A Survey on Optimistic Fair Digital Signature Exchange Protocols

Alfin Abraham
Department of Computer Science and Engineering
Karunya University
Coimbatore, Tamil Nadu, India

Vinodh Ewards
Department of Computer Science and Engineering
Karunya University
Coimbatore, Tamil Nadu, India

Harlay Maria Mathew
Department of Computer Science and Engineering
Karunya University
Coimbatore, Tamil Nadu, India

Abstract—Security services become crucial to many applications such as e-commerce payment protocols, electronic contract signing, and certified e-mail delivery, with the phenomenal growth of the Internet and open networks. For these applications fair exchange must be assured. A fair protocol allows two parties to exchange digital signatures over the Internet in a fair way, so that either each party gets the other's signature, or neither party does. This paper, gives a survey on the most important fair and optimistic digital signature exchange protocols. Optimistic, means the third trusted party (TTP) is involved only in the situations where one party is cheating or the communication channel is interrupted, i.e., TTP is off-line. As more business is conducted over the Internet, the fair-exchange problem is gaining greater importance. This paper also provides an analysis of basic features, security, and efficiency of digital signature exchange protocols.

Keywords-Fair-exchange protocols; e-commerce; digital signatures; security.

I. INTRODUCTION

As more business is conducted over the Internet, e-commerce transactions have become a major part of our economy. In such transactions, ensuring fairness is critical if the participants are to be protected from fraud. For example, suppose player A is willing to give an electronic check to player B in exchange for an electronic airline ticket. The problem is this: how can A and B exchange these items so that either each player gets the other's item, or neither player does. Both electronic checks and electronic airline tickets are implemented as digital signatures.

Furthermore, applications such as payment protocols via electronic money [11], [15], electronic contract signing [4], [6], and certified e-mail delivery [3], [5] require that fair exchange be assured. Therefore, it seems fruitful to focus our attention on the fair exchange of digital signatures. Of course, one could use an on-line trusted third party in every transaction to act as a mediator: each player sends his item to the third party, who upon verifying the correctness of both items, forwards the item to the other player. This is a rather straightforward solution.

It is more appealing and practical when the digital signature is exchanged in a fair way with off-line TTP. Because those protocols are optimistic in the sense that the TTP is not invoked in the execution of exchange unless one of the two parties misbehaves or the communication channel is out of order.

II. LITERATURE SURVEY

Optimistic fair exchange protocol uses a trusted third party, but only in a very limited fashion: the third party is only needed in cases where one player attempts to cheat or simply crashes; therefore, in the vast majority of transactions, the third party will not need to be involved at all. Compared to a protocol using an on-line third party, the optimistic approach greatly reduces the load on the third party, which in turn reduces the cost and insecurity involved in replicating the service in order to maintain availability. A fair protocol allows two parties to exchange digital signatures over the Internet in a fair way, so that either each party gets the other's signature, or neither party does. The commonly used digital signatures to exchange between two parties are RSA, DSS, Schnorr, Fiat-Shamir, GQ, and Ong-Schnorr signatures. Some optimistic protocols for fair exchange could easily leave one player hanging for a long time, without knowing if the exchange was going to complete, and without being able to do anything about it. Not only can this be a great inconvenience, it can also lead to a real loss in the case of time-sensitive data like stock quotes. Actually, fair exchange includes the following different but related issues: contract signing protocols, certified e-mail systems, non-repudiation protocols [7], [12] and e-payment schemes in electronic commerce. Protocols for all these issues have their own merits as well as flaws.

A. Verifiable Escrows Based Protocol [2]

The verifiable escrows based protocol is a fair protocol that allows two players to exchange digital signatures so that either each player gets the other's signature, or neither player does. This protocol [2] ensures timely termination for fair exchange. A trusted third party is needed only in cases where one player crashes or attempts to cheat. Here the trusted third party is used as an "escrow service". The basic idea is that Alice, the initiator, encrypts her signature under the public key of the trusted third party. So Bob, the responder, can have it decrypted by the trusted third party. Together with this escrow scheme a standard "cut-and-choose" interactive proof is used which make it verifiable. In the sense that the player who receives this escrow can verify that it is indeed the escrow of a signature of the desired form with a correct condition attached. This protocol makes use of three sub-protocols: an abort protocol for the initiator, a resolve protocol for the receiver, and a resolve protocol for the initiator. The protocol can also be used to encrypt data for maintaining data integrity while it is exchanged through the internet.

