notion of a *1-out-of-2 oblivious transfer protocol*. The authors define a message to be a "recognizable secret message" if, although the receiver cannot compute the message, he/she can authenticate it once received. An *oblivious transfer* of a recognizable secret message is a protocol by which a sender transfers a message to the receiver so that the latter gets the message with a probability of 0.5, while for the sender the a-posteriori probability that the receiver got the message is 0.5. A special case of the oblivious transfer protocol is the *1-out-of-2 oblivious transfer* protocol by which the sender is able to transfer exactly one secret out of two recognizable secrets. Using the 1-out-of-2 protocol as the basis, the authors propose protocols for contract signing, certified mail and coin flipping. As in the protocol proposed by Blum [1983], here two the players exchange the items one bit at a time.

Ben-Or et al. [1990] provide an approach in which each party gradually release information that incrementally increases the probability that a fair exchange is valid. This probability approaches 1 after several rounds of message exchanges. This protocol, unlike [Blum 1983], does not require both players to have equal computational power.

The protocols described by Blum [1983], Even et al. [1985], or by Ben-Or et al. [1990] are, however, not quite suitable for electronic commerce systems that exchange some value over the network - for example digital money. These protocols lack in simultaneity of the exchange. Thus, if midway through any of these protocols one of the parties decide to stop the exchange, then it is possible that that party will hold an unfair advantage over the other party. Such midway, unilateral termination of an exchange may be quite possible in real life. For example, the transaction may seem profitable to a player when viewed *ex ante*. However, during the course of the transaction, some event occurs that modifies the perception of the player about the transaction.

Sandholm and Lesser [1996] choose a game theoretic approach in the context of automated negotiation systems, to motivate the players to behave fairly in the transaction. The authors proposes a leveled commitment contracting protocol that allows any player to pay a penalty and withdraw from a contract due to some unexpected event happening in the course of the transaction. This ensures that no player has unfair advantage over the other player at any point in the protocol. However, the problem with this approach is that the protocol assumes that both players behave rationally during the protocol execution. For e-commerce transactions over the Internet, this may often be too strong a requirement.

3. PROTOCOLS USING AN ON-LINE TRUSTED THIRD PARTY

Third party protocols like those proposed by Bahreman and Tygar [1994], Cox et al. [1995], Deng et al. [1996], Franklin and Reiter [1997] and Zhou and Gollmann [1996] use 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 Bahreman and Tygar [1994], Deng et al. [1996] and 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 [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. [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 to 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 [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 information that X and Y are trying to exchange is never revealed to the trusted party. 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. [1998]. The first one exchanges digital signatures on some document, the second one exchanges 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. [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. [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 generable. 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 and Ray [2000]. The protocol works as follows. 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 work 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 a serious drawback as the third party is a source bottleneck. If the third party is subject to a denial-of-service attack or otherwise compromised, fair exchanged can be often compromised. 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, the third party still remains a bottleneck.

Ensuring fair exchange becomes extremely difficult if any of the players desire to be anonymous in the transaction. Anonymity ensures that the identity of any player is not revealed during the transaction. Having a third party – on-line or off-line – has serious implications for anonymous fair-exchange protocol. The evidence that is stored at the third party during the protocol execution can, in turn, often be used to trace back the identity of the true players. A number of protocols address the issue of anonymity of the players [Chaum 1985; Medvinsky and Neuman 1993; Low et al. 1994; 1996; Ray and Ray 2001]. However, none except [Ray and Ray 2001] address the problem of anonymity in the context of fair exchange.

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

ACKNOWLEDGMENT

The authors would like to take this opportunity to thank the reviewers for their profound remarks and very useful suggestions. This work has been partially supported by the National Science Foundation under grant EIA 9977548.

REFERENCES

ASOKAN, N., SCHUNTER, M., AND WAIDNER, M. 1997. Optimistic Protocols for Fair Exchange. In *Proceedings of the 4th ACM Conference on Computer and Communications Security,* T. Matsumoto, Ed. Zurich, Switzerland, 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, 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*. 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.

BEN-OR, M., GOLDRICH, O., MICALI, S., AND RIVEST, R. 1990. ”a fair protocol for signing contracts”. *IEEE Transactions on Information Theory 36,* 1, 40–46.

BLUM, M. 1983. How to Exchange (Secret) Keys. *ACM Transactions on Computer Systems 1,* 2 (May), 175–193.

CHAUM, D. 1985. ”security without identification: Transaction systems to make big brother obsolete”. *Communications of the ACM 28,* 10 (Oct.), 1030–1044.

COX, B., TYGAR, J. D., AND SIRBU, M. 1995. NetBill Security and Transaction Protocol. In *Proceedings of the 1st USENIX Workshop in Electronic Commerce*. 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, 279–297.

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 *Proceedings of the 4th ACM Conference on Computer and Communications Security,* T. Matsumoto, Ed. Zurich, Switzerland, 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*.

LOW, S., MAXEMCHUK, N., AND PAUL, S. 1994. Anonymous Credit Cards. In *Proceedings of the 2nd ACM Conference on Computer and Communications Security,* J. Stern, Ed. Fairfax, Virginia, 108–117.

LOW, S. H., MAXEMCHUK, N. F., AND PAUL, S. 1996. Anonymous Credit Cards and Their Collusion Analysis. *IEEE/ACM Transactions on Networking 4,* 6 (Dec.), 809–816.

MEDVINSKY, G. AND NEUMAN, B. 1993. Netcash: A design for practical electronic currency on the internet. In *Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, VA*. 102–106.

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.

RAY, I. AND RAY, I. 2001. ”an anonymous fair-exchange e-commerce protocol”. In *Proceedings of the 1st International Workshop on Internet Computing and E-Commerce, San Francisco, CA.*

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.

SANDHOLM, T. AND LESSER, V. 1996. Advantages of a leveled commitment contracting protocol. In *Proceedings of the 13th National Conference on Artificial Intelligence*. 126–133.

ZHOU, J. AND GOLLMANN, D. 1996. A Fair Non-repudiation Protocol. In *Proceedings of the IEEE Symposium on Security and Privacy*. Oakland, California, 55–61.