Fair Contract Signing Protocol Based On Secret Sharing

Rajasree R.S., Sonali Patil
Department Of Computer Engineering
Pimpri Chinchwad College Of Engineering,Nigdi,Pune-44

ABSTRACT

A fair contract signing protocol allows two potentially mistrusted parties to exchange their commitments to an agreed contract over the Internet in a fair way so that either each of them obtains the others signature or neither party does. The existing protocols face the problem of more number of transactions in between TTP and party. Also the time complexity and computational complexities are more. In this paper we are proposing a fair contract signing protocol based on secret sharing scheme. The proposed method satisfies property of abuse freeness and fairness. That is if the protocol is executed unsuccessfully, none of the two parties can show the validity of intermediate results to others. The proposed scheme is more reliable, secure and less complex .

Keywords*:* Contract signing, Secret Sharing, Visual Cryptography

1. Introduction

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. 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. Information is exchanged in computer networks nonsimultaneously, so at least an unfair state must be passed through. From the view point of technique, the problem of digital contract signing belongs to a wider topic: fair exchange. Actually, fair exchange includes the following different but related issues: contract-signing protocols, certified e-mail systems nonrepudiation protocols and e-payment schemes in electronic commerce .In this paper, the problem of digital contract signing between two parties is focused. Since a party’s commitment to a digital contract is usually defined as his/her digital signature on the contract, digital contract signing is essentially implied by fair exchange of digital signatures between two potentially mistrusted parties. There is a rich history of contract signing (i.e., fair exchangeof digital signatures) because this is a fundamental problem in electronic transactions.

2. Existing System

According to the involvement degree of a trusted third party (TTP), contract-signing protocols can be divided into three types: 1) gradual exchanges without any TTP; 2) protocols with an on-line TTP[1]; and 3) protocols with an off-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. However, this approach is unrealistic for most real-world applications due to the following reasons. First of all, it is assumed that the two parties have equivalent or related computation resources. Otherwise, such a protocol is favorable to the party with stronger computing power, who may conditionally force the other party to commit the contract by its own interest. At the same time, such protocols are inefficient because the costs of computation and communication are extensive. In addition, this approach has the unsatisfactory property of uncertain termination. In the second type of fair exchange protocols an on-line TTP is always involved in every exchange. In this scenario 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. Contract-signing protocols with an on-line TTP could be designed more easily since the TTP facilitates the execution of each exchange, but may be still expensive and inefficient because the TTP needs to be paid and must be part of every execution.

2.1 RSA Cryptosystem

Existing system use the RSA crypto system [8]and is now the de facto industrial standard.

Alice sets an RSA modulus n=pq whwre p and q are two safe k bit primes and sets her public key e $Є_R$ $Z^*_{\Phi(n)}$, and calculates her private key

$$d=e^{-1} \bmod \Phi(n) \qquad (1)$$

where modΦ(n) is Euler's totient function. Then, she registers her public key with a certification authority (CA) to get her certificate .After that, Alice randomly splits d into d_1 and d_2 so that $d=d_1+d_2$, where e $Є_R$ $Z^*_{\Phi(n)}$. To get a voucher V_A from a TTP, Alice is required to send
(CA,e_1,d_2)to the TTP, where

$$e_1=d_1^{-1} \bmod \Phi(n) \qquad (2)$$

The voucher is the TTP's signature that implicitly shows two facts:

1)e_1 can be used to verify a partial signature generated by using secret key d_1, and

2) the TTP knows a secret d_2 matches with RSA key pairs (d_1,e_1)and (d,e) .When Alice and Bob want to exchange their signatures on a message m, Alice first computes

$$\mu1=h(m)d1 \bmod n \qquad (3)$$

and sends (CA,VA,μ_1) to Bob, where h(.)is a secure hash function.Upon receiving , Bob checks the validity of CAand VA, and whether $h(m)=\mu_1^{e1}$mod n. If all those verificationsgo through, Bob returns his signature μ_B to Alice, since he is convinced that the expected

$$\mu_2=h(m)^{d2} \bmod n \qquad (4)$$

can be revealed by Bob or the TTP. After receiving valid μ_B Alice reveals $\mu_2=h(m)^{d2}$mod n to Bob. Finally, Bob obtains Alice'signature μ_A for message by setting , $\mu_A= \mu_1\mu_2$since we have
$h(m)Ξ\mu_A^e=h(m)^{(d1+d2)e}=h(m)^{de}$mod n. (5)

The security problem in Park 'sscheme [9]is that an honest-but-curious TTP can easily derive Alice's private key d.The reason is that with the knowledge of (n,e,e_1,d_2), the TTP knows that the integer e-(1-ed $_2$)e $_1$ is a nonzero multiple ofΦ(n). It is well known that knowing such a multiple of Φ(n),Alice's RSA modulus n can be easily factored. Consequently, the TTP can get Alice's private key by the extended Euclidean algorithm.

[5] In rsa based solution is there for fair contract signing ,The protocol is based on an RSA multisignature, which is formally proved to be secure .This protocol is fair and optimistic. Furthermore, different from the above existing schemes,theprotocol is abuse-free.But the existing system does not suit for multi party signature,whwre only a single TTP and two users can exchange their signatures

3 PROPOSED SYSTEM

This paper proposes a new secure method for fair contract signing. The protocol method is based on secret sharing[6], [7].The first step in exchanging the signatures is Registration with the TTP.The following is the registration protocol that register the users with the TTP.

3.1 REGISTRATION PROTOCOL

To use our protocol for exchanging digital signatures,both Alice and Bob has to register with the TTP.

