Signature Scheme to Secure Multisignature Generation for group Communication

Satish Kumar Nath
Lecturer, Govt. Polytechnic College, Pali

Akhilesh Gupta
Sr. Lecturer, Govt. Polytechnic College, Kota

Abstract: **Multisignature threshold schemes combine the properties of threshold group-oriented signature schemes and Multisignature schemes to yield a signature scheme that allows more group members to collaboratively sign an arbitrary message.**

In contrast to threshold group signatures, the individual signers do not remain anonymous, but are publicly identifiable from the information contained in the valid Multisignature. The main objective of our project is to propose such a secure and efficient Multisignature scheme. Our project shows that the proposed scheme eliminates the latest attacks to which other similar schemes are subject.

Multisignature is based on distributed-key management infrastructure (DKMI), which consists of distributed-key generation (DKG) protocol and distributed-key redistribution/updating (DKRU) protocol. The round optimal DKRU protocol solves a major problem with existing secret redistribution /updating schemes by giving group members a mechanism to identify malicious or faulty shareholders in the first round, thus avoiding multiple protocol executions.

I. INTRODUCTION

In this paper, java is used as the front end and Microsoft SQL Server is used as the back end. The group key is generated and stored in the database. The Multisignature is generated using this group key.

This paper applies Multisignature scheme for sending messages in a group. Multisignature is more secure and eliminates the latest attacks. Individual signers are identified by the information contained in Multisignature.

It consists of two protocols, Distributed Key Generation (DKG) and Distributed Key Regeneration/Updating (DKRU).

Java is used as the front end and MS Sql Server is used as the back end. In many applications, a group of members are required generate digital signature. Individual signers remain anonymous, due to the fact that it is computationally hard to derive the individual identities from the group signature.

The computational cost for Signature generation and verification is high. Individual signers do not remain anonymous, they are traceable.

This ensures accountability, i.e., a participant holds responsible for his contribution in the multisignature.

The Results show that multisignature for sending group messages can adapt well to the more complicated and practical group applications.

II. THRESHOLD SIGNATURE SCHEME (TSS)

In this threshold signature scheme, any malicious set of signers cannot impersonate any other set of signers to forge the signatures. In case of forgery, it is possible to trace the signing set.

This threshold signature scheme is applicable when the message is sensitive to the signature receiver; and the signatures are generated by the cooperation of a number of people from a given group of senders.

In most situations, the signer is generally a single person. However, in some cases the message is sent by one organization and requires the approval or consent of several people. In these cases, the signature generation is done by more than one consenting person. A common example of this policy is a large bank transaction, by one organization, which requires the signature of more than one partner. Such a policy could be implemented by having a separate digital signature for every required signer, but this solution increases the effort to verify the message linearly with the number of signer. To solve this problem, schemes [1-5] and threshold signature schemes [6-11] are used where more than one signers share the responsibility of signing messages.

Threshold signatures are closely related to the concept of threshold cryptography, first introduced by Desmedt [6-8]. In 1991, Desmedt and Frankel [7] proposed the first (t, n) threshold digital signature scheme based on the RSA system.

In (t, n) threshold signature scheme, any subgroup of t or more shareholders of the designated group can generate a valid group signature in such a way that the verifier can check the validity of the signature without identifying the identities of the signers. In threshold schemes, when any t or more shareholders act in collusion, they can impersonate any other set of shareholders to forge the signatures. In this case, the malicious set of signers does not have any responsibility for the signatures and it is impossible to trace the signers. Unfortunately, with threshold schemes proposed so far, this problem cannot be solved.

In multisignature schemes, the signers of a multisignature are identified in the beginning and the validity of the multisignature has to be verified with the help of identities of the signers. For multisignatures, it is indeed unnecessary to put a threshold value to restrict the number of signers.

Consider the situation, where a group of anonymous members would have to generate a multisignature.

The members of this group use pseudonyms as their identities in the public directory. What concerns the verifier most is that a message is signed by at least t members and they indeed come from that group.

Nevertheless, the verifier has no way to verify whether a user is in fact a member of that group because of the anonymity of the membership. In this case, the multisignature schemes cannot solve this problems, however, the threshold signature schemes do.

On the other hands, there are so many situations, when the signed message is sensitive to the signature receiver. Signatures on medical records, tax information and most personal/business transactions are such situations. Signatures used in such situations are called directed signatures [12-19]. In directed signature scheme, the signature receiver has full control over the signature verification process and can prove the validity of the signature to any third party, whenever necessary.

Nobody can check the validity of signature without his cooperation. Combining these ideas, we propose a digital signature scheme named as Directed -threshold multi signature scheme. The proposed scheme is based on Shamir's threshold signature scheme [20] and Schnorr signature scheme [18].

III. DESIGN AND METHODOLOGY

Signature
- Signature Generation
- Signature Verification

Cryptography
- Encryption
- Decryption

Message Transmission
- Multicasting
- Unicasting

Signature Generation: In this module we are going to generate signatures for the group members.

