

Cryptography: Secure Multisignature Generation for Group Communication

¹Neha Chaudhary, ²Aarti Kushwaha, ³Manoj Kumar Shukla, ⁴Saoud Sarwaha

^{1,3}Dept. of CSE, Sunder Deep Engineering College, Ghaziabad, UP India

²Dept. of CSE, G.B.Pant Engineering College, New Delhi, India

⁴Dept. of CSE, AFSET, Faridabad, HR, India

Abstract

Threshold Multisignature 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. The main objective of this paper is to propose such a secure and efficient Multisignature scheme. This paper shows that the proposed scheme eliminates the latest attacks to which other similar schemes are subject.

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 computational cost is reduced when compared to other schemes. We will use the multisignature in a simple application for sending group messages.

Keywords

Cryptography, Group Communication, Threshold Multisignature Scheme

I. Introduction

In distributed systems it is sometimes necessary for users to share the power to use a cryptosystem. The system secret is divided up into shares and securely stored by the entities forming the distributed cryptosystem. The main advantage of a distributed cryptosystem is that the secret is never computed, reconstructed, or stored in a single location, making the secret more difficult to compromise. Investigations within the fields of threshold group-oriented signature schemes, threshold group signature schemes, Multisignature schemes, and Threshold-Multisignature schemes resulted in explicitly defining the properties of Threshold-Multisignature schemes.

Threshold Multisignature 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.

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 share holders in the first round, thus avoiding multiple protocol executions. This paper explains 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).

- 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 computational cost is reduced when compared to other schemes.
- We have applied the multisignature in a simple application for sending group messages.

II. Digital Signature

A Digital Signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's public key.

The signature guarantees the source and integrity of the message.

III. Threshold Multisignature

IN distributed systems it is sometimes necessary for users to share the power to use a cryptosystem [1-2]. The system secret is divided up into shares and securely stored by the entities forming the distributed cryptosystem. The main advantage of a distributed cryptosystem is that the secret is never computed, reconstructed, or stored in a single location, making the secret more difficult to compromise [3].

Threshold-multisignature schemes [4] combine the properties of threshold group-oriented signature schemes [2] and multisignature schemes [5]. In the literature, threshold-multisignature schemes are also referred to as threshold signature schemes with traceability.

The combined properties guarantee the signature verifier that at least t members participated in the generation of the Group - oriented signature and that the identities of the signers can be easily established. The majority of the existing threshold-multisignature schemes belong to variants of the single signatory, generalized ElGamal signatures, extended to a group/multiparty setting.

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 problems, schemes [10-11,13,17-18] and threshold signature schemes [5-7,9,12,20] 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 [5-7]. In 1991, Desmedt and Frankel [6] 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 [1-3, 14-15, 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.

IV. Signature Generation

In this phase we are going to generate signatures for the group members.

Thus it has two schemes:

- 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.

V. Signature Verification

In this phase we will verify the group member's signatures with generated signatures.

On receiving all of the signatures, we perform the functionality of a clerk and use the public key set to authenticate the individual signature.

Participants are disqualified if their individual signatures are found to be invalid.

VI. Cryptography

Encryption- The message is encrypted using DES algorithm.

Decryption- The received message is decrypted in the receiver side

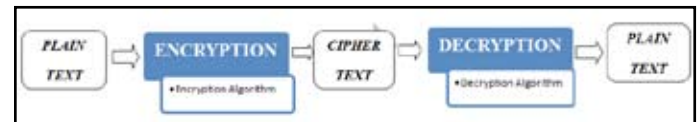


Fig. 1: Cryptography

VII. The ElGamal Cryptosystem

In 1984 Taher ElGamal presented a cryptosystem which is based on the Discrete Logarithm Problem discussed in the last section [6]. It relies on the assumption that the DL cannot be found in feasible time, while the inverse operation of the power can be computed efficiently.

The original public key system proposed by Diffie and Hellman requires interaction of both parties to calculate a common private key. This poses problems if the cryptosystem should be applied to communication systems where both parties are not able to interact in reasonable time due to delays in transmission or unavailability of the receiving party.

Thus ElGamal simplified the Diffie-Hellman key exchange algorithm by introducing a random exponent k . This exponent is a replacement for the private exponent of the receiving entity. Due to this simplification the algorithm can be used to encrypt in one direction, without the necessity of the second party to take actively part. The key advance here is that the algorithm can be used for encryption of electronic messages, which are transmitted by the means of public store-and-forward services.