1) Alice and Bob registers their public key with a CA to get their certificate CA
2) Then Both Alice and Bob sends their CA to the TTP to register with the TTP.
3) The TTP first checks that A certificate CA is valid.If the certificates are valid TTP sends a long term voucher V_a to both the users.V_a is TTP,s signature on the contract

The above registration protocol is little bit complicated .But this is to be done only once for a long period of time.

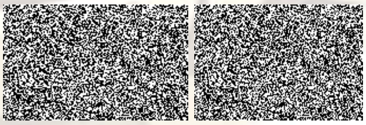
. The parties uses (2, 2) secret sharing [7] for constructng the 2 shares of their signature. The method is divided into 3 steps:

a. Construction of shares of signature
b. Distribution of shares
c. Reconstruction of signature

a. Construction of shares of signature

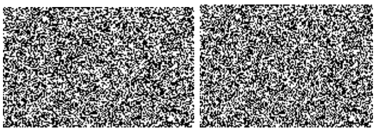
- The original signature image is considered as an input
- Apply the (2, 2) visual cryptography [7] to crate the 2 shares for the signature image.
- Both the parties will create 2 shares of their signatures.

Shares of Bob



share1 (S_B1) share2 (S_B2)

Shares of Alice
s

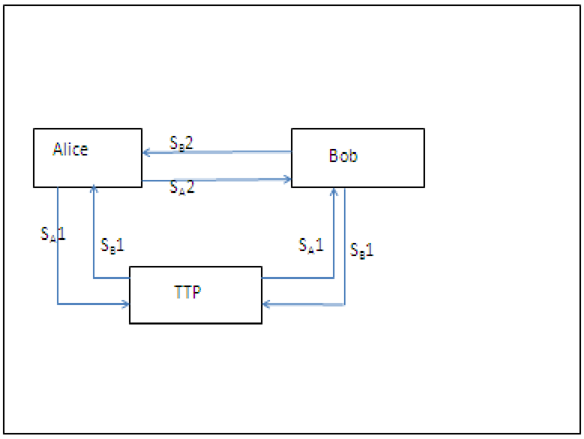


Share 1 (S_A1) Share 2 (S_A2)

b)Distribution of Shares

After the shares are constructed by both the participants the shares are to be distributed each other partialy.A partial share is given to the TTP also inorder to improve security.

DisD



Distribution Of Shares

The above figure shows the distribution of shares After registering with the TTP both Alice and bob exchange their shres by the following steps

1)Alice and Bob first send one of their shares(S_A1,S_B1) to the TTP along with their vouchers(Va,Vb).They keep the other part of their shares (S_A2,S_B2) secret.

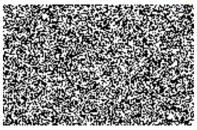
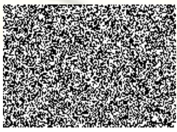
2)TTP then verifies the vouchers and stores their shares

3)Alice then sends the second part of her share(S_A2) to Bob.On receiving the share ,Bob sends the second part of his share(S_B2) to Alice

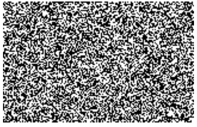
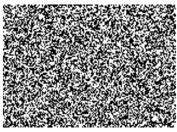
4)Now TTP can send the other part of their shares((S_A1,S_B1) to both Alice and Bob

c. Reconstruction Of Shares

1)On receiving both the shares of Alice,Bob reconstructs the original share from it

 + =ALICE

2)On receiving both the share s of Bob,Alice reconstructs the original secret by stacking 2 shares together.

 + =BOB

Our protocol guarantees the two parities involved to obtain or not obtain the other's signature simultaneously.This property implies that even a dishonest party who tries to cheat cannot get an advantage over the other.

4. Properties

1)Abuse-Freeness

If the whole protocol is not finished successfully,any of the two parties cannot show the validity of the intermediate results generated by the other to an outsider,either during or after the procedure where those intermediate results are produced.

2)Timely Termination:

The execution of a protocol instance will be terminated in a predetermined time. This property is implemented by adding a reasonable deadline in a contract. If one party does not send his/her signature to the other party after the deadline , both of them are free of liability to their partial commitments to the contract and do not need to wait any more.

3) Compatibility:

In our protocol, each party's commitment to a contract is a standard digital signature. This means that to use the protocol in existing systems, there is no need to modify the signature scheme or message forma at all. Thus, it will be very convenient to integrate the contract-signing protocol into existing software for electronic transactions.

4) High Performance:

In a typical implementation, the protocol execution in a normal case requires only interaction of several rounds between two parties, transmission of about one thousand bytes of data, and computation of a few modular exponentiations by each party.

CONCLUSION

The proposed scheme reduces the computational complexities by avoiding the use of complex equations with secret sharing algorithm. The (2, 2) secret sharing algorithm is very simple, less complex and reduces the number of transactions in between TTP and party.

The proposed scheme can be easily extended for n participants using (n, n) secret sharing. Also number of TTPs can be increased.

References

[1] 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

[5] Rajasree R. S., “RSA based solution for fair contracr signing” International Journal of Engineering Research and Technology, Vol. 1, Issue 8.

[6] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[7] M. Naor, A. Shamir, “Visual cryptography”, Proc. Eurocrypt ’94, Lecture Notes Computer Sci., Vol. 950, pp.1-12, 1994.

[8] R.L.Rivest ,A.Shamir and L.Adleman ,”Amethod for obtaining digital signature and public-key cryptosystem”,commun.ACM,vol.21 no.2 ,pp. 120-126,Feb.1978

[9] J.M.Park,E.Chhong ,H.J. Siegel and I.Ray ,”Constructing fair exchange for e-commerce via distributed computation of RSA signatures” in Proc.PODC ,2003 ,pp172-181,ACM press