An Abuse-Free Optimistic Contract Signing Protocol with Multiple TTPs

Alfin Abraham
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. For these applications fair exchange must be assured. A fair protocol allows two members participating in a contract to exchange digital signatures over the Internet in a fair way, so that either each person gets the other's signature, or neither person does. As more business is conducted over the Internet, the fair-exchange problem is gaining greater importance. The property abuse-freeness is necessary for contract signing. Abuse free means, if the protocol is not executed successfully, none of the two members involved in contract signing can show the validity of intermediate results to others. Here a contract-signing protocol in a multiple TTP scenario is described. This digital signature exchange protocol is optimistic, means the third trusted party (TTP) is involved only in the situations where one person is cheating or the communication channel is interrupted, i.e., TTP is off-line.

Keywords

Fair-exchange protocols, e-commerce, digital signatures, security.

1. INTRODUCTION

In electronic transactions the involved parties do not trust each other, hence a contract signing is needed in this situation. The contract signing is simple in the paper based scenerio due to the existence of simultaneity. Two hard copies of the same contract is signined by both person at the same place and at the same time. After that, each one keeps one copy as a legal document that shows both of them have committed to the contract. The other party could provide the signed contract to a judge in court if one party does not abide. Forging a signature is a difficult matter for a false person would need to be present physically to produce it. Instead simultaneity is achieved through the notion of fairness.

Fairness implies that at the end of the signing process either both parties have the counterpart's signature or none of them does. A fair contract signing protocol allows two mistrusted person to exchange their digital signatures to an agreed contract.A digital signature is a protocol that produces the same effect as a real signature. It is a mark that only the sender can make, but other people can easily recognize as belonging to the sender. Just like a real signature, a digital signature is used to confirm agreement to a message. A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures.

2. RELATED WORK

The contract signing i.e., the fair exchange of digital signature is a fundamental problem in electronic transactions. The contract signing protocols are of different type according to the involvement degree of a trusted third party (TTP). Thus contract signing protocol without any TTP, with an on-line TTP and with an off-line TTP are present.

The contract signing protocols with off-line TTP [1], [3], [5], [11] are practical for most applications. These protocols are optimistic in the sense that the TTP is invoked only in the situations where one party is cheating or the communication channel is interrupted. The fair exchange protocols of digital signatures by Bao et al.[5] and Ateniese [3] are constructed from verifiably encrypted signatures, while such protocol proposed by Asokan et al. [1] used verifiable escrows. These protocols are fair and optimistic, but not abuse free. That is, a party can produce verifiable intermediate result to an outsider. However, except the discrete logarithm-based scheme of Garay et al. [2], all other optimistic contract-signing protocols [1], [3], [4], [5], [15] are not abuse-free. The contract signing protocol in [11] the private key (d) is divided into two for achieving fairness and d2 is delivered to a single TTP. This contract signing protocol is fair and optimistic one. Here the signature of the initiator is generated using RSA algorithm. The partial signatures σ1 and σ2 are generated using d1 and d2. The two partial signatures are combined and decrypted using the public key pair to check the source of the message. A trapdoor commitment scheme is used for making the contract signing an abuse free by determining the correctness of the first partial signature of the initiator.

Here the partial private key d2 is delivered only to a single TTP i.e., here a centralized trusted services is present for the security. Unfortunately, this centralization may introduce a single point of failure. Even worse, it is increasingly difficult to protect any single system against the sort of attacks on the Internet. In this paper, architecture for distributing trusted services among a set of TTP's is described.

3. RSA ALGORITHM

The Rivest, Shamir, Adelman (RSA) scheme is an asymmetric cryptosystem [9]. In RSA system all the users must generate their private key pair (d, n) and kept it in secret and store their public key pair (e, n) in Key Distribution Centre (KDC). The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. For public key encryption sender receives the receiver's public key from the KDC and encrypts the message using the receiver's public key. The receiver uses his private key to decrypt the coded message. The private key is known only to the receiver himself.

A method for creating digital signature for the originator of data is to create the signature by encrypting all of the data with the originator's private key and enclosing the signature with the original data. Anyone with the originator's public key can decrypt the signature and compare the decrypted message to the original message. Because only someone with the private key can create the signature, the integrity of the message is verified when the decrypted message matches the original. If an intruder alters the original message during transit, the intruder cannot also create a new valid signature. If an intruder alters the signature during transit, the signature does not verify properly and is invalid.

The digital contract signing protocol described here is based on RSA signature scheme. The members participating in the contract signing generate their own private and public key pair. Encrypt the message using their private key and it is authenticated by decrypting it using the public key.

4. TRAPDOOR COMMITMENTS IN CRYPTOGRAPHY

In cryptography, a zero-knowledge proof or zero-knowledge protocol is an interactive method for one party to prove to another that a statement is true, without revealing anything other than the veracity of the statement. One important field of applications of trapdoor commitments is zero-knowledge proofs. A zero-knowledge proof is a protocol between two parties, in which one tries to convince other that a certain statement is true. One of the uses of zero-knowledge proofs within cryptographic protocols is while maintaining privacy honest behavior is to be enforced. The idea is to force a user to prove that its behavior is correct according to the protocol. Trapdoor commitment schemes have been used to construct zero-knowledge Proofs. Additionally, trapdoor commitments play an important role for the secure signature scheme construction.

In the contract signing to guarantee the abuse-freeness trapdoor commitment scheme is used. In a trapdoor commitment (TC) scheme [8], [11], [13] one trapdoor is created and the owner of this trapdoor can open a commitment in different ways. The owner of the trapdoor can accept the valid answer of the commitment. An outsider cannot distinguish whether this answer is revealed by the sender or forged by the receiver using the trapdoor. Thus the trapdoor commitment schemes helps as to achieve the abuse-freeness property in the contract signing scenario.

