Intelligent Manufacturing and Cloud Computing
I.S. Jesus and K. Wang (Eds.)

doi:10.3233/ATDE241379

Research on Authorization Verification Methods for Message Signatures Within Multi-Level Groups

Hu Zhang[a], Jiarui Zhang[b, 1] and Han Zhang[c]
[a]*Undergraduate Software Engineering Class of 2021, Hefei University, Hefei, China*
[b]*Department of Information Engineering, Yantai Institute of Technology, Yantai, China*
[c]*Beijing Academy of Blockchain and Edge Computing, Beijing, China*

Abstract. With the widespread adoption of digital signature,a variety of specialized digital signature methods have been developed. However, the need for authorization verification within hierarchical group structures has not garnered sufficient attention. This research has addressed this issue. Initially, the problem was delineated and formally articulated; subsequently, encryption and decryption algorithms that incorporate authorization sharing were designed, along with a description of the code;finally, the methods were validated through experimentation. The outcomes demonstrate that the proposed approach is reliable and stable, capable of effectively accommodating the authorization verification of signed messages within multi-tiered, large-scale group communications. This addresses the shortfall of current digital signature technologies, which struggle to authorize multiple verifiers within hierarchical group structures, by supplementing and refining a method for the authorization verification of signed messages among users in multi-level groups.

Keywords. Digital signature, hierarchical groups, encryption, decryption, authorization verification

1. Introduction

Whether it is government agencies, public institutions, enterprises, or social organizations, their internal organizations are hierarchical and divided by job responsibilities. The messages transmitted within the organization are also divided by topics. Generally, the messages transmitted within the organization need to be authorized to different levels or members with different responsibilities according to the different topics they belong to. The authorized person may be one or multiple. This is a very common application scenario. However, the existing digital signature technology mainly focuses on improving the security, anonymity, and untraceability of message transmission, but the demand for authorization verification within multi-level groups has not received enough attention.

[1] Corresponding Author: Jiarui Zhang, zhangjiarui099@163.com

2. Related Work

2.1. Traditional digital signature technology

Diffie and Hellman first introduced the concept of electronic signatures in 1976, and in 2003, Anderson R. provided a comprehensive definition of digital signatures.[1] It is based on the public/private key cryptographic system and is essentially an application of asymmetric encryption technology.

Common digital signature algorithms include: RSA, Elliptic Curve Digital Signature Algorithm (ECDSA), and Finite Automata-based digital signature algorithms, among others. Specialized digital signatures include group signatures, ring signatures, threshold signatures, blind signatures, proxy signatures, undeniable signatures, fair blind signatures, and signatures with message recovery capabilities.

2.2. Common digital signature

Group signatures, first introduced by Chaum and Van Heyst in 1991, allow group members to sign documents or messages using their group certificates and their private keys to generate a group signature.

As technology evolves, group signature schemes are also evolving to meet more complex scenario requirements. Backes[2] and others have studied the issue of member privacy protection in fully dynamic group signatures; Tang[3] and others have implemented a group signature method based on lattices with editable signatures and time-limited keys; Perera[3] and others have used a decentralized collaborative approach to analyze and study the tracking of group signers; Fu[4] and others have proposed a blockchain privacy protection technology monitoring scheme based on group signatures. Liu[5] and others have studied a decentralized system group signature method based on identity and optimization of the national secret SM2 algorithm.

Ring signatures were originally conceived and proposed in 2001 by Rivest, Adi Shamir, and Yael Tauman. They are a simplified version of group signatures. The signature generated has a certain parameter that forms a ring according to certain rules, hence the name ring signature. There is no need for a manager in ring signatures, nor is there a need for cooperation among ring members.

Currently, the industry's research on ring signatures is mainly focused on improving its security, efficiency, and practicality. Jingzhong[6] and others designed an electronic voting protocol based on ring signatures and secure multi-party computation; Kugusheva[7] and others implemented a blockchain voting method based on ring signatures; Yang[8] and others studied the design method of blockchain smart contracts based on ring signatures; Wang[9] and others studied a quantum ring signature scheme based on the quantum finite automaton signature method.

