NVEO
Natural Volatiles &
Essential Oils

Exchange Secure Digital Signatures Using Rsa Algorithms

Dr.C.THIRUMOORTHI

Associate Professor Department of Computer Science Hindusthan College of Arts and Science
Bharathiar University, Coimbatore.

Abstract

This research paper proposes a new contract-signing procedure for two mutually distrusted parties. Our protocol is based on an RSA multi-signature, which is formally proved to be secure. Our protocol is fair and optimistic. Furthermore, different from the above existing schemes, our protocol is abuse-free. The motivation is that we integrate an interactive zero-knowledge procedure, 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. Technical analysis and discussion are provided in detail to show that our scheme is secure and efficient.

Keywords: RSA multi-signature, zero knowledge protocol, Encryption, Decryption, abuse –freeness property.

1. INTRODUCTION

An abuse free fair contract signing protocol, based on the standard RSA signature scheme allows two potentially mistrusted parties to exchange their digital signatures on a contract in an efficient and secure way. Like the existing RSA-based solutions, the new protocol is fair and optimistic, i.e., two parties get or do not get the other's digital signature simultaneously, and the trusted third party is only wanted in abnormal cases that occur rarely. Though, dissimilar from all previous RSA based contract signing procedure, 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.

In additional words, each party cannot satisfy an outsider to accept the incomplete 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. The main aim of this paper is to develop an interface wherein the two parties can interact with the abuse free fair contract signing protocol such that at any point of time they can be free of the held that the other party is cheating them. The contract signing protocol does not give any results until and unless the entire contract is signed by both the parties and no intermediate results are available to both the parties through which they can get benefited by showing them to the third party.

1.2 PROBLEM ANALYSIS

This research work proposes a new contract-signing procedure for two equally distrusted parties. Our protocol is based on an RSA multi-signature, which is formally proved to be secure. Our protocol is fair and optimistic. Furthermore, different from the above existing schemes, our protocol is abuse-free.

Moreover, we exploit trapdoor commitment schemes to enhance this zero-knowledge protocol so that the abuse-freeness property can be fully achieved. Technical analysis and discussion are provided in detail to show that our scheme is secure and efficient.

2. LITREATURE SURVEY

Contract is an agreement where the rules of the game are specified. It allows the mutually suspicious parties to overcome distrust of each other, because their misconduct can be revealed and penalized. Parties can cooperate then with minimal risks. SLA (Service Level Agreement) is a specific type of contract which states the quality of services that has to be maintained. SLAs are decided between a service consumer anda service provider.

No contract or SLA would be of any usage if it is signed. A signed contract is a convincing certificate to an impartial third party that an agreement has actually occurred. In our thesis we define signing as a sequence of transactions the VO service provider and service consumer need to indulge into in order to exchange electronic signatures on the previously agreed SLA.

Electronic signing should not be confused with electronic/digital/cryptographic signatures. The latter can be thought of as an outcome of a signing process. Electronic signatures are based on a public-key infrastructure and involve PKI certificate. The strength of electronic signatures is related to a cryptographic algorithm used. Electronic signatures provide integrity of a message (SLA in our case), non-repudiation evidence and authentication evidence. Electronic/digital signature can be defined as a construct that authenticates both the origin and the contents of a message in a manner that is provable to a disinterested third party

Signing contracts is not a novel phenomenon. In fact, signing and various visual marks associated with it, e.g. signatures and seals, have been around for so long, that they have even acquired a cultural meaning that differs from country to country [PROTO18]. Signing today has essentially the same function as in ancient times with the exception that it has moved to a digital world: contracts have become ‘electronic contracts’ and signing – ‘electronic signing’.

3.METHODOLOGY

3.1 RSA ALGORITHM

The RSA algorithm is used for both public key encryption and digital signatures. It is the most widely used public key encryption algorithm. The basis of the security of the RSA algorithm is that it is mathematically infeasible to factor sufficiently large integers. The RSA algorithm is believed to be secure if its keys have a length of at least 1024-bits.

