A Practical Approach of Fairness in Web-based E-learning

Debajyoti Konar, *Member IAENG* and Chandan Mazumdar

Abstract— **In this paper we present a practical approach of fairness in E-learning on demand. A generalized model of E-learning is also presented here. The paper also presents a GSR Fair Exchange protocol for E-learning on demand that ensure fairness in true sense without using an additional trusted third party. A detailed analysis of the properties is also presented in this paper. We conclude this paper by indicating future area research.**

Keywords- Correctness of course; E-learning; Fair Exchange; Gradual Secret Release; Money atomicity;

I. INTRODUCTION

In today's world of distance learning, delivery of course materials on demand is shifted to E-delivery for low cost and high efficiency. Since transactions in such cases transcend the boundaries of states and countries, it may become difficult to trace maliciously behaving transacting parties. Moreover, since transactions are made over public channels such as the world-wide web, *information security* becomes a major barrier to the success of such E-transactions. This situation leads to major research efforts on information security services, viz., *confidentiality*, *integrity, availability, authentication* and *non-repudiation*. Among these, *non-repudiation* is a security service that creates, collects validates and maintains the cryptographic evidences to support settlement of possible dispute among the transacting parties. The transacting parties will have more confidence in taking part in E-learning with the provision of *non-repudiation* service. Two or more parties involved in a commercial transaction can identify their activities as a sequence of message exchanges, or in short a protocol. During these exchanges in the protocol, a non-repudiation service protects all transacting parties from false denial of having been involved in the transaction. The fairness of these protocols of transaction is the way that guarantees that either all the parties obtained what they want or none do. The issue of *fairness* is becoming increasingly important in fast growing scenario of E-learning, E-governance; broadly E-commerce. The current proliferation of on-line activities makes it difficult for a user to establish the credibility of a counter party in a commercial transaction on the internet. So *E-learning protocols* are required to provide mutual guarantees to the protocol participants and ensure fairness. As a result, fairness of these protocols has become an important field of research. A common approach to ensure fairness is to include a Trusted Third Party (TTP) in the transactions, in *Inline, Online or Offline* mode. In many of these TTP-based protocols, some important application specific properties are maintained. But, the subscription to and maintenance of such TTPs are costly. In a second approach, instead of using a TTP, Secrets ate released gradually resulting in so-called Gradual Secret Release (GSR) protocols. But, most of such protocols fail to provide application specific properties. The challenge is to develop GSR protocols with acceptable fairness for e-learning activities, which satisfy the application specific properties. Availability of E-payment systems and online banking coupled with the popularity and rising demand of e-learning, provides the motivation of this research.

In this paper we describe briefly some previous work in section II. The section III outlines fairness in E-transaction by defining the most required terms and providing symbols and notations and section IV presents the approaches to achieve the practical fairness in E-learning. Then we present a model to develop GSR fair exchange protocols for E-learning and also a Practical Fair exchange GSR Protocol along with the analysis of its properties in section V. Section VI concludes the paper by indicating future scope of work.

II. PREVIOUS WORK

In this section we discuss briefly some related work in providing fair-exchange broadly in E-commerce or in other E-transactions. In previous works, trusted third party (TTP) is used in most of the fair exchange protocols either in offline mode or in online mode. By using the third party in off-line mode, the optimistic fair exchange protocols have a considerable contribution in the field of fair exchanges in E-commerce. There are some GSR protocols for fair exchange in which the participants increase the probability of fair exchange gradually over several rounds of message exchanges. The idea of using a trusted third party in on-line mode to obtain non-repudiation of origin and delivery of an email message was proposed by Deng et al. [3] and Zhou and Gollmann [5]. In essence, these protocols are similar. An E-Payment Protocol to Realize Fair- Exchange *by Q.Zhang,K.Mayes, K. Markantonakis et. al* in 2004 [17] has been designed to provide a user centric m-payment solution over internet by ensuring fair exchange, customer's anonymity and implementing an embedded biometric authentication framework for high security requirement. The correctness of the product is assured by theory of cross validation within this protocol. But maintaining on-line third party makes the protocol costly in implementation and use. There are several fair exchange protocols that use third party in offline mode, when it is required and hence they are optimistic fair exchange protocol. These protocols are designed either to sign a contract or to purchase a digital product. An Optimistic Contract Signing Protocol [7] has

Manuscript received October 04, 2011.