In 1991, Desmedt and Frankel made a groundbreaking proposal of the (t, n) threshold signature scheme, a milestone contribution that marked the digital signature method based on Multi-Party Computation (MPC) technology entering a new era. By splitting the private key and distributing it to multiple signers, a valid signature can only be generated when a certain number of signers participate.

The latest research progress in threshold signatures includes Tang[10] and others proposing an efficient threshold signature scheme based on lattices with functional interchangeability; Kachouh[11] and others have studied a threshold elliptic curve

digital signature algorithm for multi-party applications. In addition, with the continuous development and application of blockchain technology, threshold signature technology is expected to be more widely applied and promoted in the future.

The concept of blind signatures was first proposed by David Chaum in 1982. In blind signatures, the message holder submits an encrypted message, which has been blinded, to the signer for signing, making it a special type of digital signature method.

The latest research progress in blind signatures includes Shim[12] and others who analyzed the cryptography of lattice-based blind signatures and blind ring signature schemes; Ma[13] and others who designed an attribute-based blind signature scheme using elliptic curve cryptography; Jiang[14] and others who analyzed and constructed the cryptography in identity-based partial blind signature schemes; Sumathy[15] and others who designed a quantum blind signature protocol based on quantum teleportation and entanglement for quantum secure communication in security service bases.

In summary, the aforementioned widely used digital signature technologies have achieved significant results in terms of signer anonymity, untraceability of the signer, privacy protection of the message content, and signature security. However, the application demand for the signer to designate (authorize) a verifier, especially to designate (authorize) multiple verifiers within a group, still requires further research. In light of this, this study is committed to improving a method for authorized verification of signed messages between users in a multi-level group, in order to make up for the regret that existing digital signature technologies cannot authorize multiple verifiers within multi-level groups.

3. Research on Authorization Verification Methods for Message Signatures within Multi-Level Groups

3.1. Problem definition and formalization representation

The research scenario for the project is as follows: In a group G, there are n (where n is no less than 3) group members (users). A message signed by any user can only be verified and the original message retrieved by authorized group members; unauthorized group members are unable to obtain the original message.The core process is as follows:

Let: the group members be $U_i(i = 1,2,..., n)$, the original message M, and the ciphertext C_i signed by U_i.Assuming that user U_i wants C_i to be received and decrypted only by users in U_{sup}, a subset of members in group G, the problem can be expressed as:

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

$$\mathrm{Sig}_{(U_I \to U_{\sup})}(M) = C_i \tag{1}$$

$$\mathrm{Ver}_{(U_j \in U_{\sup})}(C_i) = M \tag{2}$$

In this context:Equation (1) indicates that a group member U_i signs the message M to produce a ciphertext C_i, and authorizes the members included in the subset U_{sup} to verify and decrypt it. Equation (2) states that a group member U_j , who is a part of

U_{sup} , is the only one who can verify and decrypt the ciphertext C_i to obtain the original message M .

3.2. Key algorithm design

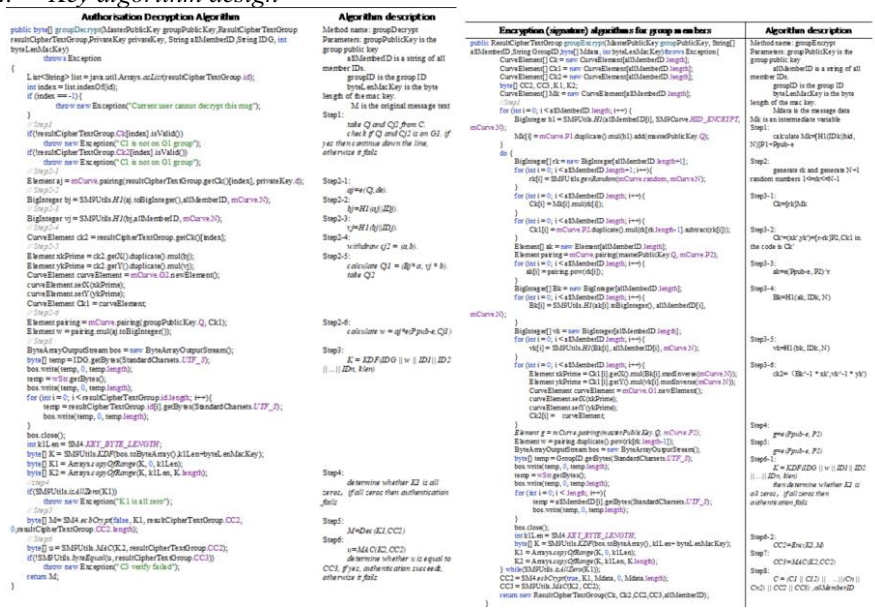

Figure 1. Signature Algorithm

The code encrypts and decrypts data using the SM9 algorithm, based on the master public key, group ID, data, and MAC key length.