Thus it has two sub modules,
- Individual Signature Generation
- Multiple Signature Generation.

The Individual signature is generated with Participants private key.

Participants broadcast the message and the signature to all protocol participants.

Using the ElGamal Algorithm, the individual signature is generated.

Any subset β of t or more members can represent the group and sign an arbitrary message m.

IV. OUTCOME AND SIGNIFICANCE

***INPUT*:**
- User gives the username as entry input
- User gives the password as entry input
- User gives the message for transmission
- System gives the input private key for users
- System gives the input public key for users
- System gives the hash value using the private key
- System gives the Signature from the hash value
- System gives the Encrypted message from the user input message
- System transfers the message signature.

OUTPUT:
- User receives the encrypted message
- System automatically generates the output signature for verification
- System automatically decrypts the message using Elgamal algorithm
- System automatically shows the sender details
- System automatically shows the decrypted message.

V. Conclusions and Future Work

In this paper, we proposed an A secure MultiSignature Scheme for sending group messages was introduced.

The efficiency of the proposed system outperforms other system. The Multisignature scheme fulfills all security requirements.

Thus Multisignature scheme can be applied in group communication to improve the efficiency.

Future Work done by the group

VI. REFERENCES

[1] Harn L. and Kiesler T, "New Scheme for Digital Multisignatures.Electronic Letters" 25(15): p.p. 1002-1003, 1989.

[2] Hardjono T. and Zheng Y, "A practical Digital Multisignature Scheme Based on DLP", Advance in cryptology –Auscrypt-92, p.p. 16 – 21, 1992.

[3] Itakura K. and Nakamura K, "A Public Key C cryptosystem Suitable for Digital Multisignatures.NEC Research and Develop", p.p.1-8. 1983.

[4] Okamoto T, "A digital Multi-signature scheme using bijective PKC", ACM transactions on computer systems, Vol 6, No -8, p.p. 432-441, 1988.

[5] Ohta K. and Okamoto T, "A digital multisignature scheme based on Fiat-Shamir scheme", Advance in Cryptology Asiacrypt, p.p. 75 – 79, 1991.

[6] Desmedt, Y, "Society and group oriented cryptography", In Advances in Cryptology –Crypto -87, Proceedings. p.p. 457-469. New York: Springer Verlag, 1988.

[7] Desmedt, Y. and Frankel Y, "Shared Generation of Authenticators and Signatures", In Advances in Cryptology – Crypto -91, Proceedings. p.p. 457-469. New York: Springer Verlag, 1991.

[8] Desmedt, Y, "Threshold cryptography", European Transactions on Telecommunications and Related Technologies, Vol. 5, No. 4, p.p.35 – 43, 1994.

[9] Gennaro R., Jarecki Hkrawczyk S., and Rabin T, "Robust threshold DSS signature", Advances in Cryptology – Euro Crypto, Proceedings. p.p.354 -371, Berlin-Heidelberg: Springer Verlag, 1996.

[10] Harn , "(t, n) Threshold signature scheme and digital multisignature', Workshop on cryptography and Data security, Proceedings p.p.61-73. Chung Cheng Institute of Technology, ROC, June 7-9. 1993.

[11] Rabin, T, "A simplified approach to threshold and proactive RSA', In Advances in Cryptology –Crypto, Proceedings p.p. 89-104. New York: Springer Verlag, 1998.

[12] Boyar, J., Chaum D., Damgard I. and Pederson T, "Convertible undeniable signatures", Advances in Cryptology – Crypto, 90, LNCS # 537,p.p.189-205, 1991.

[13] Chaum D, 'Zero-knowledge undeniable signatures. Advances in Cryptology", Eurocrypt, 90, LNCS # 473,p.p.458-464, 1991.

[14] Chaum D, "Designated confirmer signatures, Advances in Cryptology Euro crypt, 94 LNCS # 950,p.p.86-91, 1995.

[15] Lim C.H. and P.J.Lee, "Security Protocol", In Proceedings of International Workshop, (Cambridge, United Kingdom), Springer-Verlag, LNCS # 1189, 1996.

[16] Mullin R.C., Blake I.F., Fuji – Hara R. and Vanstone S.A, 'Computing Logarithms in a finite field of characteristic two', SIAM J. Alg.Disc.Meth. p.p.276 – 285, 1985.

[17] Okamoto T, “Designated confirmer signatures and public key encryption are equivalent”, Advances in Cryptology – Crypto, 94 LNCS # 839, p.p.61-74, 1994.

[18] Sunder Lal and Manoj Kumar, “A directed signature scheme and its applications”, Proceedings, National Conference on Information Security, p.p. 124 – 132, New Delhi, 8-9 Jan 2003.

[19] Yen S.M. and Laih C.S, “New digital signature scheme based on Discrete Logarithm”, Electronic Letters, Vol. 29 No. 12 pp. 1120-1121, 1993.

[20] Schnorr C.P, “Efficient signature generation by smart cards”, Journal of Cryptology, 4(3), p.p.161-174, 1994.