Debajyoti Konar is with West Bengal University of Technology, Kolkata – 700 064, India. (konar.d@gmail.com)

Cgandan Mazumdar is with Jadavpur University, Kolkata – 700 032, India. (chandan.mazumdar@gmail.com)

been designed by *Asokan, Shoup and Waidner* to provide a service to Originator and Responder for obtaining each other's commitment on a previously agreed. On the other hand there are some effective works to provide the fair exchange protocols for purchasing of digital goods through E-commerce. An Anonymous Fair Exchange E-commerce Protocol [11] by Ray and Ray uses customer, customer's bank, merchant, merchant's bank and an additional offline TTP as transacting parties to achieve fairness, correctness of the product and customer's anonymity properties. An Optimistic Anonymous Protocol with Validated Receipt *I. Ray et al* [20] also involves customer (C), merchant (M) and customer's bank (B), along with an additional offline TTP to achieve fairness and *validated receipt* properties. Both the protocols are for E-trading. The GSR protocols have extensive communication requirements. On the other hand the cost of maintaining third party is nil, which makes these protocols cost effective in implementation for E-commerce. The GSR protocol presented by *Blum* [2] can be used in conjunction with digital signatures to sign contracts and send certified emails. This protocol provides a mechanism to exchange secrets between two parties. To motivate the participants to behave fairly in the transaction *Sandholm and Lesser* use game theory in their work [4]. The authors propose a contracting protocol, which is in essence a fair exchange protocol. To ensure fairness in contracting, the protocol allows any player to pay a penalty and withdraw from a contract during the execution. This game theoretic approach in the protocol assumes that all the participants behave rationally, but without a very strong reason to behave rationally, it is too daring a assumption.

III. DEFINITIONS & NOTATIONS

To present the definitions we refer the principal parties in message exchange as originator or sender in one side and responder or recipient of message in other side. Here we also refer another participating party in message exchange, which is trusted third party.

Fairness: An important property in these non-repudiation protocols is fairness with which neither party can gain an advantage by quitting prematurely or otherwise misbehaving during a transaction.

Probabilistic fairness: A non-repudiation protocol is e-fair if and only if the probability that at the end of a protocol execution either originator or sender got the non-repudiation of receipt evidence for the message m, and responder or recipient got the corresponding message m as well as the non-repudiation of origin evidence for this message, or none of them got any valuable information, is greater than (1-e).

An Optimistic Fair-Exchange Protocol: It is a fair-exchange protocol that relies on a trusted third party but does not require the active involvement of the third party.

Money Transfer Instruction (MTI): An instruction issued by any transacting party of the protocol to his/her bank consisting the information regarding the amount to be transferred, the account which is to be debited and the account in which the amount is to be credited.

Course Requisition (CR): In the scope of this E-learning '*Course Requisition*' can be defined as a message containing the information regarding the course, the student intends to subscribe, the price of the digital course, identity of the student.

Digital Demand Draft or Pay-order (P): In this protocol 'Digital Demand Draft or Pay-order' can be defined as a message containing the information regarding the amount and currency that is to be credited, the account in which the payment is to be credited and a nonce to prevent the replay.

Correctness of course: It is a property of an E-learning protocol to ensure that the digital course the student is about to receive from an institute, is the same as the digital course the student intended to subscribe, before the student pays for it [11].

Money Atomicity: An e- transaction protocol satisfies the money atomicity property if money is neither created nor destroyed during the execution of the protocol [20].

