iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VII **Month of publication:** July 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Contract Signing Protocol Based on RSA Signature

Sheetal M Rao[#1], Asst Prof Varsha Vaidya[*2]
[#]*Information Science, VTU*

Abstract— A reasonable contract-marking convention permits two conceivably doubted equalities to trade their responsibilities to a concurred contract over the Internet in a reasonable manner, so that either each of them acquires the other's signature or neither one of the parties does. Taking into account the RSA mark conspire, another advanced contract-marking convention is proposed in this paper. Like the current RSA-based answers for the same issue, the convention is reasonable, as well as idealistic, since the trusted outsider is included just in the circumstances where one gathering is swindling or the correspondence channel is intruded. Besides, the proposed convention fulfills new property ill-use freeness. That is, if the convention is executed unsuccessfully, none of the two gatherings can demonstrate the legitimacy of middle of the road results to others. This misuse free reasonable contract marking convention in view of the RSA mark gives both security and effectiveness.

Keywords— Contract signing, Cryptographic protocols, Digital signatures, e-commerce, Fair-exchange and RSA Security

I. INTRODUCTION

In normal life there are different electronic exchanges workable for the brisk exchange of data from one gathering to other. Amid the trading of data between two gatherings decency between the gatherings is imperative in light of the fact that one gathering can't trust on the other gathering. Thus the arrangement is to assemble an agreement marking convention for the gatherings that needs to trade the data or needs to contract anything

An ill-use free reasonable contract marking convention, in view of the standard RSA mark plan permits two possibly doubted gatherings to trade their advanced marks on an agreement in an effective and secure way. Like the current RSA-based arrangements, the new convention is reasonable and hopeful, i.e., two gatherings get or don't get the other's advanced mark at the same time, and the trusted outsider is just required in anomalous cases that happen at times. Nonetheless, not the same as all past RSA based contract marking convention, the proposed convention is further ill-use free. That is, if the agreement marking convention is executed unsuccessfully, each of the two gatherings can't demonstrate the legitimacy of halfway results created by the other party to outcasts. At the end of the day, every gathering can't persuade a outcast to acknowledge the halfway responsibilities originating from the other party. This is a critical security property for contract marking, particularly in the circumstances where halfway duties to an agreement may be useful to an unscrupulous gathering or an outcast. The primary point of this undertaking is to build up an interface wherein the two gatherings can cooperate with the ill-use free reasonable contract marking convention such that anytime of time they can be free of the prospect that the other party is conning them. The agreement marking convention does not give any outcomes until and unless the whole contract is marked by both the gatherings and no transitional results are accessible to both the gatherings through which they can get profited by revealing to them to the outsider.

The fundamental point of this undertaking is to add to an interface wherein the two gatherings can cooperate with the ill-use free reasonable contract marking convention such that anytime of time they can be free of the prospect that the other party is swindling them. The agreement marking convention does not give any outcomes until and unless the whole contract is marked by both the gatherings and no transitional results are accessible to both the gatherings through which they can get profited by demonstrating to them **to the outsider.**

II. RELATED WORK

From the perspective purpose of strategy, the issue of advanced contract marking fits in with a more extensive topic: fair trade, i.e., how to empower two (or different) possibly doubted equalities trading computerized things over open PC systems like the Internet in a reasonable manner, so that each party gets the other's thing, or neither one of the party does..

There is a rich history of agreement marking (i.e., reasonable trade of advanced marks) in light of the fact that this is an essential issue in electronic exchanges. As per the association degree of a trusted outsider (TTP), contract-marking conventions can be separated into three sorts: 1) slow trades with no TTP; 2) conventions with an on-line TTP; and 3) conventions with a logged off TTP.

