An Efficient and Fairness Contract Signing for Network Transaction

[1.]V. R. Arulmozhi, [2.] S. Nagendra Prabhu, [3.]M. Thivya
[1,2,3.]M.E
[1,2.]Department of CSE, R.V.S ETGI, [3.]Department of E&I, R.V.S CET
Dindigul – 624005. Tamilnadu.

***Abstract*— Contract signing plays a very important role in any business transaction, in particular in situations where the involved parties do not trust each other to some extent already. As electronic commerce is becoming more and more important and popular in the world, it is desirable to have a mechanism that allows two parties to sign a digital contract via the Internet. This requirement is essentially captured by the concept of fairness: At the end of the protocol, either both parties have valid signatures for a contract or neither does, even if one of them tries to cheat or the communication channel is out of order. Existing contract protocols without the property of abuse-freeness is a risk for a honest party, as a possible dishonest party maybe does not really want to sign the contract with her, but only use her willingness to sign to get leverage for another contract. And so the existing contract-signing protocols are not abuse-free. This project proposes a new contract-signing protocol for two mutually distrusted parties. This protocol is based on an RSA multi signature, which is formally proved to be secure. This protocol is fair and optimistic. However, different from all previous RSA-based contract-signing protocol, the proposed protocol is further abuse-free. That is, if the contract-signing protocol is executed unsuccessfully, each of the two parties cannot show the validity of intermediate results generated by the other party to outsiders, during or after the procedure where those intermediate results are output.**

Index Terms—Contract signing, cryptographic protocols, digital signatures, e-commerce, fair-exchange, RSA, security

I. INTRODUCTION

An important issue in electronic commerce is how to exchange electronic data between two potentially distrusted parties in an efficient and fair manner. Examples of such exchanges include signing of electronic contracts, certified e-mail delivery and fair purchase of electronic goods over communication networks such as the Internet. As more business is conducted over the Internet, the fair exchange problem assumes increasing importance. 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. Therefore, it seems fruitful to focus our attention on the fair exchange of digital signature. Whenever a message is sent over the Internet, there is no assurance that it will be delivered to the intended recipient. Even if the message has been delivered, the recipient may claim otherwise. This may be unpleasant particularly in today's society where networked computers are increasingly being used to exchange items between distrusted parties. In the real world, some form of simultaneity can be achieved thanks to the physical proximity of the parties involved with an exchange. For instance, two parties can sign a contract simultaneously by holding the contract itself. Contract signing is an important part of any business transaction, in particular in settings where participants do not trust each other to some extent already. A fair contract-signing protocol allows two potentially mistrusted parities to exchange their commitments (i.e., digital signatures) to an agreed contract over the Internet in a fair way, so that either each of them obtains the other's signature, or neither party does.

II. BASIC CONCEPTS:

A. Digital Signature:

A Digital Signature is a digital code which can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. To be effective, digital signatures must be unforgeable.A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message and that the message was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

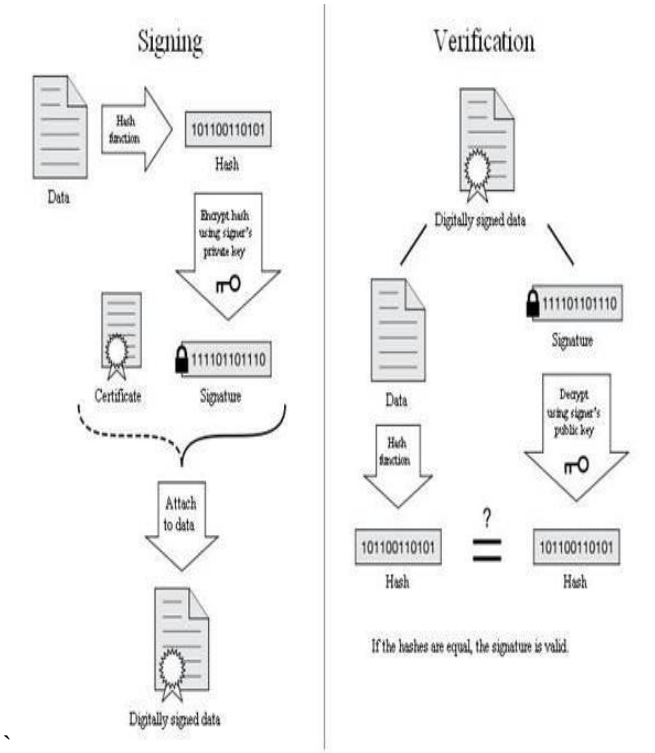


FIG: 1 DIGITAL SIGNATURE

B. RSA Multi signature:

A digital multi signature is a digital signature of a message generated by multiple signers with knowledge of multiple private keys. An efficient RSA multi signature scheme based on Shamir's identity-based signature (IBS) scheme. This is the first efficient RSA-based multi signature scheme with both fixed length and the verification time. The proposed identity-based multi signature scheme is secure against forgerability under chosen -message attack. It is also secure against multi-signer collusion attack and adaptive chosen-ID attack.