1) *Merits:*Since the TTP is off-line its intervention in the protocol can be reduced. In making use of the trusted third party the players need not sacrifice their privacy. The protocol can accommodate any common signature scheme such as RSA, DSS, Schnorr, Fiat-Shamir, GQ, and Ong-Schnorr signatures, .etc. without modification.

2) *Demerits:*The creator of the encryption has the ability to control the conditions under which the encryption could be decrypted by the TTP. The overheads of computation and communication are usually expensive. In particular, the scheme is inefficient, since expensive cut-and-choose techniques [20] are used to prove the correctness of the encrypted signature. Another drawback is that it requires the participating members to execute considerable amounts of computations during the interactive zero-knowledge proof.

B. Park et al.'s RSA-Based Multisignature Protocol[15]

For e-commerce applications the fair exchange must be assured. In this protocol [15] a method of constructing an efficient fair-exchange protocol by distributing the computation of RSA signatures is described. By using the features of multisignature model, the protocol is constructed that require no zero-knowledge proofs in the exchange protocol, so the computation can be reduced. Only in the protocol setup phase, the use of zero-knowledge proofs is needed. In this approach fairness is ensured by splitting an RSA private key into two parts. The signer holds both parts while the TTP holds just one of the parts.

1) *Merits:*This scheme uses multisignatures that are compatible with the underlying standard signature scheme, which makes it possible to readily integrate the fair-exchange feature with existing e-commerce systems. Zero-knowledge proofs are not used in the exchange protocol, of this approach which significantly increases efficiency.

2) *Demerits:*This protocol is insecure, because an honest-but-curious TTP can easily derive a user's private key after the end of his/her registration. Dodis and Reyzin [19] had broken this protocol by pointing out this problem. When this protocol is not executed successfully any of the two parties can show the validity of the intermediate results to an outsider. This is an important security requirement for contract-signing, where partial commitments to a contract may be beneficial to a dishonest party or an outsider.

C. Generic Fair Non-Repudiation Protocols with Transparent Off-Line TTP [8]

In non-repudiation service irrefutable evidences need to be generated, exchanged, and validated via computer networks. After the completion of such a transaction, each involved party should obtain the expected items. If any dishonest party denies his/her participation in a specific transaction, others can refute such a claim by providing electronic evidences to a judge. This non-repudiation protocol [8] is a generic fair protocol with transparent off-line TTP. This protocol is exchanges a digital message and an irrefutable receipt between two mistrusting parties over the Internet. At the end of this protocol execution, either both parties obtain their expected items or neither party does, hence it is said to be fair.

1) *Merits:*In this protocol each involved party can independently exploit any secure standard signature scheme to generate non-repudiation evidences that is two involved parties are not required to use the same signature scheme. The generated non-repudiation evidences are the same regardless of whether the TTP is involved or not in the protocol execution. Fairness is achieved at the end of protocol execution, i.e., either the sender Alice obtained the evidence of receipt (EOR) or the receiver Bob got the corresponding message as well as the evidence of origin (EOO), or none of them can get those items.

2) *Demerits:*In this protocol the TTP always stores all the state information in its searching database and the TTP's storage is limited. It is necessary to correctly record whether a protocol instance indexed by a label has been aborted or recovered.

D. Bao et al's Fair Contract Signing Protocol [13]

In contract signing protocol, two mutually distrusted parties exchange their commitments to a contract in a fair way such that either each of them can obtain the other's commitment, or neither of them does. A practical and efficient approach for fair contract signing is using an invisible trusted third party. This contract signing protocol [13] preserves fairness while remaining optimistic in the sense that the trusted party need not be involved in the protocol unless a dispute occurs. The protocol is a generic scheme since any secure digital signature scheme and most of secure encryption algorithms can be used to implement it.

