Group Signature Resistant Against Colluding Attack

Kumari Sonam [1], Jeevan Kumar [2]

[1] M. Tech, CSE Dept., R. V. S College of Engg. & Tech., Jamshedpur
[2] Professor, CSE Dept., R. V. S College of Engg. & Tech., Jamshedpur

Abstract

Group signature is a digital signature extension that allows a group member to sign a document anonymously on behalf of the group. Using public parameters of the group, any client can validate the documents legitimacy. The group signature does not expose the identity of the group member. In the event of a legal dispute, an authorized group member can use the signed document to reveal the identity of the group member. Group signatures have a wide range of uses in the corporate world, banks, and e-commerce. In this project, we created a group signature protocol using the Python programming language. The proposed technique has been shown to be robust to colluding attacks. Furthermore, even if some members quit the group the group signature remains valid. The proposed system confirms the full traceability feature. The method has a wide range of real-world applications, including e-banking, e-voting, and e-commerce.

Keywords: : Group signature, python, colluding attack, anonymously

1. Introduction

A digital signature is a mathematical system that ensures the authenticity of digital data or documents. A genuine digital signature provides a recipient with reason to trust that the information was provided by a known sender , such that the sender cannot deny sending the message and that it was not altered in transit. Digital signatures are mostly used in software distribution, financial transactions, and legal matters where it is critical to identify forgery or tampering with digital information. Extending the concept of digital signature into the group, Chaum and Heyst proposed a new signature technique, group signature scheme, which allows a group member to sign messages anonymously on behalf of the group.

Any client can confirm the legitimacy. Only the group's public key and parameters were used to generate the signature. A signed message cannot be used to determine the identity of a group member. In the event of a disagreement, a designated entity may expose the identity of a signer or member. The main feature of group signature is the security of the information or data, which makes it more important and appealing for many real-time applications, such as e-cash, e-bidding, and e-commerce, where the importance of signer privacy and anonymity is very high and important for an organization. When signing communications, a group signature method is intended to ensure anonymity and accountability for individual members of the group. However, in some cases, attackers may try to collaborate and pool their resources in order to breach the anonymity of the scheme and reveal the names of anonymous signers. This is referred to be a conspiring attack.

Group signature is a cryptographic mechanism that allows members of a certain group to sign communications or documents collectively while keeping the signer's anonymity. The identity of the signer is known in a traditional digital signature, but in group signatures, the identity of the individual signer is hidden among a group of signers. This capability makes group signatures very suitable for applications that require secrecy and anonymity. A signature's core features are authenticity, nonforgery, nonreusability, and irrevocability. These properties protect the message from various cryptographic attacks such as disguise, alteration, and fabrication. Over the previous three decades, numerous digital signature systems have been released; but, as technology progresses, the security services they provide can be easily subverted. At the moment, digital signatures are derived using public-key cryptography techniques. However, some of these signature techniques, such as RSA, are less robust over time.

2. Literature Survey

Cryptography is the process of encrypting information and converting it into an unreadable format known as cipher text. Only individuals with a secret key can convert the message to plain text. Although modern cryptography techniques are almost unbreakable, encrypted messages can sometimes be broken through cryptanalysis, commonly known as code breaking. Cryptography systems are broadly classified into symmetric-key systems, which use a single key that both the sender and recipient have, and systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses, but in the case of signatures, a public key system is used, with the signer signing with the private key and the verifier verifying with the public key. The Group Signature Scheme Is Comprised On Four Major Entities. The group manager is a trusted authority who is in charge of creating and managing the group. It generates the public key for the group and assigns private keys to each group members. these are the individuals who have their own private keys as well as the group's public key. They can sign communications anonymously on behalf of the group using their private keys. When a group member wants to sign a message, they use their private key in conjunction with the group's public key to generate a group signature. Anyone can validate and verify the signature, but it does not reveal the name of the specific person who signed the letter. A verifier utilises the group's public key and the signature itself to validate the group signature. The verification process confirms that the signature is authentic and came from a member of the group, but it does not expose the identity of the signer. Group signatures allow anonymity through the employment of specialized cryptographic methods and protocols. These techniques are intended to withstand assaults that could reveal the signer's identity based on the signature or patterns in the signing process. Group signatures are used in privacy-preserving authentication and authorization systems, in which a user may prove their membership in a certain group without disclosing their identity. Group signatures have also been used in secure electronic voting systems to protect voter privacy while maintaining voting process integrity. Group signatures, however, are not without difficulties. One critical feature is preventing collaboration between group members and the group manager, which might lead to the signature system being abused. Furthermore, balancing anonymity and traceability is a sensitive undertaking, since perfect anonymity may allow harmful behaviour, whilst excessive tracking may undermine the objective of group signatures.