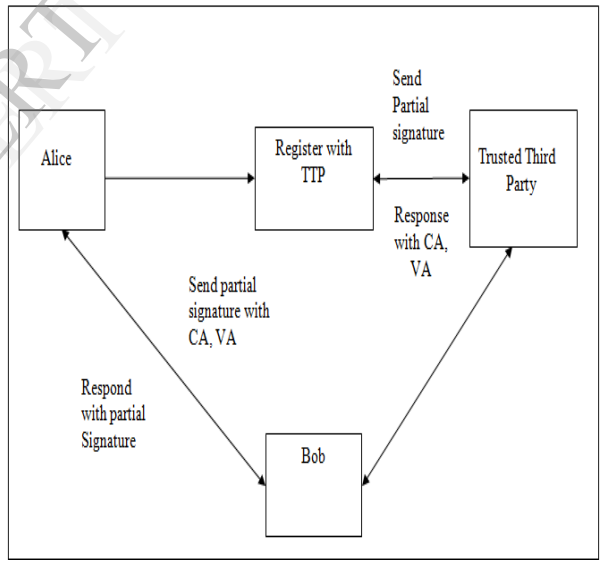
III. BACKGROUNDS

In the existing system, contract signing (i.e., fair exchange of digital signatures) is a fundamental problem in electronic transactions. According to the involvement degree of a trusted third party (TTP), contract-signing protocols can be divided into two types: 1) gradual exchanges without any TTP; 2) protocols with an on-line TTP. Early efforts mainly focused on the first type of protocols to meet computational fairness: Both parties exchange their commitments/secrets "bit-by-bit." If one party stops prematurely, both parties have about the same fraction of the peer's secret, which means that they can complete the contract off-line by investing about the same amount of computing work, e.g., exclusively searching the remaining bits of the secrets. The major advantage of this approach is that no TTP is involved. But at the same time, such protocols are inefficient because the costs of computation and communication are extensive. In an on-line TTP, it is always involved in every exchange. In this scenario, a TTP is essentially a mediator: a) Each party first sends his/her item to the TTP; b) then, the TTP checks the validity of those items; c) if all expected items are correctly received, the TTP finally forwards each item to the party who needs it. Generally speaking, contract-signing protocols with an on-line.

IV. PROPOSED WORK

The proposed system, based on the RSA signature scheme, a new digital contract-signing protocol is proposed. Like the existing RSA-based solutions for the same problem, our protocol is not only fair, but also optimistic, since the trusted third party is involved only in the situations where one party is cheating or the communication channel is interrupted. Furthermore, the proposed protocol satisfies a new property— *abuse-freeness*. The reason is that we integrate an interactive zero-knowledge protocol, proposed for confirming RSA undeniable signatures into our scheme to prove the validity of the intermediate results. Moreover, we exploit trapdoor commitment schemes to enhance this zero-knowledge protocol so that the abuse-freeness property can be fully achieved. That is, if the protocol is executed unsuccessfully, none of the two parties can show the validity of intermediate results to others. In the proposed system, it present the first abuse-free fair contract signing protocol based on the RSA signature, and show that it is both secure and efficient.

A. Block Diagram:



V. REGISTRATION PROTOCOL

The TTP is linked with Alice and Bob by reliable communication channels, i.e., messages inserted into such a channel will be delivered to the recipient after a finite delay. To use our protocol for exchanging digital signatures, only the initiator Alice needs to register with the TTP. That is, Alice is required to get a long-term voucher from the TTP besides obtaining a certificate from a CA. To this end, the following procedures are executed

1) Alice first sets an RSA modulus n=pq , where p and are q two k-bit safe primes, Alice selects her random public key e, and calculates her private key d , Finally, Alice registers her

public key with a CA to get her certificate , which binds her identity and the corresponding pubic key together.
2) Alice randomly splits d into d1 and d2, and computes e1, At the same time, she generates a sample message-signature pair Then, Alice sends to the TTP but keeps secret.
3) The TTP first checks that Alice's certificate is valid. After that, the TTP checks that the triple is prepared correctly. If everything is in order, the TTP stores d2 securely, and creates a voucher Va by computing. That is, is the TTP's signature on message, which guarantees that the TTP can issue a valid partial signature on behalf of Alice by using the secret.

VI. CONTRACT SIGNING

Contract signing plays a very important role in any business transaction, in particular in situations where the involved parties do not trust each other to some extent already. In the paper-based scenario, contract signing is truly simple due to the existence of "simultaneity." That is, both parties generally sign two hard copies of the same contract at the same place and at the same time. After that, each party keeps one copy as a legal document that shows both of them have committed to the contract. If one party does not abide by the contract, the other party could provide the signed contract to a judge in court. As electronic commerce is becoming more and more important and popular in the world, it is desirable to have a mechanism that allows two parties to sign a digital contract via the Internet. However, the problem of contract signing becomes difficult in this setting, since there is no simultaneity any more in the scenario of computer networks. In other words, the simultaneity has to be mimicked in order to design a digital contract-signing protocol. This requirement is essentially captured by the concept of fairness: At the end of the protocol, either both parties have valid signatures for a contract or neither does, even if one of them tries to cheat or the communication channel is out of order.