1) *Merits:*Compared with the existing protocols, this protocol is very efficient since only several basic cryptographic operations are required. This protocol have major advantage on fairness over Micali's [9] protocol.

2) *Demerits:*When comparing the security requirement timeliness the schemes in [7] [10] [18] satisfy timeliness by providing both the abort and recovery protocols, this scheme meet only weak timeliness due to the usage of a deadline. But using deadline is an interesting method to achieve stateless TTP.

E. An Abuse-free Fair Contract Signing Protocol Based on the RSA Signature [1]

In any business transaction, to some extent the involved parties do not trust each other. A contract signing is needed in such situations. This protocol [1] allows two parties to sign a digital contract via the Internet in a fair way. A fair contract signing protocol allows two mistrusted parties to exchange their digital signatures to an agreed contract. Here for achieving fairness the private key of the initiator is split into two parts and the TTP hold one part which is kept secret. The initiator holds both parts of the private key. This digital contract signing protocol is based on the RSA signature and it is optimistic since the trusted third party is involved only in the situations where one party is cheating or the communication channel is interrupted. Furthermore, if the protocol is executed unsuccessfully, none of the two parties can show the validity of intermediate results to others. Hence the protocol is abuse-free. The abuse-freeness is guaranteed through a cryptographic primitive, called trapdoor commitment scheme. Abuse-freeness is an important security requirement for contract-signing protocols, especially in the situations where partial commitments to a contract may be beneficial to a dishonest party or an outsider.

1) Merits*:*This protocol provides abuse-freeness which is an important security requirement for contract signing. Under the standard assumption that the RSA problem is intractable [14], [17], the protocol is provably secure in the random hash function model [16]. There is no need to modify the signature scheme or message format to use the protocol in existing systems. Thus, it will be very convenient to integrate the contract-signing protocol into existing software for electronic transactions.

2) Demerits:The overhead of communication becomes larger, since this scheme exploits interactive protocol to prove the validity of partial signature.

III. COMPARISON OF THE REFERENCED PROTOCOLS

The table shows the comparison of basic features, security, and efficiency between the protocols. In the category of basic features, the properties such as transparent TTP or not, off-line or on-line TTP are considered. Here two main security requirements are compared: fairness and timeliness. The protocol which guarantees the two parties involved to obtain or not obtain the other's signature simultaneously is fair. This property implies that even a dishonest party who tries to cheat cannot get an advantage over the other party. At any possible state in the protocol execution, each honest party can complete the protocol unilaterally, i.e., without any cooperation of the other (potentially malicious) party then it provides timeliness. In the efficiency evaluation; the costs of communication is compared.

Some protocol provides timeliness, a protocol provides timeliness if and only if all honest parties always have the ability to reach, in a finite amount of time, a point in the protocol where they can stop the protocol while preserving fairness. Various types of TTP can be considered according to their involvement in the protocol. Online TTP - A TTP involved during each session of the protocol but not during each message's transmission, is said to be online. Off-line TTP - A TTP involved in a protocol only in case of an incorrect behavior of a dishonest entity or in case of a network error, is said to be off-line. Transparent TTP - An off-line TTP producing evidences indistinguishable from the evidences, the parties involved in the contract signing should have exchanged in a faultless case is said to be transparent.

TABLE I. COMPARISON OF BASIC FEATURES, SECURITY AND EFFICIENCY

Parameters	**Protocols**				
	Verifiable Escrows Based Protocol	Park et al.'s RSA-Based Multisignature Protocol	Generic Fair Non-Repudiation Protocols with Transparent Off-Line TTP	Bao et al.'s Fair Contract Signing Protocol	An Abuse-free Fair Contract Signing Protocol Based on the RSA Signature
Fairness	Yes	Yes	Yes	Yes	Yes
Timeliness	Yes	Yes	Yes	Yes (weak)	Yes
Transparent TTP	No	Yes	Yes	Yes	Yes
TTP Involvement	Off-line	Off-line	Off-line	Off-line	Off-line
No: of Messages	4	3	3	3	7
TTP's Statlessness	No	Yes	No	No	Yes

IV. CONCLUSION

The aim of this paper is to give an analysis of fair and optimistic digital signature exchange protocols with off-line TTP. Throughout the paper I surveyed some selected fair and optimistic digital signature exchange protocols. A brief study of the fair optimistic protocols exchanging digital signatures is carried down and the analysis of the basic feature, security and efficiency of the protocols is performed.