Early endeavors fundamentally centered around the first kind of conventions to meet computational reasonableness:

©IJRASET 2015: All Rights are Reserved

Both sides trade their duties/privileged insights "bit-by-bit."If one gathering stops rashly, both sides have about the same division of the peer's mystery, which implies that they can finish the agreement logged off by contributing about the same measure of processing work, e.g., solely looking the remaining bits of the insider facts. The real point of interest of this methodology is that no TTP is included. Then again, this methodology is improbable for most certifiable applications because of the accompanying reasons. Above all else, it is expected that the two gatherings have proportional or related calculation assets. Something else, such a convention is good to the gathering with more grounded registering force, who may conditionally constrain the other party to confer the agreement by its information own advantage. In the meantime, such conventions are wasteful since the expenses of calculation and correspondence are broad. This methodology has the inadmissible property of questionable end. For instance, assume two gatherings are marking a house-deal contract. In the event that the convention stops rashly as an afterthought of the purchaser, the dealer will never make certain whether the purchaser is proceeding with the convention, then again has ended and maybe even has occupied with another house-deal contract-marking convention with another vender. The purchaser may be in a comparative circumstance if the convention ended as an afterthought of the merchant. In the second kind of reasonable trade conventions an on-line TTP is constantly included in every trade. In this situation, a TTP is basically a go between: an) Each gathering first sends his/her thing to the TTP; b) then, the TTP checks the legitimacy of those things; c) if every normal thing are accurately received, the TTP at last advances everything to the gathering who needs it. As a rule, contract-marking conventions with an on-line TTP could be composed all the more effortlessly since the TTP encourages the execution of every trade, except may be still lavish and wasteful since the TTP needs to be paid and must be a piece of each execution (however perhaps not included in every stride). In hone, the on-line TTP is inclined to turn into a bottleneck in the entire framework, particularly in the circumstance where numerous clients depend on a solitary TTP.

Contrasted with the plans having a place with the past two sorts, contract-marking conventions with logged off TTP are additionally engaging and reasonable for most applications since those conventions are hopeful as in the TTP is not conjured in the execution of trade unless one of the two gatherings gets out of hand or the correspondence channel is out of request. Bao et al. [2] and Ateniese [4] built reasonable trade conventions of advanced marks from unquestionably scrambled marks, while Asokan et al. [3], proposed such conventions by utilizing unquestionable escrows. The essential thoughts behind those two cryptographic primitives are comparable, as clarified underneath. To get the advanced mark from the other party, Bob, a gathering, Alice, first scrambles her mark under the TTP's open encryption key, also, demonstrates to Bob that the cipher text undoubtedly relates to her mark, intelligently or no interactively. At that point, Bob sends his advanced mark (or some computerized thing) to Alice. Subsequent to getting the normal thing from Bob, Alice uncovers her mark to Bob. The fact is that if Alice declines to do as such subsequent to getting Bob's thing, the TTP can decode Alice's scrambled mark and sends the outcome to Bob. The distinction between those two sorts of plans is that in the evident escrow-based plans, Alice, the maker of the encryption, can control the conditions under which the encryption could be unscrambled by the TTP. In spite of the fact that their procedures can be connected to an assortment of mark plans, the overheads of processing and correspondence are generally lavish.

III.EXISTING SYSTEM

Contract marking is genuinely basic because of the presence of "concurrence". That is, both sides by and large sign two printed copies of the same contract at the same spot and in the meantime. After that, every gathering keeps one duplicate as an authoritative record that shows them two have focused on the agreement. On the off chance that one gathering does not keep the agreement, the other party could give the marked contract to a Contract marking is genuinely basic because of the presence of "concurrence". That is, both sides by and large sign two printed copies of the same contract at the same spot and in the meantime. After that, every gathering keeps one duplicate as an authoritative record that shows them two have focused on the agreement. On the off chance that one gathering does not keep the agreement, the other party could give the marked contract to a judge in court. As the electronic business is turning out to be more essential and mainstream on the planet, it is attractive to need ajudge in court. As the electronic business is turning out to be more essential and mainstream on the planet, it is attractive to need 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.