3.1.1 Digital Signing

In order to sign a message the sender does the following:

1. Produces a hash value of the message
2. Uses his/her private key (n, d) to compute the signature

$$S = M^d \text{ mod n}$$

3. Sends the signature S to the recipient

3.1.2. Signature Verification

The recipient does the following in order to verify the message:

1. Uses the senders public key (n, e) to compute the hash value

$$V = S^e \text{ mod n}$$

2. Extracts the hash value from the message
3. If both hash values are identical then the signature is valid

3.2 KEY GENERATION ALGORITHM

1. Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
2. Compute n = pq and (phi) ϕ = (p-1)(q-1).
3. Choose an integer e, 1 < e < phi, such that gcd(e, phi) = 1.
4. Compute the secret exponent d, 1 < d < phi, such that ed ≡ 1 (mod phi).].
5. The public key is (n, e) and the private key (d, p, q). Keep all the values d, p, q and phi secret. [We prefer sometimes to write the private key as (n, d) because you need the value of n when using d.]

- n is known as the modulus.
- e is known as the public exponent or encryption exponent or just the exponent.
- d is known as the secret exponent or decryption exponent.

3.3 ENCRYPTION

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer m, 1 < m < n Computes the ciphertext c = m^e mod n.
3. Sends the cipher text c to B.

3.3.1.DECRYPTION

1. Uses his private key (n, d) to compute m = c^d mod n.
2. Extracts the plaintext from the message representative m.