Timeliness: A non-repudiation protocol provides timeliness if and only if preserving fairness all honest parties always has the ability to reach a point in the protocol where they can stop the protocol in a finite amount of time [15].

TABLE I: NOTATIONS

T_i	Transaction involving purchase of m
A_{prv}, A_{pub}	A's private and public keys
A_{iprv}, A_{ipub}	A's private and public keys for T_i
$A \rightarrow B$:X	A sends X to B
[X,*K*]	Encryption of X with key *K*
CC(X)	Cryptographic checksum of X
c	The digital course material
CR	Course Requisition by the student for digital course
MTI	Money Transfer Instruction
P	Pay Order or Digital Draft
ack	Acknowledgement message
rcpt	:Receipt of message
rcpt(ack)	:Receipt of acknowledgement
final_accept	:Final acceptance of the payment

IV. APPROACH ES FOR ACHIEVING PRACTICAL FAIRNESS IN E-TRANSACTION

Gartner, Pagnia and Vogt approached a formal definition of *fairness in E-commerce* [26] in 1999. They considered *strong fairness in E-commerce* as form of fairness which can be ensured completely within the system without additional assumptions about participating nodes. A probabilistic approach to define the fairness of a fair exchange protocol has also been considered by the researchers. An E-commerce protocol is e-fair [12], [15] if and only if the probability that sender got the NRR evidence for the message and the recipient got the corresponding message, as well as the NRO evidence for this message or none of them got any valuable information, is > (1-e). Zhou specifically defined the

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

fairness in 2001 [9] as a property which provides the originator and the recipient with valid irrefutable evidence after completion of the protocol, without giving a party an advantage over the other party in any possible incomplete protocol run. In 2002, Kremer et al categorically presents a definition of *strong and weak fairness* [15]. A Fair exchange protocol is said to be the provider of *strong fairness* if and only if at the end of a protocol execution either one party got the non-repudiation of receipt evidence for a message and the other got the corresponding message as well as the non-repudiation of origin evidence for this message, or none of them got any valuable information [15]. Otherwise the protocol is said to be the *weak fairness* provider. There are concepts of strong, eventually strong and weak fairness in [26] too. In their definition, weak fairness allows sufficient evidence to be gathered during the protocol execution to resolve the conflicts outside the system. Keeping the above definitions of *fairness* and their forms in view, a practical form of *fairness* is defined in this work, namely, *fairness in true sense*. In particular, to hold *fairness in true sense* a NR protocol is required to ensure the following:

(a) one party is not able to deny to send the digital content what s/he supposed to send
(b) the other party is not able to deny the receipt of the digital content what s/he received
(c) either party is able to have the correct digital content against his/her own digital content.

A fair exchange protocol should not give the originator an advantage over the recipient or vice-versa. Fairness is a complex term and has been used in many different areas with different connotation. In E-commerce, it refers to a property that does not discriminate any party on getting advantage during the transaction. Approaches for fair exchange reported in existing literature mainly are of two categories.

(i) TTP Protocols: which use inline, online or offline trusted third party to achieve fair exchanges. There are several published literatures, which provide protocols with TTP [6] – [8], [10], [11], [13], [14], [16], [18], [19], [22] – [25].

(ii) GSR Protocols: Zhou defined the *Gradual Exchange Protocol* [9] as a protocol where two parties gradually disclose the expected items in many steps. *Gradual Exchange* approach can be utilized without any third party in achieving *fairness*. Classically, in *Gradual Exchange* approach the transacting parties release their keys (referred as secrets) bit by bit.

In this paper, the term Gradual Secret Release approach or GSR is used in a much generalized context. The term '*secret'* refers to the expected message; not specifically the keys only. Accordingly, here GSR Protocol is defined as a protocol in which transacting parties gradually disclose the expected messages step by step. Though the number of GSR protocols in published literatures is considerably less than the number of protocols with TTP, there are some GSR protocols [1], [2], [5], [21] for signing contract or trading the goods.