IV.PROPOSED SYSTEM

In this Paper primary issue is on the advanced contract marking. Since a party's dedication to a computerized contract is generally characterized as his/her advanced mark on the agreement, computerized contract marking is basically inferred via reasonable trade of computerized marks between two conceivably doubted equalities. There is a rich history of agreement

©IJRASET 2015: All Rights are Reserved

marking (i.e., reasonable trade of computerized marks) in light of the fact that this is a crucial issue in electronic exchanges. In the proposed convention the TTP is disconnected from the net and summoned just if any of the gathering tricks or the correspondence system is out of request. In this protocol the signature exchange part makes use of RSA Trapdoor Commitment schemes to verify the partial signature of Alice.

A. Registration Protocol

To utilize the convention for trading advanced marks, just the initiator Alice needs to enroll with the TTP. To this end, the accompanying techniques are executed.

1) Alice first sets a RSA modulus, where p and q are two k-bit safe primes. At that point, Alice chooses her irregular open key, and figures her private key $d = e^{-1} \bmod \phi(n)$, where $\phi(n) = (p - 1)(q-1)$. At that point Alice enrolls her open key with a CA to get her declaration CA.

2) Alice arbitrarily parts d into d1 and d2 such that d=d1+d2 mod $\phi(n)$ by choosing $d_1 \in_R \mathbb{Z}^*_{\phi(n)}$,she computes $e_1 = d_1^{-1} \bmod \phi(n)$. At the same times she creates an example message mark pair. At that point Alice sends the (C_A, w, σ_w, d_2) to TTP and keeps (d, d_1, d_2, e_1) with her as a mystery.

3) The TTP first watches that Alice's testament CA is legitimate. After that, the TTP watches that the triple is organized adequately. In the event that everything is all together, the TTP stores d2 safely and makes a voucher by processing the VA as by $V_A = \mathrm{Sign}_{TTP}(C_A, w, \sigma_w)$.

To approve the rightness of the triple, the TTP needs to do the accompanying :-

1)To start with, the TTP accepts that **w** is a component of request at minimum of $p'q'$ by checking $w \in \mathbb{Z}_n^* \setminus \{1, -1\}$, and both $\gcd(w-1, n)$,and $\gcd(w+1, n)$ are non prime factors of n.

2) At that point, Alice is obliged to demonstrate that she knows the discrete logarithm бw of to the base **w** through a zero-learning convention intuitively or non intelligently

3) At last, the TTP checks whether $w \equiv (\sigma_w w^{d_2})^e$ .In the event that every one of those acceptances pass, the TTP acknowledges as a substantial triple also, makes the voucher for Alice.

B. Signature Exchange Protocol

1)To start with, the initiator Alice processes her incomplete mark б1=h(m)^d1 mod n and after that sends the triple to the responder Bob.

2) After getting , Bob first confirms that CA is Alice's endorsement issued by a CA and that VA is Alice's voucher made by the TTP. At that point, Bob checks if the characters of Alice, Bob, and the TTP are accurately indicated as a feature of the agreement. On the off chance that each one of those acceptances hold, Bob starts the accompanying intuitive zero-information convention with Alice to check whether б1 Alice's substantial fractional mark on contract is Surely.

a) Bob picks two numbers aimlessly, and sends a test to Alice by computing c=(б1)^2i *(бw)^j mod n

b) Subsequent to getting the test, Alice computes the respondence, and after that profits her dedication to Bob by selecting an irregular number, where TCcom is the responsibility calculation of a safe trapdoor duty plan which relies on upon Bob's open key.

c) When the dedication is gotten, Bob sends Alice the pair to demonstrate that he arranged the test appropriately.

d) Alice checks whether the test is for sure arranged accurately. In the event that the answer is certain, Alice decommits the duty by uncovering the respondence to Bob.

3)After verifying Alice partial Signature б1 bob sends his signature бB on contract to Alice. After receiving бB from Bob ,Alice verifies whether бB is Bob's valid signature .If its true then sends her б2 .

4) After receiving б2 value from Alice ,Bob verifies that h(m)^2=(б1б2)^2e mod n. is true bob verifies б2 as valid and Alice as true on the contract and the contract is signed successfully between Alice and Bob .