3.4 SIGNATURE VERIFICATION

1. Uses sender A's public key (n, e) to compute integer v = s^e mod n.
2. Extracts the message digest from this integer.
3. Independently computes the message digest of the information that has been signed.
4. If both message digests are identical, the signature is valid.

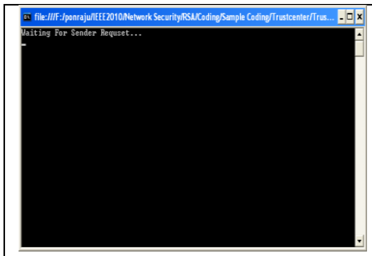
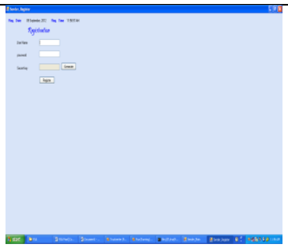
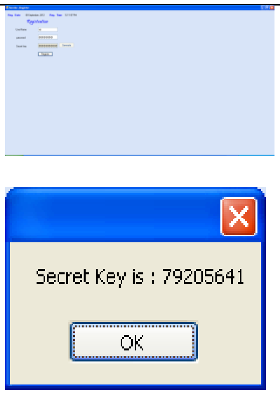
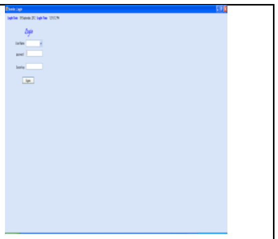
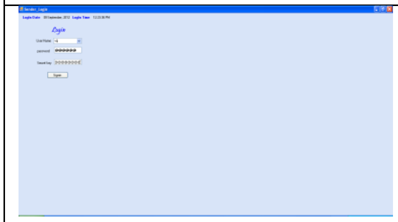
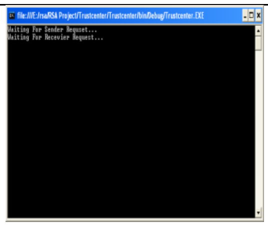
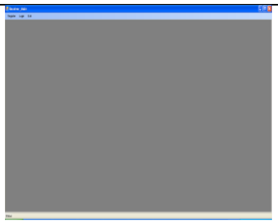
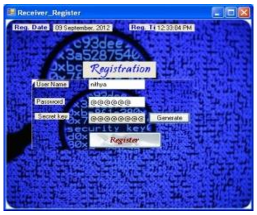
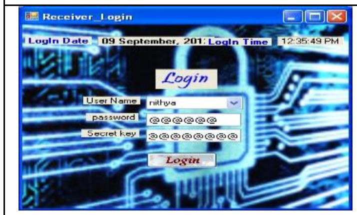
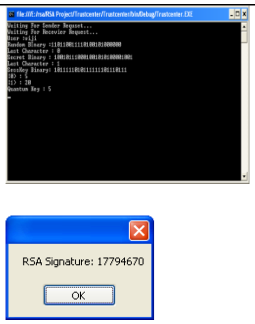
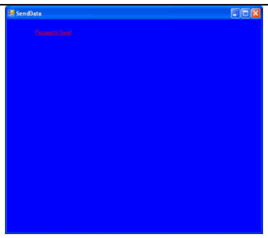
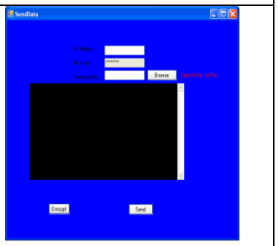
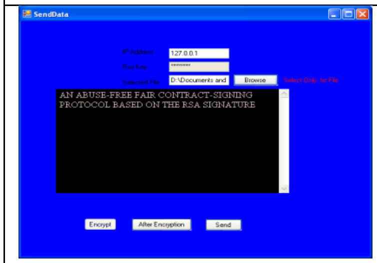
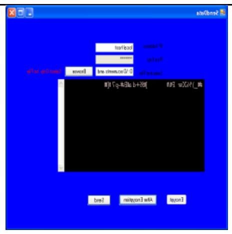
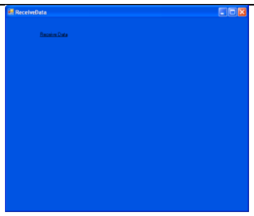
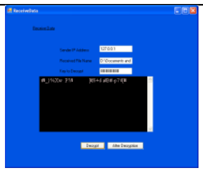
From the view point of technique, the problem of digital contract signing belongs to a wide topic: fair exchange, i.e., how to enable two (or multiple) potentially mistrusted parities exchanging digital items over computer networks in a fair way, so that each party gets the other’s item, or neither party does. Actually, fair exchange includes the following different but related issues: contract signing protocols certified e-mail systems, non-repudiation protocols and repayment schemes in electronic commerce.