V. MODEL TO DEVELOP GSR FAIR EXCHANGE PROTOCOLS FOR E-LEARNING

In the scenario of E-transaction an E-learning protocol should hold fairness in true sense and in addition to that it should hold *money atomicity* and *correctness of the course* properties. Involving Student (S), Institute (I), Student's Bank (SB) and Institute's Bank (IB) as transacting parties, here a methodology is proposed to develop a GSR Fair Exchange Protocol for E-learning. The model naturally does not involve an additional TTP. Method for developing a GSR Fair Exchange Protocol for E-learning includes four building blocks viz. *Building Assumption*, *Placing Course Requisition*, *Paying Fees* and *Delivering Course*. Here the paradigms of different building blocks are being presented.

Building Assumption: Building the assumptions regarding technical infrastructure to of the protocol such as:

a. The institute hosts its digital course, encrypted with a key in the form of [c, K_1] along with all of its details, like, fees, terms and conditions, detailed structure of the course etc. in its own website so that the students can download it.
b. It is assumed that the student has an account with the student's bank and the institute has an account with the institute's bank. It is also assumed that the corresponding banks behave rationally by maintaining all type of confidentiality of their account holders for the business. Here the Banks are being used for financial transactions only.
c. It is assumed that the key distribution scheme for the proposed protocol is secure and identity of any party can not be revealed only by the IP address. It is also assumed that, the scheme of encryptions is strong enough to provide the integrity of messages and signatures and it is same for all transacting parties.
d. It is assumed that each party keeps a copy of each message, s/he is sending and the technical infrastructure is strong enough to handle the communication requirements for the message exchanges in the protocol and is fail-safe to handle the log records corruption in any site.
e. The fixed period for time-out is known to all concern parties.

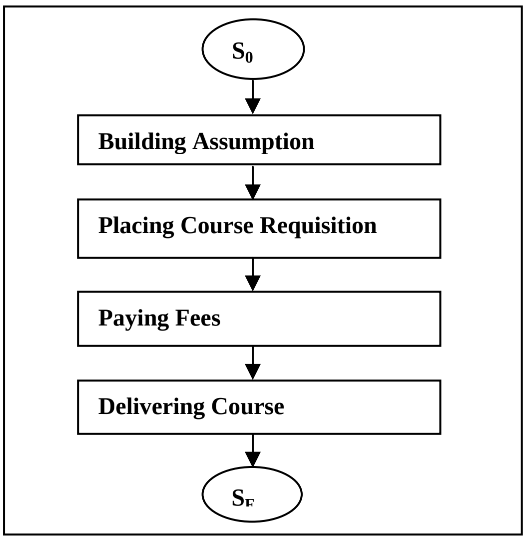

Figure 1: Model to develop GSR Fair Exchange protocols for E-learning

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Placing Course Requisition: This includes both the placing of requisition for the digital course (*c*) by student and accepting the requisition by the institute. The method includes the following activities:

a) Student has to prepare a Course Requisition and place it to Institute.
b) Institute has to encrypt the product taking the asymmetric encryption mechanism 'Theory of Cross Validation', and has to accept the requisition.

Paying the Fees: In this module both the student's bank and Institute's bank have to be used for financial transaction. We outline the activities of this module as follows:

a) Student has to issue the MTI to his/her bank mentioning the institute's account information.
b) The student's bank has to prepare pay-order and directly send to the institute's account in institute's bank.
c) Student and Institute have to get the payment information from their respective banks, beside their own transaction.

Delivering Courses: This module includes two major activities; the delivery of the digital course and the acceptance of delivery. The activities can be outlined as follows:

a) Institute has to prepare a message to send the decryption key taking theory of cross validation as encryption mechanism.
b) Decrypting the digital course student has to send the acceptance message.

Starting from the initial state, say S_0, and ending at final state, say S_F, each of the above activities will lead the system through fair states, making the GSR protocol fair in true sense as a whole.