4. Experimental Validation of an Authorisation Verification Method for Message Signatures within Multilevel Groups

4.1. Experimental environment

Device Model: Precision 3660-China HDD Protection
CPU: 12th Gen Intel(R) Core(TM) i9-12900K
Memory: 32GB DDR5 4800MHz
GPU: NVIDIA GeForce RTX 3080
Operating System: Windows 10

4.2. Experimental methods

Java JDK17 & JPBC Experiment Overview

Simulation: Virtual nodes represent group members with unique IDs, public/private keys.

Authorised Users: Randomly selected user nodes within the group.

Method: Use JPBC for encryption/decryption. Simulate increasing group size (10-50 members) and authorised users (1-5). Measure algorithm correctness, encryption/decryption efficiency.

Experimental objectives:1) Verify correctness of encryption/decryption.;2) Evaluate stability as group size and authorised user count increase.Experimental results and analysis

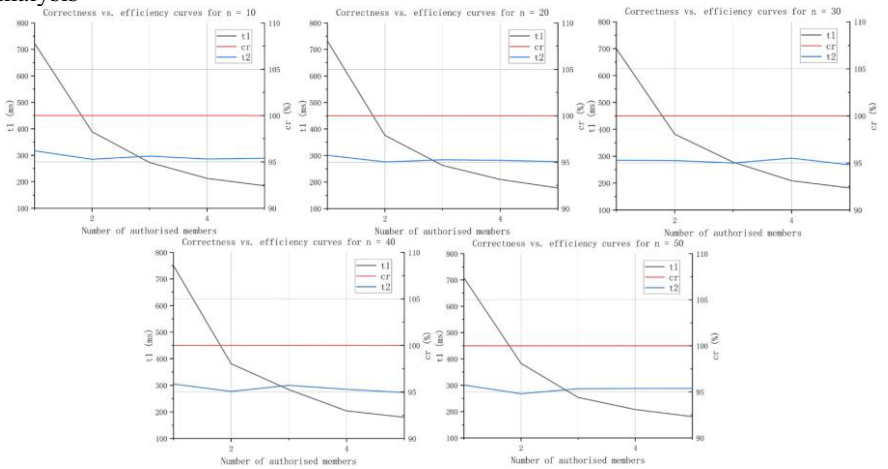

Figure 2.

Among Fig. 2. shows the correctness vs. efficiency curve for n=10, n=20, n=30, n=40,n=50. cr(%) is the algorithm correctness rate; t1 is the average encryption time; and t2 is the average decryption time of the authorised members.

Experimental data reveals that:(1) Regardless of group size, the accuracy (cr) of the core algorithm remains 100% as the number of authorized users increases.(2) Within each experiment, t1 fluctuations are within 500ms regardless of changes in b.(3) Encryption time is less correlated with group size n and more inversely related to the number of authorized users b.(4) t2 fluctuations are minor, unrelated to both n and b, consistent within and across experiments.

In conclusion, experiments and analysis confirm the reliability and stability of the proposed core algorithm, effectively accommodating authorization verification for multi-level, large-scale group message signatures.

5. Conclusions and Recommendations

In response to the reality that the demand for authorization verification in multi-level groups has not received enough attention, this paper proposes an algorithm that fuses message signatures to authenticate authorized verification users. The algorithm is implemented and experimentally verified, proving the reliability and stability of the proposed algorithm, specifically demonstrated by a 100% correct rate. Although the number of authorized verification users increases, the encryption time is independent of the number of group members and negatively correlated with the number of authorized users, with a fluctuation range of no more than 500ms. In terms of decryption time for authorized verification users, the fluctuation range is no more than 50ms and independent of the number of group members and authorized users. This indicates that the proposed algorithm is effective in adapting to the application of large-scale, multi-level group message signatures authorization verification, which is particularly valuable in hierarchical and role-based groups, such as government agencies,

enterprises, societies, etc. where group members need to be authorized to access different topics within the group.