To summarise , group signatures are an effective approach for achieving anonymity in digital signatures within a defined group. By balancing privacy and accountability, group signatures have found uses in a variety of fields where the identity of individual signers is critical. Group signature systems are likely to see additional developments and practical implementations as cryptography research advances. A colluding attack happens when a subset of group members conspire to misuse their signing capabilities, allowing them to violate the group signature scheme's anonymity requirements. This poses a severe risk to the scheme's security and privacy, as it defeats the goal of giving anonymous signatures. A strong group signing scheme must be carefully constructed with security mechanisms that make it extremely difficult or computationally infeasible for a colluding subset of group members to divulge the identity of a signer in order to withstand colluding attacks. A group signature scheme's resistance to conspiring attacks can be improved by using the following approaches and features. Secure Hash Functions, Digital Signatures, and Zero-Knowledge Proofs:

The strategy should be built on strong cryptographic primitives such as secure hash functions, digital signatures, and zero-knowledge proofs. These primitives serve as the foundation for ensuring the group signature scheme's security features.

Trusted Group Manager: The group manager is an important part of the group signature method. To avoid colluding attacks, the group manager should be trustworthy and not collude with any subgroup of group members to compromise anonymity. To avoid single points of failure, the group manager may be a third-party entity or a decentralized consensus mechanism in practise.

A number of group signature methods have been presented since Chaum's initial proposals. Chen and Pedersen developed a technique that permits new members to join the group dynamically and proposed using group signatures in e-bidding. Camenisch and Stadler presented the first group signature technique that can be utilised for large groups, because the group public key and signatures have lengths that are independent of group size. Later, Kim et al. expanded their approach to support efficient member revocation. Ateniese and Tsudik identified certain barriers to real-world applications of group signatures, such as coalition attacks and member elimination .According to the literature, the group signature systems currently in use can be broadly divided into two sorts: public-key registration types and certificate-based types. In the former category, only known-order groups are used to build. However, in these methods, the number of group members affects both the group public key and the signature size. It results in a significant issue for big groupings. The group signature of the latter type is based on the zero-knowledge proof of knowledge (SPK) of the membership certificate, and members are given membership certificates. As a result, neither the size of a group signature nor its public key is dependent on the number of group members. The group signature is an extension of the digital signature concept with some strict conditions, one of which being resistance against conspiring attacks. Because the entire strength of a secure system is based on the trust and security parameters used in the system, if collusion is possible, the signature can be easily forged, crashing the entire system of signing the document and posing a threat to the security of digital information or messages.

3. Methodology

The proposed technique is implemented using the Python programming language to store the key parameters. The suggested technique is implemented in Python Big integer numbers, with the Crypto and Security packages being used to generate secret key parameters for members and the hash function algorithm being used for the signature generation phase.

3.1 key generation: A group signature is a cryptographic primitive that allows a number of users to sign messages or documents jointly while preserving each signer's privacy inside the group. David Chaum and Eugene van Heyst first presented the idea in 1991. With the extra feature of signer anonymity, group signatures offer a means to combine the advantages of digital signatures, which guarantee the validity and integrity of messages.

3.2 Group Formation: The group manager, a trusted authority in charge of setting up and overseeing the group signature system, initiates the procedure. A group public key is created and distributed to all group members by the group admin.

3.3 Key Generation: To receive their private key, each group member goes through a key generation process. Private keys are created and distributed to each group member by the group manager. Members of the group sign communications on their behalf using these private keys.

3.4 Signature creation: To sign a message or document, a group member needs to combine their private key with the group's public key. The signature indicates the group's collective approval while concealing the signer's identity.

3.5 Signature Verification: A third party (the verifier) utilizes the group's public key and the signature itself to validate a group signature. Verification confirms that the signature is legitimate and that it was generated using one of the legitimate private keys linked to the group public key.

3.6 Anonymity and Unlinkability: Anonymity is a group signature's primary characteristic, along with unlinkability. The verifier can attest that the signature is genuine and was provided by an authorized group member, but it is unable to identify the precise individual who signed it. Additionally, group signatures provide unlinkability, which prevents correlation or linking between numerous signatures generated by the same group member at various times.

3.7 Opening and Tracing: Group signature methods typically provide a mechanism that enables "opening" a signature, even when individual identities are kept secret during routine verification. Opening a signature entails disclosing the signer's identity in specific situations, such as when an authorized authority is required to track down criminal activity or look into a dispute.

3.8 Revocation: The ability to revoke a single group member's signing authority is a crucial component of group signatures. Revocation is required to keep the system secure and accountable, especially when a group member is hacked or behaves maliciously.

