# A Verifiable Multi Secret Sharing Scheme

*A B. Tech Project Report Submitted*
*in Partial Fulfillment of the Requirements*
*for the Degree of*

**Bachelor of Technology**

*by*

**Siddharth Bansal**
(200101093)

*under the guidance of*

**Prof. Sukumar Nandi**

**to the**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI**
**GUWAHATI - 781039, ASSAM**

# CERTIFICATE

*This is to certify that the work contained in this thesis entitled "**A Verifiable Multi Secret Sharing Scheme**" is a bonafide work of **Siddharth Bansal** (**Roll No. 200101093**), carried out in the Department of Computer Science and Engineering, Indian Institute of Technology Guwahati under my supervision and that it has not been submitted elsewhere for a degree.*

Supervisor: **Prof. Sukumar Nandi**

Professor,

May, 2023 — Department of Computer Science & Engineering,

Guwahati. — Indian Institute of Technology Guwahati, Assam.

# Acknowledgements

I express my gratitude to Prof. Sukumar Nandi and Mr. Saurav Gupta, my supervisor, for their indispensable direction, assistance, and steadfast motivation during the project. Their expertise significantly aided my exploration of Secret-sharing and related algorithms.

I extend my appreciation to the CSE department for granting me the opportunity to undertake this B.Tech Project and for fostering a favorable learning setting.

I am thankful to my family, friends, and peers for their encouragement throughout the duration of this project.

Finally, I recognize the significance of the books, research papers, and online sources that played a crucial role in the development of this project.

# Abstract

*In the world of information security, key management plays a pivotal role in safeguarding sensitive data and ensuring secure communication. One fundamental aspect of key management is secret sharing, a cryptographic method that distributes a confidential piece of information among multiple entities. This technique adds an extra layer of security by necessitating collaboration for secret reconstruction. Recognizing the potential vulnerabilities in traditional secret-sharing approaches, the evolution of Verifiable Secret Sharing (VSS) has become paramount. VSS not only addresses issues of dishonesty within the sharing process but also introduces mechanisms for verifying the integrity of the shared secrets, enhancing the overall trustworthiness of collaborative cryptographic schemes. Our proposed scheme enables the detection and identification of cheating by dealers, participants, or combiners, and does not require private channels for the transfer of secrets as well making it lightweight.*

# Contents

# Chapter 1

# Introduction

In the realm of information security, the proper management of cryptographic keys is of paramount importance. However, a persistent challenge arises when determining who can be entrusted with safeguarding these keys, especially in scenarios with numerous potential custodians, none of whom can be unequivocally deemed fully trustworthy. Traditional security paradigms, relying on a single entity or a limited set of individuals to possess and protect cryptographic keys, introduce a vulnerability that secret sharing addresses.

Secret sharing transforms key management by introducing a collaborative model. Instead of concentrating the entire key in the hands of one or a few custodians, this approach divides the cryptographic key into multiple shares, distributing them among different entities. By acknowledging the practical reality that not all custodians can be fully trusted, secret sharing ensures the security of the key even if some custodians prove untrustworthy or fall victim to compromise. This distributed responsibility enhances security, providing a resilient and adaptive solution in scenarios where absolute trust in any single custodian is unattainable. Secret sharing started as a method to share one secret but has evolved to be able to share multiple secrets at once.

## 1.1 Background

### 1.1.1 Secret Sharing

In the realm of secret sharing algorithms, various methodologies have been proposed, each rooted in distinct mathematical concepts. Adi Shamir introduced the Lagrange polynomial interpolation-based scheme, forming the foundation for what is now known as Shamir's Secret Sharing [Sha79]. Other notable contributors, such as Blakley[BLA79] and Mignotte[Mig83], suggested alternative approaches based on hyperplane geometry and the Chinese Remainder Theorem, respectively. These schemes collectively fall under the umbrella of $(t, n)$ threshold secret sharing (TSS), where $n$ represents the number of authorized participants (shareholders), and $t$ signifies the minimum number of shares required to reconstruct the secret.