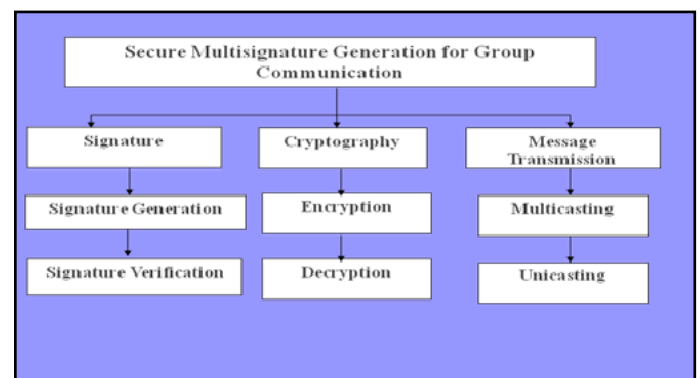


Fig. 2: System Architecture

VIII. Conclusion

- 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.

References

- [1] Y. Desmedt, "Society and Group Oriented Cryptography: A New Concept", Proc. Advances in Cryptology—CRYPTO '87, 1987.
- [2] Y. Desmedt, "Threshold Cryptography", European Trans. Telecomm., Vol. 5, No. 4, pp. 449-457, 1994.
- [3] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems", Proc. Advances in Cryptology—EUROCRYPT '99, May 1999.
- [4] C.-M. Li, T. Hwang, N.-Y. Lee, "Threshold-Multisignature Schemes where Suspected Forgery Implies Traceability of Adversarial Shareholders", Proc. Advances in Cryptology—EUROCRYPT '94, May 1994.
- [5] A. Boldyreva, "Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme", Proc. Public Key Cryptography—PKC '03, 2003.
- [6] C.-T. Wang, C.-H. Lin, and C.-C. Chang, "Threshold Signature Schemes with Traceable Signers in Group Communications," Computer Comm., Vol. 21, No. 8, pp. 771-776, 1998.
- [7] W.-B. Lee, C.-C. Chang, "(t,n) Threshold Digital Signature with Traceability Property", J. Information Science and Eng., Vol. 15, No. 5, pp. 669-678, 1999.
- [8] Z.-C. Li, J.-M. Zhang, J. Luo, W. Song, Y.-Q. Dai, "Group-Oriented (t, n) Threshold Digital Signature Schemes with Traceable Signers", L Proc. Second Int'l Symp. Topics in Electronic Commerce (ISEC '01), Apr. 2001.
- [9] P. Horster, M. Michels, H. Petersen, "Generalized ElGamal Signatures for One Message Block", Proc. Second Int'l Workshop ITSecurity, Sept. 1994.
- [10] L. Harn, Y. Xu, "Design of Generalised ElGamal Type Digital Signature Schemes Based on Discrete Logarithms", Electronics Letters, Vol. 30, No. 24, pp. 2025-2026, 1994.
- [11] G. Wang, "On the Security of the Li-Hwang-Lee-Tsai Threshold Group Signature Scheme", Proc. Fifth Int'l Conf. Information Security and Cryptography (ICISC '02), Nov. 2002.
- [12] H. Pedersen, "How to Convert Any Digital Signature Scheme into a Group Signature Scheme", Proc. Fifth Int'l Workshop Security Protocols, Apr. 1997.
- [13] L. Zhou, Z.J. Haas, "Securing Ad-Hoc Networks", IEEE Network, special issue on network security, Vol. 13, No. 6, pp. 24-30, 1999.
- [14] T.P. Pedersen, "A Threshold Cryptosystem without a Trusted Party", Proc. Advances in Cryptology—EUROCRYPT '91, 1991.
- [15] M. Stadler, "Publicly Verifiable Secret Sharing", Proc. Advances in Cryptology—EUROCRYPT '96, 1996.
- [16] P.-A. Fouque, J. Stern, "One Round Threshold Discrete-Log Key Generation without Private Channels", Proc. Public Key Cryptography—PKC '01, Feb. 2001.
- [17] R. Zhang, V.H. Imai, "Round Optimal Distributed Key Generation of Threshold Cryptosystem Based on Discrete Logarithm Problem", Proc. Applied Cryptography and Network Security (ACNS '03), Oct. 2003.
- [18] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, "Proactive Secret Sharing or: How to Cope with Perpetual Leakage", Proc. Advances in Cryptology—CRYPTO '95, 1995.
- [19] Y. Desmedt, S. Jajodia, "Redistributing Secret Shares to New Access Structures and Its Applications", Technical Report ISSETR- 97-01, Dept. of Information and Software Eng., School of Information Technology and Eng., George Mason Univ., July 1997.
- [20] T.M. Wong, C. Wang, J.M. Wing, "Verifiable Secret Redistribution for Archive System", Proc. First Int'l IEEE Security in Storage Workshop, Dec. 2002.