A GSR Fair Exchange protocols for E-learning on demand: The protocol starts when the student (S) enters into the website of the Institute (I) to have the details of the course and being satisfied with the course decides to subscribe it. After that the protocol may be described as follows:

1) I → S: [c, K_1], I_{ipub}; */*S selects a product c from I's website*/*

2) S → I: CR [CC(CR), I_{iprv}] [S_{ipub}, I_{ipub}]; */*S places the Course Requisition to I*/*

3) I → S: [*Abort*, I_{iprv}]; */* I aborts*/*
Or
I → S: [CC(CR), I_{iprv}] [c.r, $K_1 x K_2$] [CC([c.r, $K_1 x K_2$]), I_{iprv}] [r,K_1] [CC([r, K_1]), I_{iprv}] [I_{acct}, IB_{pub}] [CC([I_{acct}, IB_{pub}]), I_{iprv}] [CC(S_{ipub}), I_{iprv}];
*/*Accepting the Course Requisition, I sends encrypted product and account information including student's public key encrypted with institute's private key*/*

4) S → SB: [[MTI, S_{prv}], SB_{pub}]; */* S instructs SB to prepare pay-order and to send it to IB*/*

5) SB → IB: [[P,B_{sprv}],IB_{pub}]; */*SB sends the pay-order to IB*/*
Or
SB → S: [*Failure*, S_{pub}]; */*SB fails to send pay-order and informs S*/*

6) SB → S: [P,SB_{prv}]; */*SB sends a copy of payment details to S*/*

7) S → I: [P, I_{ipub}]; */*S forwards the copy of payment details to I*/*
Or
S → I: [*Abort*, S_{iprv}]; */*S aborts if message 5 is failure message*/*

8) IB → SB: [*ack*, IB_{prv}]; */*IB sends acknowledgement of payment-clearance to SB*/*

9) IB → I: [*ack*, IB_{prv}]; */*IB sends copy of acknowledgement of payment-clearance to I*/*

10) I → IB: [*rcpt(ack)*, I_{prv}]; */*I sends a receipt of acknowledgement to IB*/*

11) SB → S: [[*ack*, IB_{prv}], SB_{prv}]; */*SB forwards a copy of acknowledgement of payment-clearance to S*/*

12) S → SB: [*rcpt(ack)*, S_{prv}]; */*S sends a receipt of acknowledgement to SB*/*

13) I → S: [K_2^{-1}, S_{ipub}] [CC(K_2^{-1}), I_{iprv}] [r^{-1}, S_{ipub}] [CC([r^{-1}), I_{iprv}]; */*I sends decryption key to S*/*

14) S → I: [*rcpt*, S_{iprv}]; */*S sends receipt of decryption key to I*/*

15) I → S; [[*final_accept*, [*ack*, IB_{prv}]], I_{iprv}]; */*I sends final acceptance and payment receipt to S*/*

Analysis of the Properties: As designed our proposed protocol is not using any third party not even in offline mode. It uses gradual secret release technique to provide the *fairness in true sense* without offering any advantage to either the customer or the merchant. The protocol holds a property, by which the *correctness of course* is being ensured to the customer. The protocol also provides the *money atomicity* property. Here we propose that the protocol holds the above said properties.

Fairness: Regarding this property in this protocol a practical form of *fairness* has been defined above, namely, *fairness in true sense*. We have to show that, neither party, participating in the protocol can gain an advantage by misbehaving during a transaction. Let us consider the contradiction, i.e. some parties can gain advantages within the scope of protocol. To disprove this let us consider the following cases:

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Case1: Let the institute misbehaves by denying the receipt of payment. But, in this protocol the student (S) is getting the information from his/her bank that the exact payment has been sent to the institue's account through message 6. Again, by message 11 s/he (S) is getting signed copy of the acknowledgement from his/her bank (SB) regarding the encashment of the payment into institute's account, signed by institute's bank (IB), which student's bank (SB) is getting from institute's bank (IB) through message 8. So the student (S) have two important documents, viz, [[*ack*, IB_{prv}], SB_{prv}] & [P,SB_{pub}], which can legally prove that s/he has done the payment to institute's account in institute's bank.
These facts lead to a situation where institute (I) is not in an advantage such that s/he can deny the receipt of payment.