©IJRASET 2015: All Rights are Reserved

Volume 3 Issue VII, July 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

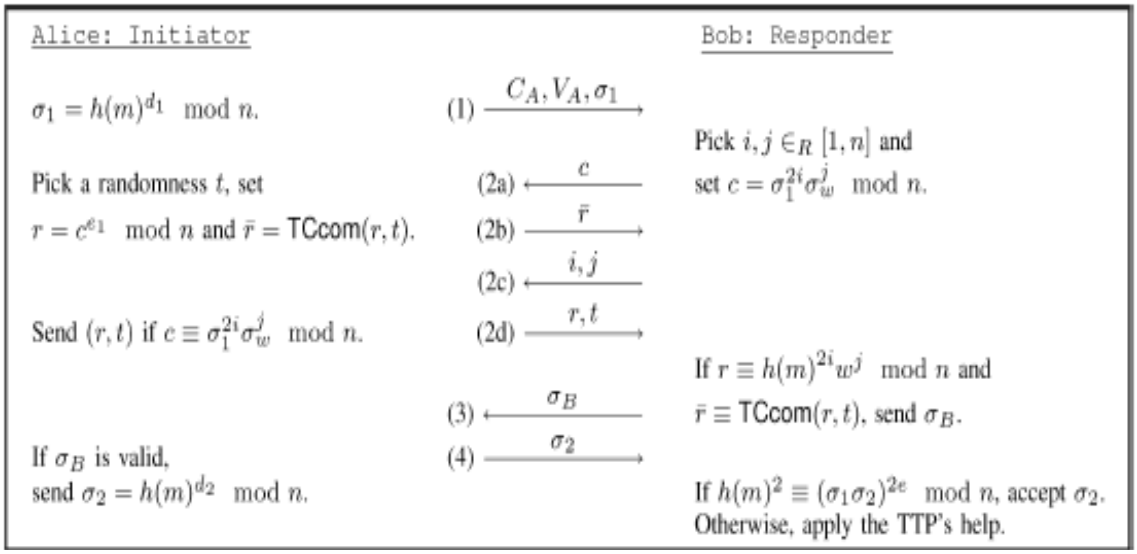


Fig 4.2 Signature Exchange Protocol

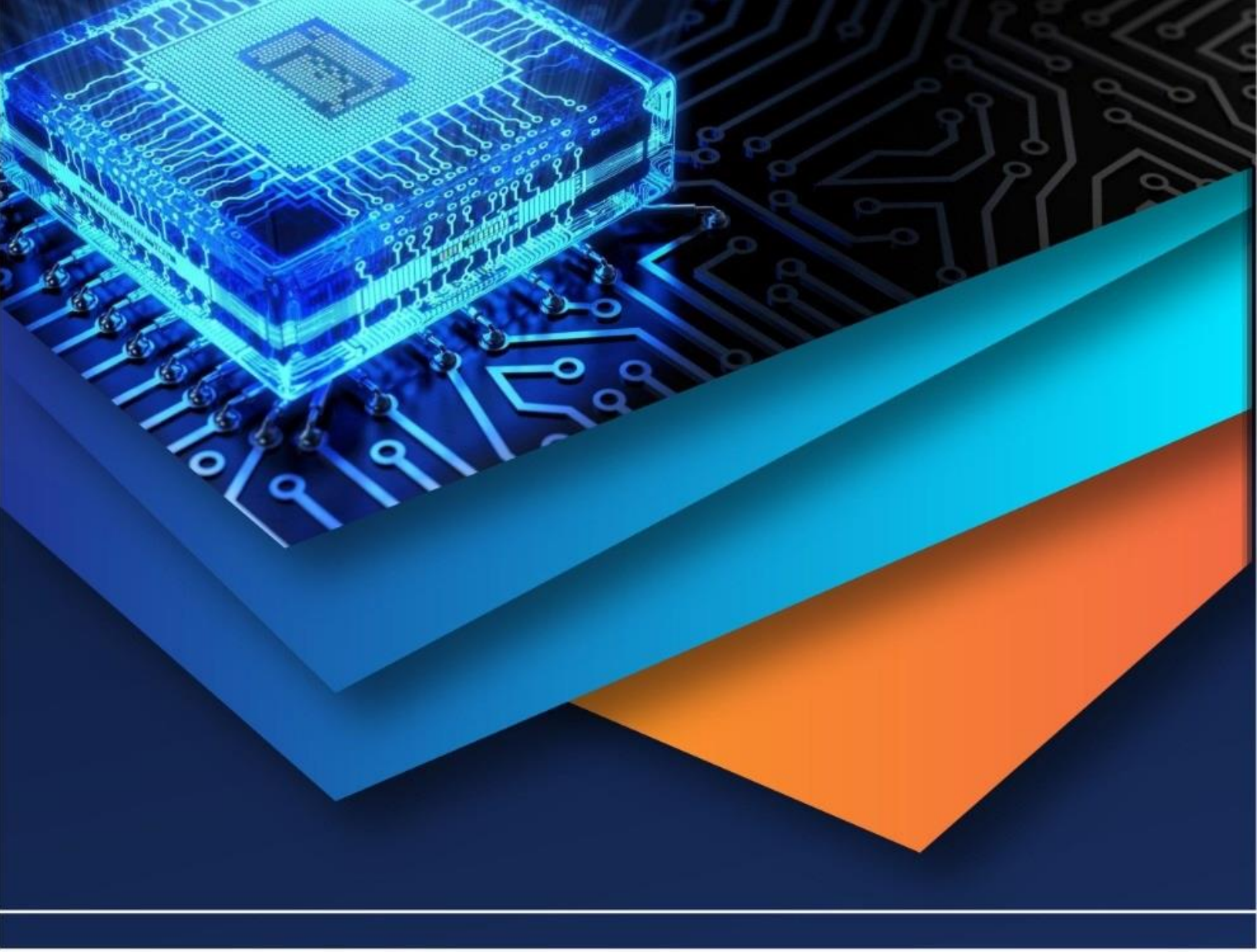
V. CONCLUSIONS

In this paper, taking into account the standard RSA mark plan, another proposed protocol is computerized contract-marking convention that permits two conceivably questioned gatherings to trade their computerized marks on an agreement in a proficient and secure way. Like the current RSA-based arrangements, the new convention is reasonable and idealistic, i.e., two gatherings get or don't get the other's computerized mark all the while, and the TTP is just required in strange cases that happen sporadically. Here our protocol is executed successfully without any conflict so the TTP is not invoked. Then again, unique in relation to all past RSA-based contract signing convention, the proposed convention is further misuse free. That is, if the agreement marking convention is executed unsuccessfully, each of the two gatherings can't demonstrate the of middle results produced by the other party to pariahs, amid or after the method where those halfway results are yield. This is a critical security property for contract marking, particularly in the circumstances where fractional duties to an agreement may be advantageous to a deceptive part.

REFERENCES

[1] 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.
[2] 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.
[3] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange ofdigital signatures," in Proc. EUROCRYPT'98, 1998, vol. 1403, LNCS, pp. 591–606, Springer-Verlag.
[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] A. Alaraj and M. Munro, "An e-Commerce Fair Exchange Protocol that Enforces the Customer to be Honest". International Journal of Product Lifecycle Management, IJPLM, Vol.3, Nos.2/3, pp. 114-131, 2008
[6] A. Nenadic, N. Zhang, and S. K. Barton, "A Secure and Fair DSA-based Signature Exchange Protocol ", the 9th IEEE Symposium on Computers and Communications (ISCC'2004), Alexandria, Egypt June 29-July 1, 2004, pp. 412-417
[7] Z. Shao "Security analysis of two RSA-Based fair document exchange protocol". In: Proceedings of the Second International Workshop on Computer Science and Engineering, Qingdao, China, pp. 55-59, 2009
[8] X. Liang, Z Cao, R. Lu, and L Qin "Efficient and secure protocol in fair document exchange", Computer Standards & Interfaces, Vol. 30 (2008), pp. 167–176, 2008
[9] 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.
[10] 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.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)