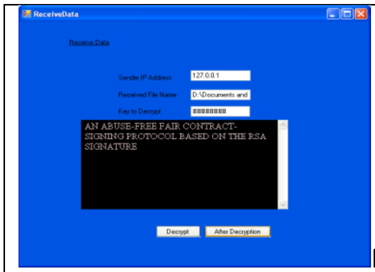
In this paper, we mainlyfocus on the problem of digital contract signing. Since aparty’s commitment to a digital contract is usually defined as his/her digital signature on the contract, digital contract signing is essentially implied by fair exchange of digital signatures between two potentially mistrusted parities. There is a rich history of contract signing (i.e., fair exchange of digital signatures) because this is a fundamental problem in electronic transactions.

4. EXPERIMENT RESULTS

This paper proposes a new contract-signing protocol for two mutually distrusted parties. Our protocol is based on an RSA multi-signature, which is formally proved to be secure. Our protocol is fair and optimistic. Furthermore, different from the above existing schemes, our protocol is abuse-free.

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. Technical analysis and discussion are provided in detail to show that our scheme is secure and efficient.

 file:///F:/ponraju/IEEE2010/Network Security/RSA/Coding/Sample Coding/Trustcenter/Trus... Waiting For Sender Request... Fig 1: Trusted Sender Screen	 Fig 2: Sender Registration Form	 Secret Key is : 79205641 OK Fig 3: Secret Key Generation	 Fig 4: Sender login form
 Fig 5: RSA Key Generation	 file:///E:/rsa/RSA Project/Trustcenter/Trustcenter/bin/Debug/Trustcenter.EXE Waiting For Sender Request... Waiting For Receiver Request... Fig 6: Trusted Sender Waiting for Receiver Request	 Fig 7: Receiver Main Form	 Receiver_Register Reg. Date 09 September, 2012 Reg. Ti 12:33:04 PM Registration User Name nithya Password @@@@@@ Secret key @@@@@@@@ Generate Register Fig 8: Receiver Registration Form
 Receiver_Login Login Date 09 September, 201 Login Time 12:35:49 PM Login User Name nithya password @@@@@@ Secret key @@@@@@@@ Login Fig 9: Receiver Secret Key Generation	 file:///E:/rsa/RSA Project/Trustcenter/Trustcenter/bin/Debug/Trustcenter.EXE Waiting For Sender Request... Waiting For Recevier Request... User :viji Random Binary :11011001111010010100000 Last Character : 0 Secret Binary : 10010111000100101010000100l Last Character : 1 SessKey Binary: 1011111010111111101110111 {0} : 5 {1} : 20 Quantum Key : 5 RSA Signature: 17794670 OK Fig 10: Group Key Generated	 Fig 11: Proceed Data to the Sender Form	 Fig 12: Sending Data Main Form
 SendData IP Address 127.0.0.1 Rsa Key ******** Selected File D:\Documents and Browse Select Only .txt File AN ABUSE-FREE FAIR CONTRACT-SIGNING PROTOCOL BASED ON THE RSA SIGNATURE Encrypt After Encryption Send Fig 13: Enter Data to be send	 Fig 14: Encrypt and send the data	 Fig 15: Receiver Data Form	 Fig 16: Encrypted Data Will be received



Sender IP Address: 127.0.0.1
Received File Name: D:\Documents and
Key to Decrypt: ##########

AN ABUSE-FREE FAIR CONTRACT-SIGNING PROTOCOL BASED ON THE RSA SIGNATURE

Fig 17: Decrypt the Received Data

5. CONCLUSION

In this paper, based on the standard RSA signature scheme, we proposed a new digital contract-signing protocol that allows two potentially mistrusted parties to exchange their digital signatures on a contract in an efficient and secure way. Like the existing RSA-based solutions, the new protocol is fair and optimistic, i.e., two parties get or do not get the other's digital signature simultaneously, and the TTP is only needed in abnormal cases that occur occasionally. 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. Technical details are provided to show that our protocol meets a number of desirable properties, not only those just mentioned.

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] C. Thirumoorthi and T. Karthikeyan, "Easy optimization of image transformation using sFFT algorithm with HALIDE language," 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, 2014, pp. 1188-1190, doi: 10.1109/IC3I.2014.7019723.

[5] C.Thirumoorthi and T. Karthikeyan, "Embedded zero tree Wavelet (EZW) Algorithm based Image Transformation for Easy Optimization with HALIDE Language", International Journal of Applied Engineering Research (IJAER), ISSN 0973-4562 Vol. 10 No.55 (2015) , Page No 1551-1554, June- 2015.

[6] C.Thirumoorthi and T. Karthikeyan, “Medical image compression technique with transform method for lung cancer CT scan image: A Review”, in International Journal of control Theory and Applications (IJCT) (ISSN 0974-5572), International science press, Serials publications, Volume 9, issue 26, pp 193-200, August 2016.

[7] C.Thirumoorthi and T. Karthikeyan, “A novel approach on discrete cosine transform based image compression technique for lung cancer”, Biosciences Biotechnology Research Asia (BBRA), Vol. 13, issue 3, page no: 1679-1688, September 2016. Print ISSN: 0973-1245, Online ISSN: 2456-2602.

[8] C.Thirumoorthi and T. Karthikeyan, “A hybrid medical image compression techniques for lung cancer”, Indian Journal of Science and Technology (IJST) (ISSN (Print):0974-6846 ISSN (Online):0974-5645), Volume 9, Issue 39, pp 1-6, October 2016.

[9] C.Thirumoorthi and T. Karthikeyan, “A study on discrete wavelet transform compression algorithm for medical images”, in Biomedical Research, Allied Academies Journals (ISSN 0970-938X (print) 0976-1683 (Electronic)), Volume 28, Issue 4, page no 1574-1580, February 2017.

[10] 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.

[11] 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.

[12] 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.

[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] F. Bao, “Colluding attacks to a payment protocol and two signature exchange schemes,” in Proc. ASIACRYPT’04, 2004, vol. 3329, LNCS, pp. 417–429, Springer-Verlag.

[15] 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.

[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.