In a scheme for threshold secret sharing (TSS), the individual possessing the secret (referred to as the dealer) divides the secret $S$ into $n$ shares denoted as $\{s_1, s_2, ..., s_n\}$ and subsequently allocates these shares among authorized participants, each holding a single share. The critical feature of TSS lies in the requirement that the original secret $S$ can only be reconstructed when at least $t$ shares are collectively accessible. The entity responsible for combining the shares, determining the threshold number of participants, and reconstructing the secret is known as the combiner. This combiner can either be one of the participants or a distinct trusted entity. This introduces adaptability to the secret-sharing procedure.

In simple terms, TSS is a method where a dealer, possessing a secret, wants to share it among a group of participants. The group is denoted as P and consists of n members, where each member is represented as $P_1, P_2, \ldots, P_n$.

In this process, the dealer converts the secret into n shares and disperses them among participants, each receiving precisely one share. The crucial property is that any assembly of $t$ or more participants possesses the capability to accurately reconstruct the initial secret. Significantly, any subgroup of participants with fewer than $t$ members remains incapable of gaining any information about the original secret.

Participants can collaborate and combine their shares to reconstruct the secret, or they can submit their shares to a trusted third party (the combiner) for the same purpose. This ensures that the secret-sharing scheme is secure and provides a reliable mechanism for secure collaboration and reconstruction.

### 1.1.2 Verifiable Secret Sharing

Shamir's original secret-sharing scheme relies on trustworthiness from all involved parties, including the dealer, participants, and combiner. However, this trust assumption may not always hold in real-world scenarios, where the dealer may act maliciously, participants may provide deceptive shares, or adversaries may pose as the combiner to gain unauthorized access.

To address these trust-related concerns, the concept of Verifiable Secret Sharing (VSS) was introduced. This scheme enables participants to independently verify the accuracy of their shares and the overall reconstruction process, enhancing transparency and trust in the secret sharing protocol.

Building upon this, Zhao et al.[ZZZ07] extended the principles into a Verifiable Multi-Secret Sharing scheme (VMSS). VMSS incorporates mechanisms for participants to autonomously verify the entire secret-sharing process, ensuring both the shares and secrets remain secure. This advancement significantly bolsters the security of scenarios involving the simultaneous sharing of multiple secrets.

### 1.1.3 Elliptic Curve Discrete Logarithm Problem (ECDLP)

ECDLP is a security mechanism utilized to ensure the safety of a proposed scheme. This section contains a basic introduction to the topic. In ECDLP, given an elliptic curve E and two points $N_1$ and $N_2$ on the curve, the problem is to find an integer n such that n$N_1 = N_2$, and this is computationally infeasible.

The Elliptic Curve Diffie-Hellman (ECDH) protocol is an elliptic curve-based key exchange algorithm that enables two parties to independently generate a shared secret over an untrusted communication channel without explicitly exchanging the secret itself. The public parameters of ECDH are $q$, the order of the finite field $Z_q$; $a$ and $b$, constants that constitute the elliptic curve E; $G$, a point on the curve; and $H(.)$, a one-way collision-resistant hash function.

The ECDH protocol operates as follows: - The two parties choose their secret keys ($a$ for party A and $b$ for party B) and compute their corresponding public keys ($aG$ and $bG$) on the elliptic curve. - Party A sends its public key ($aG$) to Party B. - Party B sends its public key ($bG$) to Party A. - They then use their private key and the received public key to compute the mutual secret S = $a(bG) = b(aG)$.

This protocol's security relies on the computational infeasibility of the ECDLP.

## 1.2 Motivation

Verification mechanisms are crucial for secret-sharing schemes. Most Verifiable Secret Sharing (VSS) schemes enable participants to verify their shares, preventing cheating by the dealer, allowing the combiner to detect cheating by participants, and identifying cheaters through share verification. These VSS schemes assume that the combiner is honest. However, a malicious third party can impersonate the combiner and request shares from participants. If enough participants submit their shares to this fake combiner, the secret will be revealed. Multi-secret sharing schemes that have cheater detection and identification capabilities also provide combiner verification properties, but research in the field of combiner verification is limited. Kandar and Dhara[KD20] proposed a password-based authentication scheme for combiner verification. Nonetheless, this approach necessitates a trusted dealer and private channels for distributing shares, a practical limitation. This incentive prompts us to introduce a verifiable multi-secret sharing scheme designed to detect dishonest behavior across all three entities, all achieved without the reliance on private channels.