REFERENCES

[1] G. Wang, "An abuse-free fair contract signing protocol based on the RSA signature," IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, pp. 158–168, Mar 2010

[2] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 591–606, Apr. 2000.

[3] M. Abadi, N. Glew, B. Horne, and B. Pinkas, "Certified e-mail with a light on-line trusted third party: Design and implementation," in Proc. 2002 Int.World Wide Web Conf. (WWW'02), 2002, pp. 387–395, ACM Press.

[4] G. Ateniese, "Efficient verifiable encryption (and fair exchange) of digital signature," in Proc. ACMConf. Computer and Communications Security (CCS'99), 1999, pp. 138–146, ACM Press.

[5] G. Ateniese and C. Nita-Rotaru, "Stateless-receipient certified e-mail system based on verifiable encryption," in Proc. CT-RSA'02, 2002, vol. 2271, LNCS, pp. 182–199, Springer-Verlag.

[6] F. Bao, R. H. Deng, and W. Mao, "Efficient and practical fair exchange protocols with off-line TTP," in Proc. IEEE Symp. Security and Privacy, 1998, pp. 77–85.

[7] S. Gürgens, C. Rudolph, and H. Vogt, "On the security of fair nonrepudiation protocols," in Proc. ISC'03, 2003, vol. 2851, LNCS, pp. 193–207, Springer-Verlag.

[8] G. Wang, "Generic non-repudiation protocols supporting transparent off-line TTP," J. Comput. Security, vol. 14, no. 5, pp. 441–467, Nov. 2006.

[9] S. Micali, "Simple and fast optimistic protocols for fair electronic exchange," in Proc. PODC'03, 2003, pp. 12–19, ACM Press.

[10] J. Zhou, R. Deng, and F. Bao. Some remarks on a fair exchange protocol. In: Public Key Cryptography (PKC'00), LNCS 1751, pp. 46-57. Springer-Verlag, 2000.

[11] C. Boyd and E. Foo, "Off-line fair payment protocols using convertible signatures," in Proc. ASIACRYPT'98, 1998, vol. 1514, LNCS, pp. 271–285, Springer-Verlag.

[12] S. Kremer, O. Markowitch, and J. Zhou, "An intensive survey of fair non-repudiation protocols," Comput. Commun., vol. 25, no. 17, pp. 1606–1621, Nov. 2002, Elsevier.

[13] F. Bao, G. Wang, J. Zhou, and H. Zhu, "Analysis and improvement of Micali's fair contract signing protocol," in Proc. ACISP'04, 2004, vol. 3108, LNCS, pp. 176–187, Springer-Verlag.

[14] M. Bellare and R. Sandhu, The Security of Practical Two-Party RSA Signature Schemes 2001 [Online]. Available: http://www-cse.ucsd. edu/users/mihir/papers/

[15] J. M. Park, E. Chong, H. J. Siegel, and I. Ray, "Constructing fair exchange protocols for e-commerce via distributed computation of RSA signatures," in Proc. PODC'03, 2003, pp. 172–181, ACM Press.

[16] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proc. 1st ACM Conf. Computer and Communications Security (CCS'93), 1993, pp. 62–73, ACM press.

[17] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[18] O. Markowitch and S. Kremer. An optimistic non-repudiation protocol with transparent trusted third party. In: Information Security Conference (ISC'01), LNCS 2200, pp. 363-378. Springer-Verlag, 2001.

[19] Y. Dodis and L. Reyzin, "Breaking and repairing optimistic fair exchange from PODC 2003," in Proc. ACM Workshop on Digital Rights Management (DRM'03), 2003, pp. 47–54, ACM Press.

[20] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in Proc. CRYPTO'86, 1987, vol. 263, LNCS, pp. 186–194, Springer-Verlag.