5. PROPOSED SCHEME

In this section, a new contract signing scenario is described based on the RSA signature [14] and under the standard assumption the RSA problem is intractable [7], this scenario is provably secure in the random hash function model [10]. Here the basic idea of dividing the private key into d1 and d2 such that d = d1 + d2 mod $\phi(n)$, is used as it is did in [15] and for achieving the abuse free property the trapdoor commitment scheme described in [11] is used. The contract signing protocol described in [2], [15], [11] make use only a single TTP. Hence for these protocols in a single TTP scenario a centralized trust is present.

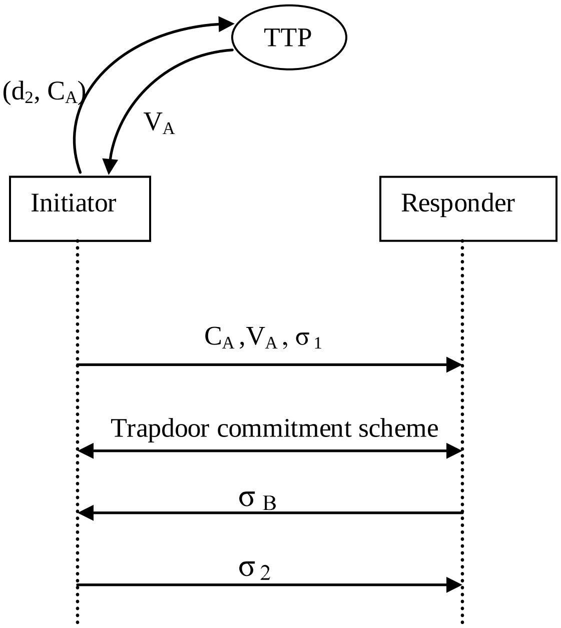

Figure 1. Multiple TTP Scenario

In the single TTP scenario shown in Figure 1 the initiator generate his RSA private and public key pairs. The private key is divided into two and a partial private key d2 is send to a TTP to keep it secret. When the public key registers with a certification authority (CA), the certificate CA which is issued by CA is also send to TTP. After checking CA's validity TTP stores d2 securely and creates a voucher VA which send back to the initiator.

The initiator and the responder exchanges their commitments i.e., their digital signature and the TTP is invoked in the situation where cheating occurs. The members need to communicate with the single TTP for resolving the conflict. The problem is that, a single point of failure may occur in this scenario and it is difficult to protect a single system against the attack.

5.1 Multiple TTP Scenario

The fault tolerance of a single TTP can be established by distributing it among multiple TTP's. Thus, no single TTP has to be trusted completely. The overall system derives its integrity from a majority of correct TTP's

The participants in the multiple TTP scenario consist of n TTP's, indexed 1,…….,n, a trusted dealer and an adversary. Here assumes that all faulty TTP's are controlled by the adversary [6]. Some TTP's are corrupted means they are faulty and the remaining ones are honest. Beginning the adversary select a subset of l TTPs to corrupt. The dealer, here the initiator generates a public key e and a private key d. The private key is divided in to two di and dj like in single TTP scenario as d1 and d2. The dj is further divided into n private key share d j1, d j2…………d jn and the verification keys. The dealer keeps d1 and the remaining private key shares are divided to each TTP.

The private key shares of the corrupted TTP's are obtained by the adversary.

In signature exchange the initiator first exchange his partial signature by encrypting the message using di. For checking the correctness of this partial signature the responder performs a trapdoor commitment scheme. If the signature is correct, the responder sends his signature to the initiator. After checking the correctness of responders signature initiator sends the partial signature obtained by encrypting the message using dj. In case the initiator cheats the responder by giving wrong signature the TTP's are invoked. When giving request for the signature the TTP's outputs a signature share for the given message.

6. CONCLUSION

The aim of this paper is to give an abuse free optimistic contract signing protocol with multiple TTP's. Here the digital signature is based on RSA digital signature scheme and the trust in a single TTP is divided into multiple TTP. Thus this proposed protocol avoids single point of failure. The trapdoor commitment scheme explained in [11] makes this protocol an abuse free one where the abuse freeness is a necessary property in contract signing.

7. REFERENCES

[1] 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.

[2] J. Garay, M. Jakobsson, and P. MacKenzie, "Abuse-free optimistic contract signing," in Proc. CRYPTO'99, 1999, vol. 1666, LNCS, pp. 449–466, Springer-Verlag.

[3] 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.

[4] 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.

[5] 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.

[6] V. Shoup, "Practical threshold signatures," in Proc. EUROCRYPT'00, 2000, vol. 1807, LNCS, pp. 207–220, Springer-Verlag.

[7] 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/

[8] R. Gennaro, "Multi-trapdoor commitments and their applications to proofs of knowledge secure under concurrent man-in-the-middle attacks," in Proc. CRYPTO'04, 2004, vol. 3152, LNCS, pp. 220–236, Springer-Verlag.

[9] Mr.P.Balakumar, Dr.R.Venkatesan, " Biometrics Based File Transmission Using RSA Cryptosystem". (IJCNS) International Journal of Computer and Network Security Vol. 2, No. 4, April 2010.

[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] G. Wang." An Abuse Free Fair Contract Signing Protocol Based on the RSA Signature". In: Proc. of the IEEE Information Forensics and Security vol. 5, march 2010.

[12] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in Proc. CRYPTO'91, vol. 576, LNCS, pp. 129–140, Springer-Verlag, 1991.

[13] M. Fischlin, "Trapdoor Commitment Schemes and Their Applications," PhD. Dissertation, Fachbereich Mathematik, Johann Wolfgang Goethe-University Frankfurt am Main, Frankfurt, Germany, 2001.

[14] 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.

[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.