The security characteristics of group signature schemes, such as anonymity, unforgeability, and traceability, are carefully taken into account when they are constructed. To maintain the success and viability of the plan, it is imperative to strike the proper balance between anonymity and traceability.

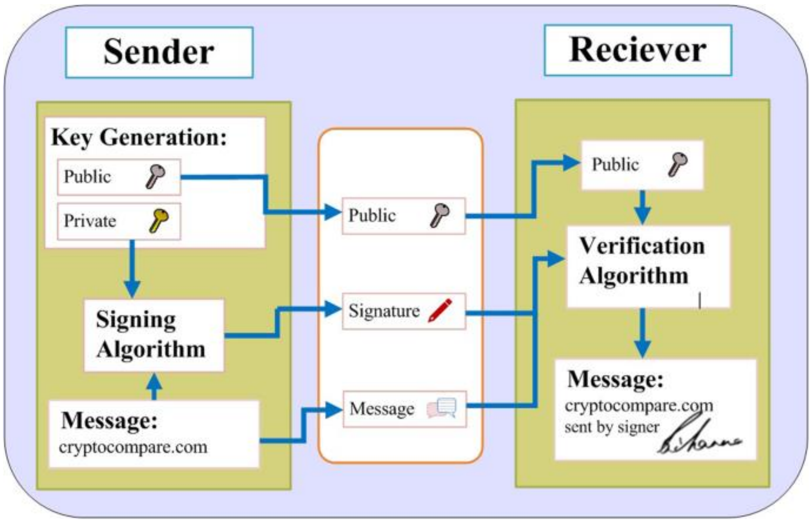

Fig1:Block Diagram Of Group Signature Scheme

It's crucial to remember that while group signatures provide considerable privacy and anonymity benefits, they also pose difficulties, such as maintaining a secure revocation procedure and guarding against collusion among group members. To overcome these difficulties and prepare group signature schemes for practical applications, such as privacy-preserving authentication, secure e-voting systems, and anonymous access control systems, researchers are always working to improve and refine them.

4. Conclusion and Future Work:

4.1 Conclusion :

The suggested group signature technique is a secure scheme based on the assumption of a key generation and verification using Python Programmin Language. The suggested technique is shown to be resistant to colluding attacks, such that neither the group manager nor any set of group members can produce a valid signature on behalf of a group member.

4.2Future Work:

the cost of signature verification is higher than that of other standard signature schemes, on the security front, this scheme is very safe against many active attacks and can be very useful in an organisation, where the group manager can be equivalent to the chief executive officer, the signers can be employees of the organization, and the verifier can be a specific customer. This approach can also be used in e-voting, e-cash, and e-commerce applications.

5.References:

1Amadeo M, Campolo C, Molinaro A. Information-centric networking for connected vehicles: a survey and future perspectives. *IEEE Commun Mag*. 2016; **54**(2): 98-104.

2.Jakubiak J, Koucheryavy Y. State of the Art and Research Challenges for VANETs. In: IEEE Consumer Communications and Networking Conference; 2008.

3.Qian Y, Moayeri N. Design of secure and application-oriented VANETs. Paper presented at: Proceedings of the Vehicular Technology Conference; 2008:2794–2799; VTC Spring, IEEE.

4.Bauza R, Gozalvez J, Sanchez-Soriano J. Road traffic congestion detection through cooperative vehicle-to-vehicle communications. Paper presented at: Proceedings of the 2010 IEEE 35th Conference on IEEE Local Computer Networks (LCN); 2010:606–612.

5..Karagiannis G, Altintas O, Ekici E, et al. Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Commun Surv Tutor*. 2011; **13**(4): 584-616.

6. Camenisch. Efficient and generalized group signatures. volume 1233, pages 465–479. Springer-Verlag, 1997.

7.D. Chaum and e. Hyest group signature .lecture notes on computer science 547(8):257-265, 1991.

8. El Bansarkhani. R and Misocki. R .,2018, April . G- Merkle : A hash based group signature scheme from standard assumptions. In *International Conference on Post- Quantum Cryptography (pp.441-463). Cham: Springer International publishing.*

*9.*Teh Je Sen, MostsumAlawida, and Jia Jie Ho. “Unkeyed hash function based on chaotic sponge construction and fixed-point arithmetic.” *Nonlinear Dynamic* 100, no.1(2020):713-729.

10. Binti Suhaili, S. and Watanbe,T., 2017, November . Design of high- throughput SHA-256 hash function based on FPGA. In 2017 6th International conference on Electrical Enginneering and Informatics(ICEEI)(pp. 1-6). IEEE.