Case2: Let the student intends to subscribe the course and misbehaves by denying the payment. But, as described in the protocol the student (S) is issuing the payment instruction to his/her bank (SB) and the bank is sending the payment to institute's bank, not to the institute. The student receives only the copy of a payment details form his/her bank. So, if the student intends to subscribe a course s/he has to instruct his/her bank to pay and the payment is getting credited in institute' account in institute's bank directly.
These facts show that it is not possible to deny the payment by the student if s/he intends to subscribe a course.

Case 3: Let the student does not receive the correct course but the institute gets the correct payment. But, as described in the protocol the student initially downloads [c,K_1] from the institute's website. Before paying for the course, the student also receives a copy of encrypted course from the institute in the form of [cr,K_1 x K_2], [r,K_1], where c.r is the product of c and r. The student multiplies [c,K_1] with [r,K_1] and the resulting product is compared with [cr,K_1 x K_2]. If both a match, then only the student instructs his/her bank to prepare the pay-order and send it to institute's account in institute's bank.
Thus within the scope of this protocol this is not possible that the institute gets the correct payment but the student does not receive the correct course.

Case 4: Let the institute does not receive the correct payment but the student gets the correct course. This is only possible if the protocol allows the student to receive the course before paying for it. But, in this protocol institute sends the course in encrypted form through message exchange 3. To have the actual course the student must have the decryption key, which is provided by the institute by the message exchange 13. In between the student instructs his/her bank to prepare the pay-order and send it to institute's account in institute's bank. Then the student's bank sends the pay-order directly to the student's account. After having an acknowledgement that the exact payment has been credited to its account the institute sends the decryption key to the student by message exchange 13. This shows that this not possible in this protocol such that the institute does not receive the correct payment but the student gets the correct course.

Thus the above four cases contradicts that some parties can gain advantages within the scope of protocol. Hence, by Involution Law of propositional logic, the protocol satisfies the *fairness* property.

***Correctness of course*:** As described in the protocol the student initially downloads [c,K_1] from the institute's website. Before paying for the course demanded, the student also receives a copy of encrypted course from the institute in the form of [cr,K_1 x K_2], [r,K_1], where c.r is the product of c and r. The customer multiplies [c,K_1] with [r,K_1] and the resulting product is compared with [cr,K_1 x K_2]. For any two messages m , $m_c < n_1, n_2$, [m, K_1 x K_2] $\equiv$ [m_c, K_1] mod n_1 iff m= m_c and [m, K_1 x K_2] $\equiv$ [m_c, K_2] mod n_2 iff m= m_c. If both match in the above said comparison, the student is confident that the course s/he is about to receive from the institute, is the same as the course s/he demanded, before paying for a course. Hence the protocol satisfies the *correctness of the product* property.

Money Atomicity: To show that the proposed protocol satisfies the Money Atomicity property, we have to show that, within the scope protocol the pay-order is neither created nor destroyed during the execution of the protocol.
To do so, let us consider the contradiction, i.e. the pay-order can be created or destroyed during the execution of the protocol. To disprove this let us consider the following cases:

Case1: Let the pay-order can be created in two different ways, viz., using the same pay-order to get credited in the institute's account for multiple times by the institute and using the same pay-order to get multiple courses by student respectively. Both the cases are the pay-order is being replayed. But as described in the protocol, a nonce value is used within the pay-order to forestall these replays. Also in the protocol, the pay-order prepared by the student's bank against the instruction of the student and is being sent to the institute's bank for crediting the specified amount to the institute's account. The institute receives only copy of payment details and the pay-order is directly received by the institute's bank from the student's bank. Neither the student nor the institute gets the pay-order directly in their hand. Thus the pay-order can not be created within the scope protocol.