VII. RSA SIGNATUTRE

The proposed system based on the RSA signature. The basic idea is that Alice first splits her private key d into d1and d2 so that d=d1+d2 mod □(n). Then, only d2 is delivered to the TTP, while Alice keeps (d, d1, d2) as secrets. To exchange her signature with Bob, Alice first sends partial signature to Bob, and proves that is prepared correctly in an interactive zero-knowledge way protocol.

VIII. FAIR EXCHANGE

Assume that a contract has been agreed between Alice and Bob before they begin to sign it. In addition, it is supposed that the contract explicitly contains the following information: a predetermined but reasonable deadline, and the identities of Alice, Bob, and the TTP.
1) First, the initiator Alice computes her partial signature, and then sends the triple to the responder Bob. Here, is a cryptographically secure hash function.
2) Upon receiving, Bob first verifies that is CA is Alice's certificate issued by a CA, and that is Alice's voucher created by the TTP. Then, Bob checks if the identities of Alice, Bob, and the TTP are correctly specified as part of the contract. If all those validations hold, Bob initiates the following interactive zero-knowledge protocol with Alice to check whether Alice's valid partial signature on contact is indeed.

a) Bob picks two numbers at random, and sends a challenge to Alice by computing
b) After getting the challenge c, Alice calculates the respondence, and then returns her commitment to Bob by selecting a random number, the commitment algorithm of a secure trapdoor commitment scheme which depends on Bob's public key.
c) When the commitment is received, Bob sends Alice the pair to show that he prepared the challenge C properly
d) Alice checks whether the challenge is indeed prepared correctly, i.e., If the answer is positive, Alice recommit the commitments by revealing the respondence to Bob.

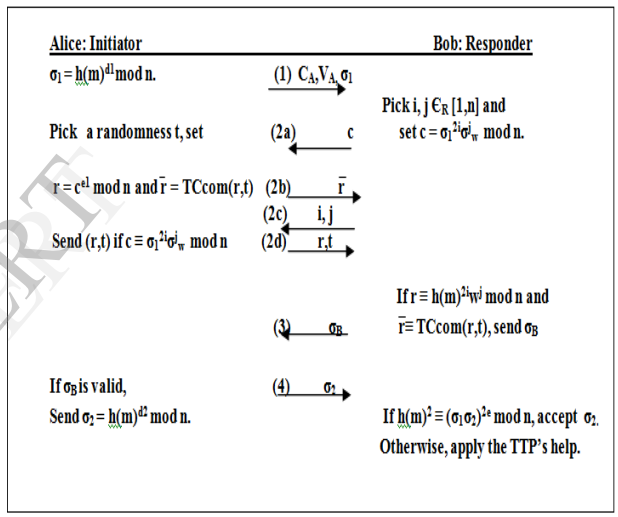


Fig : Signature Exchange Protocol

IX. CONCLUSION

However, different from all previous RSA-based contract-signing protocol, the proposed protocol is further abuse-free. That is, if the contract-signing protocol is executed unsuccessfully, each of the two parties cannot show the validity of intermediate results generated by the other party to outsiders, during or after the procedure where those intermediate results are output. In other words, each party cannot convince an outsider to accept the partial commitments coming from the other party. This is an important security property for contract signing, especially in the situations where partial commitments to a contract may be beneficial to a dishonest party or an outsider. Finally, using the technique of threshold RSA signature, the proposed protocol could be extended for the scenarios where the trust on a single TTP needs to be distributed into multiple TTP's, or a contract is required to be signed only by a given quota of members cooperatively.

X. FUTURE WORK

There are two directions for future research related to this topic: First, it would be nice to find a more efficient method of performing verifiable encryption, because even a less general or less secure, but more efficient method would be interest. Second, the fact that our trusted third party is off-line means that we could afford to implement it as a distributed, fault-tolerant system, making it highly secure using potentially expensive cryptographic techniques, and eliminating the single point of failure.

REFERENCES

[1] 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.

[2] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," in Proc. EUROCRYPT'98, 1998, vol. 1403, LNCS, pp. 591–606, Springer-Verlag.

[3] 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.

[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] 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.

[8] F. Bao, "Colluding attacks to a payment protocol and two signature exchange schemes," in Proc. ASIACRYPT'04, 2004, vol. 3329, LNCS, p. 417–429, Springer-Verlag.

[9] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in Proc. CRYPTO'02, 2002, vol. 2442, LNCS, pp. 354–368, Springer-Verlag.

[10] 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.

[11] 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/.