## 1.3 Organization of The Report

In this chapter, we discussed the introduction and basic outline of the secret-sharing mechanisms, including verifiable secret sharing and the Elliptic Curve Discrete Logarithm Problem.

The rest of the report is organized as follows:-

1. In Chapter 2, we discuss the previous works in Verifiable Secret Sharing and their main contributions.

2. In Chapter 3, we discuss the proposed scheme with the initialization phase and the algorithm.

3. In Chapter 4, we discuss the possible future scope of the project to be continued in the next phase.

# Chapter 2

# Review of Prior Works

Traditional secret-sharing algorithms operate under the presumption that both the dealer and all participants are trustworthy, a condition not always guaranteed. Verifiable Secret Sharing (VSS) schemes were developed to address potential dishonesty, such as incorrect share generation by a dealer or fraudulent share submissions by participants. Chor et al. [CGMA85] were pioneers in this field, introducing a VSS scheme aimed at detecting dealer cheating. This approach was subsequently refined by Harn and Lin [HL09], who expanded the framework to include cheater detection and identification for participants.

Shao and Cao [SC05] introduced an effective Verifiable Multi-Secret Sharing (VMSS) scheme, extending the YCH[YCH04] scheme. Nevertheless, this framework did not consider the potential for dealer dishonesty and heavily depended on private channels, resulting in substantial operational expenses.

Zhao et al.[ZZZ07] introduced an enhanced VMSS scheme also based on the YCH [YCH04] model, effectively addressing both the issues of dealer dishonesty and the high costs associated with private channels. Another notable contribution in this domain was made by Dehkordi and Machhadi [DM08a], who proposed a VMSS scheme incorporating the complexity of the discrete logarithm problem and the RSA cryptosystem for verification purposes. They further extended their research to include schemes based on non-homogeneous linear recursion and Elliptic Curve Cryptography (ECC) [DM08b]. The robustness of these schemes primarily hinges on the strength of the elliptic curve RSA and the complexity of ECDLP.

Endurthi et al. [ETV14] developed a VMSS scheme derived from the Asmuth-Bloom [AB83] and Mignotte [Mig83] schemes. This particular scheme is notable for allowing participants to acquire reusable multiple sets of shares, which are also verifiable for potential dealer dishonesty. The VSS scheme introduced by Kandahar and Dhara [KD20]is distinguished by its capability to verify all three entities involved in the process. However, it falls short of facilitating the simultaneous sharing of multiple secrets.

# Chapter 3

# Proposed Scheme

in this section, we propose a verifiable threshold multi-secret sharing scheme. We first provide the initial setup for the algorithm.

## 3.1 Initialization Phase

The domain parameters are:

- $q$: the order of the finite field $Z_q$
- two constants $a$ and $b$ which define the elliptic curve E
- $G$: a point on the curve
- $H(.)$: a one-way collision-resistant hash function
- $m$: the order of $< G >$ i.e. $m$ is the least positive number satisfying $m.G = O$

We consider a secure Bulletin board (SBB) as a trusted entity that is used by the entities of our proposed scheme to publish keys and other public values in an authentic manner. We have assumed the following properties for the secured bulletin board:

- All the entities in the scheme are authenticated on the SBB.

- The entities' identities are verified every time they access the SBB.
- If a participant acts as the combiner as well, they will have to register with the SBB two separate times, once as the combiner and once as a participant.