Case 2: Let the pay-order can be destroyed in two different ways, viz., not using the pay-order by the institute to get credited in the institute's account or by loosing the pay-order by the institute before getting it credited. But as described in the protocol, the student instructs his/her bank to prepare the pay-order and send it to the institute's bank for crediting the specified amount to the institute's account. The institute receives only copy of payment details from the student and the pay-order is directly received by the institute's bank from the student's bank. So, there is no scope that the pay-order can be destroyed.

Thus the above two cases contradict that the pay-order can be created or destroyed during the execution of the protocol. Hence, by Involution Law of propositional logic, the protocol satisfies *the money atomicity* property.

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

VI. CONCLUSIONS

In the current scenario of E-learning *fair exchange* is one of the pertinent issues and it is to be addressed by all type of E-learning protocol. Along with the *fairness*, one of the important objectives E-learning protocols is to ensure *money atomicity* and *correctness of course* property within the scope of protocol. Majority of the protocols proposed in the literature rely on trusted third party to provide the said properties. Whether the protocol is offline or online, the cost to maintain the trusted third party is a major concern in the implementation. Keeping these in our mind, in this paper we proposed a GSR Fair Exchange Protocol for E-learning on demand that ensures *fairness* in true sense without using an additional trusted third party. The properties of the protocol also include *money atomicity*, *correctness of the course*. Here, we provided a detailed analysis of the properties.

To the best of our knowledge there is no other E-learning protocol which offers all these properties without using an third party. However, in future a lot of improvement remains to be done. We plan to check the feasibility of operation of this protocol in conjunction with other protocol. We also plan to study the performance of the protocol by applying different load of transaction, which will help to optimize the protocol. We believe our work in this paper will extend the area of applicability of Fair Exchange protocol in E-transaction and strengthen the GSR approach to develop the Fair Exchange protocol so that people can participate in such transaction with more assurance.

References

[1] S. Even, O. Goldreich, A. Lempel, "*A randomized protocol for signing contracts*", Communications of the ACM 28 (6) pp.637-647, June, 1985.

[2] M.Bulm "*How to exchange (secrete) keys*", ACM Transactions on Computer Systems, 1, pp. 175-193, 1993.

[3] R.H. Deng, L. Gong, A.A. Lazar, W. Wang, "*Practical protocols for certified electronic mail*", Journal of Network and System Management, Vol. 4 (3), pp. 279-297, 1996.

[4] Jianying Zhou and Dieter Gollmann. "*A Fair Non-repudiation Protocol*". Proceedings of 1996 IEEE Symposium on Security and Privacy, pp. 55-61, Oakland, USA, May 1996.

[5] T.W. Sandholm, V.R. Lesser, "*Advantages of a leveled commitment contracting protocol*", Proc. Of 13th National Conference on Artificial Intelligence, Portland or The MIT Press, Massachusetts, , pp. 126-133, 1996.

[6] M.K. Franklin, M.K. Reiter, "*Fair exchange with a semi-trusted third party"*, Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, Association for Computing Machinery, New York, , pp. 1-6, April, 1997.

[7] N. Asokan, Victor Shoup, and Michael Waidner. "*Asynchronous Protocols for Optimistic Fair Exchange*". Proceedings of 1998 IEEE Symposium on Security and Privacy, pp. 86-99, Oakland, USA, May 1998.

[8] Olivier Markowitch and Steve Kremer. "*A Multi-party Optimistic Non-repudiation Protocol*". Lecture Notes in Computer Science 2015, Proceedings of 3rd International Conference on Information Security and Cryptology, pp. 109 - 122, Seoul, Korea, December 2000.

[9] Jianying Zhou. "*Non-repudiation in Electronic Commerce*". ISBN 1-58053-247-0, Computer Security Series, Artech House, 2001.

[10] Olivier Markowitch and Shahrokh Saeednia. "*Optimistic Fair Exchange with Transparent Signature Recovery*". Lecture Notes in Computer Science 2339, Proceedings of 2001 Financial Cryptography, pp. 339-350, Grand Cayman, Cayman Islands, February 2001.