It is evident from this study that the group size and the number of authorized users can be expanded to a wider range, such as n=1000 and b=20. In addition, the virtual machine technology used in this experiment can be ported to real distributed network nodes and further refined with possible network failures, low bandwidth, etc. to obtain more precise conclusions, which can guide related scene applications.

6. Acknowledgment

This study was supported by the following grants: Blockchain Technology Innovation and Application Programme for Higher Schools, Department of Education of Anhui Province (No. 2020qkl33); Natural Science Foundation of Hefei City (No. 202301).

References

[1] R. Anderson, "Digital Signature," in Encyclopedia of Computer Science, 2003, pp. 581-583.
[2] Backes M, Hanzlik L, Schneider-Bensch J. Membership privacy for fully dynamic group signatures[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019: 2181-2198.
[3] M. N. S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C.-M. Cheng, and K. Sakurai, "Decentralized and Collaborative Tracing for Group Signatures," in Proc. 2022 ACM Asia Conf. Comput. Commun. Secur. (ASIA CCS '22), 2022, pp. 1258-1260.
[4] K. Fu, L. Wang, W. Shao, W. Wang, S. Zhang, S. Xu, and S. Hu, "Supervisory Scheme for Blockchain Privacy Protection Technique Based on Group Signature," in Proc. 2021 ACM Int. Conf. Intell. Comput. Emerg. Appl., 2021, pp. 223-228.
[5] J. Liu, T. Kang, and L. Guo, "An Identity-Based Group Signature Approach on Decentralized Systems and Chinese Cryptographic SM2," in Proc. 8th Int. Conf. Commun. Inf. Process., 2022, pp. 142-148.
[6] Jingzhong W, Yue Z, Haibin L. Electronic voting protocol based on ring signature and secure multi-party computing[C]//2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). IEEE, 2020: 50-55.
[7] A. Kugusheva and Y. Yanovich, "Ring Signature-Based Voting on Blockchain," in Proc. 2019 2nd Int. Conf. Blockchain Technol. Appl., 2019, pp. 70-75.
[8] H. Yang, L. Yuan, and S. Wang, "Design of Blockchain Smart Contract Based on Ring Signature," in Proc. 2021 9th Int. Conf. Commun. Broadband Netw., 2021, pp. 108-114.
[9] H. Wang, G. Yao, and B. Wang, "A Quantum Ring Signature Scheme Based on the Quantum Finite Automata Signature Scheme," in Proc. IEEE 15th Int. Conf. Anti-Counterfeiting, Secur., Ident. (ASID), 2021, pp. 135-139.
[10] G. Tang, B. Pang, L. Chen, and Z. Zhang, "Efficient Lattice-Based Threshold Signatures With Functional Interchangeability," IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 4173-4187, 2023.
[11] B. Kachouh, L. Sliman, A. E. Samhat, and K. Barkaoui, "Demystifying Threshold Elliptic Curve Digital Signature Algorithm for Multi-Party Applications," in Proc. 2023 Australasian Comput. Sci. Week, 2023, pp. 112-121.
[12] K. A. Shim and Y. An, "Cryptanalysis of Lattice-Based Blind Signature and Blind Ring Signature Schemes," IEEE Access, vol. 9, 2021, pp. 134427-134434.
[13] R. Ma and L. Du, "Attribute-Based Blind Signature Scheme Based on Elliptic Curve Cryptography," IEEE Access, vol. 10, 2022, pp. 34221-34227.
[14] Y. Jiang, L. Deng, and B. Ning, "Identity-Based Partially Blind Signature Scheme: Cryptanalysis and Construction," IEEE Access, vol. 9, 2021, pp. 78017-78024.
[15] G. Sumathy, A. Suresh, R. Udendhran, A. Maheshwari, and A. Prasath Selvaraj, "Quantum Teleportation and Entanglement-Based Quantum Blind Signature Protocol for Quantum Secure Communication in Security Service Bases," in Proc. 5th Int. Conf. Inf. Manage. Mach. Intell. (ICIMMI '23), 2024, art. no. 56, pp. 1-10.