## 3.2 Algorithm

The algorithm is shown below:

1. The dealer initiates the exchange of pseudo-shares $\{x_1, x_2, x_3, ..., x_n\}$ with participants and simultaneously establishes a secret with the combiner($\phi_c$) through the ECDH protocol.
2. Subsequently, the dealer selects pseudo secrets $s_1, s_2, ..., s_n$ and conceals the actual secrets by combining them with both the pseudo secrets and the combiner's secrets, making the outcome publicly accessible.
3. The encoding of pseudo secrets into n shares involves embedding them into a function, representing the shares as points on the function. Linear interpolation enables the reconstruction of pseudo secrets from a sufficient number of shares.
4. The combiner sends a submission request for pseudo shares to participants, accompanied by a verification message to ensure the request's authenticity.
5. Participants generate secret keys for communication with the combiner using ECDH, employing these keys to mask their shares. The combiner can subsequently decode these masked values using the generated secret keys.
6. Pseudo secrets are reconstructed by the combiner from the received shares through linear interpolation. Leveraging these pseudo secrets and the combiner secret established earlier allows for the recovery of the original secrets.

# Chapter 4

# Conclusion and Future work

In this report, we introduce a threshold multi-secret sharing scheme that can be verified. The proposed scheme has the ability to detect any cheating done by the dealer, participants, or combiner and also allows for cheater identification. To ensure security, a secure bulletin board is used as a trusted authority, and all entities must be registered with it. Since every entity must access the SBB in an authenticated manner, the possibility of any man-in-the-middle attack is mitigated.

No private channel was used between participants, dealers, and combiners to transfer any pseudo-secrets/secrets. The use of ECC ensures that the scheme is computationally lightweight.

## 4.1 Future Work

Our plan is to implement the proposed algorithm in order to determine the actual time complexities of each step. Additionally, we will attempt to verify the proposed verifiability of the entities by examining scenarios where cheating is perpetrated by the dealer, participants, or the combiner.ng.

# References

[AB83] Charles Asmuth and John Bloom. A modular approach to key safeguarding. *IEEE transactions on information theory*, 29(2):208–210, 1983.

[BLA79] G. R. BLAKLEY. Safeguarding cryptographic keys. In *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318, 1979.

[CGMA85] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)*, pages 383–395, 1985.

[DM08a] Massoud Hadian Dehkordi and Samaneh Mashhadi. An efficient threshold verifiable multi-secret sharing. *Computer Standards  Interfaces*, 30(3):187–190, 2008.

[DM08b] Massoud Hadian Dehkordi and Samaneh Mashhadi. Verifiable secret sharing schemes based on non-homogeneous linear recursions and elliptic curves. *Computer Communications*, 31(9):1777–1784, 2008.

[ETV14] Anjaneyulu Endurthi, Appala Naidu Tentu, and V Ch Venkaiah. Reusable multi-stage multi-secret sharing scheme based on asmuth-bloom sequence. *International Journal of Computer Applications*, 975:8887, 2014.

[HL09] Lein Harn and Changlu Lin. Detection and identification of cheaters in (t, n) secret sharing scheme. *Designs Codes and Cryptography*, 52:15–24, 07 2009.

[KD20] Shyamalendu Kandar and Bibhas Chandra Dhara. A verifiable secret sharing scheme with combiner verification and cheater identification. *Journal of Information Security and Applications*, 51:102430, 2020.

[Mig83] Maurice Mignotte. How to share a secret. In Thomas Beth, editor, *Cryptography*, pages 371–375, Berlin, Heidelberg, 1983. Springer Berlin Heidelberg.

[SC05] Jun Shao and Zhenfu Cao. A new efficient (t,n) verifiable multi-secret sharing (vmss) based on ych scheme. *Applied Mathematics and Computation*, 168(1):135–140, 2005.

[Sha79] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[YCH04] Chou-Chen Yang, Ting-Yi Chang, and Min-Shiang Hwang. A (t,n) multi-secret sharing scheme. *Applied Mathematics and Computation*, 151(2):483–490, 2004.

[ZZZ07] Jianjie Zhao, Jianzhong Zhang, and Rong Zhao. A practical verifiable multi-secret sharing scheme. *Computer Standards  Interfaces*, 29(1):138–141, 2007. ADC Modelling and Testing.