[11] Indrakshi Ray and Indrajit Ray. "An Anonymous Fair-Exchange E-Commerce Protocol." *Proceedings of the First International Workshop on Internet Computing and E-Commerce*, *San Francisco, CA*, *April*, 2001. http://www.cs.colostate.edu/~iray/research/icec01.pdf.

[12] Steve Kremer and Jean-Francois Raskin. "*A Game-based Verification of Non-repudiation and Fair Exchange Protocols*". Lecture Notes in Computer Science 2154, Proceedings of 12th International Conference on Concurrency Theory, pp. 551-565, Aalborg, Denmark, August 2001. [44]

[13] Olivier Markowitch and Steve Kremer. "*An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party*". Lecture Notes in Computer Science 2200, Proceedings of 2001 International Conference on Information Security, pp. 363-378, Malaga, Spain, October 2001.

[14] Nicolas Gonzalez-Deleito and Olivier Markowitch. "*An Optimistic Multi-party Fair Exchange Protocol with Reduced Trust Requirements*". Lecture Notes in Computer Science 2288, Proceedings of 4th International Conference on Information Security and Cryptology, pp. 256-267, Seoul, Korea, December 2001.

[15] Steve Kremer, Olivier Markowitch, and Jianying Zhou. "*An Intensive Survey of Fair Non-repudiation Protocols*". Computer Communications, 25(17): pp. 1606-1621, November 2002.

[16] Silvio Micali. "*Simple and Fast Optimistic Protocols for Fair Electronic Exchange*". Proceedings of 2003 ACM Symposium on Principles of Distributed Computing, pp. 12-19, Boston, USA, July 2003.

[17] Q. Zhang, K. Mayes and K. Markantonakis. "*A Practical E-Payment Protocol To Realize Fair-Exchange*". http://www.scc.rhul.ac.uk/public/QZKMKEM%201.pdf, 2004.

[18] Guilin Wang. "*Generic Fair Non-repudiation Protocols with Transparent Off-line TTP*". Proceedings of 4th International Workshop for Applied PKI, pp. 51-65, Singapore, September 2005.

[19] Jianying Zhou, Feng Bao, and Robert Deng. "*Minimizing TTP's Involvement in Signature Validation*". International Journal of Information Security, Vol 5 pp. 37-47, May, 2005.

[20] Indrajit Ray, Indrakshi Ray, and N. Natarajan. "*An Anonymous and Faliure Resilient Fair-exchange E-commerce Protocol*". Decision Support Systems, 39(2005): pp. 267-292, 2005.

[21] Huaping Li et. al: "*Fair E-Commerce Protocols without a Third Party"* Proceedings of ISCC (IEEE) 2006, pp. 324-327, 2006.

[22] Alaraj. A, Munro. M: "*An e-Commerce fair exchange protocol for exchanging digital products and payments*" ICDIM (IEEE) 2007, Vol. 1, Issue 28-31, pp. 248 – 253, October, 2007.

[23] Yusuke Okada et. al.: "*An optimistic fair exchange protocol and its security in the universal composability framework*" International Journal of Applied Cryptography 2008 - Vol. 1, No.1, pp. 70 – 77, 2008.

[24] Dae Hyun Yum and Pil Joong Lee: "*Efficient Fair Exchange from Identity-Based Signature*" IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 2008 E91-A(1): pp. 119-126, 2008.

[25] Xuan Yang, et.al. "*Chameleon-Based Optimistic Fair Exchange Protocol*" Proceedings of International Conference on Embedded Software and Systems, 2008, pp. 298-302, 2008.

[26] Gartner, F.C., Pagnia, H, Vogt, H, *"Approaching a Formal Definition of Fairness in Electronics Commerce"*, Procd. Of 18th IEEE Symposium on Reliable Distributed System, 1999, pp. 354 – 359.

ISBN: 978-988-19251-1-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)