Pseudorandom Secret Sharing With QR Codes

Ilayda Dogan   
Department of Computer Engineering  
*Faculty of Engineering , Dokuz Eylul University*Izmir , Turkiye  
ilay.dogannn@gmail.com

*Abstract*— This paper investigates the integration and implications of Pseudo-Random Secret Sharing (PRSS) in cryptographic applications, focusing on improving security measures in secret sharing algorithms. PRSS offers a new approach by incorporating pseudo-random values into traditional secret sharing, aiming to strengthen the confidentiality of shared secrets in various scenarios. Additionally, this document examines the theoretical foundations and various application areas of the Secret Sharing approach. A secret can be securely divided into pieces using a cryptographic technique known as "Secret Sharing" and these pieces can then be given to trusted others. The Secret Sharing method is discussed in this document along with its various applications.

# Introduction

Information security has long relied on the discipline of cryptography. In many application domains, information security and secrecy are crucially important. As sensitive data and information are now routinely shared and kept electronically in the digital era, guaranteeing its security and secrecy has taken on a crucial role.

A essential requirement for individuals, companies, and governments alike is safeguarding personal data from unwanted access or disclosure. Sensitive information must be shielded from unwanted access in financial organizations, military systems, the healthcare sector, and many other domains. It's necessary to reduce the risks that could result in single points of failure in order to ensure the security of such data. Despite their effectiveness, traditional information security measures like encryption are not impenetrable because they frequently rely on a single key or password. This has led to a growing requirement for safe secret keeping and disclosure. This restriction begs the question: What happens when more than one person or organization is required to jointly protect information for which no one party has sole responsibility? As a cryptographic approach created to address this need, the Secret Sharing method is crucial.

A secret (such as a password or key) is securely divided into parts using the encryption technique known as "secret sharing," which has roots in the middle of the 20th century. The secret is then required to be restored by sending the secret's pieces to various devices or individuals. The original secret cannot be replicated until a certain amount of shares are merged. With this strategy, it is unnecessary for one organization to own the complete secret, enhancing security and lowering the possibility of unauthorized access. Take a bank account key as an illustration. If this key is kept by a single person, there is a significant security risk in the event that person loses access for any reason or maliciously uses it. However, through Secret Sharing, this key is broken up into bits and given to various people we trust, one piece at a time. A specific amount of these pieces must be put together in order to restore the key. This prevents a mistake or malicious activity from jeopardizing the entire system at a single location.

Since its origin, the idea of secret sharing has undergone tremendous development and found multiple uses in numerous industries. It was initially developed as a means of safe data storage, but it has since been applied to secure communications, access control, digital signatures, and even voting systems based on cryptography. Because of its adaptability, confidential sharing is a useful tool in the always changing information security environment.

A secret (such as a password or key) is divided into pieces and distributed to various people or entities using the Shamir's Secret Sharing cryptographic technique. In order to divide a secret into parts, numerous pieces are formed, and any of these pieces must reach a specified threshold value before they may view the others or reconstruct the secret. This algorithm has 3 basic steps.

Making a polynomial based on how many people the secret's owner wishes to share it with is the first stage. The threshold value and this polynomial's degree are both determined. Parts of the secret are formed in the second stage by the values of various points from the generated polynomial. The owner of the secret grants these points to other individuals or groups. Finally, those seeking to obtain the secret gather an adequate number of secrets to reach the limit imposed by the secret's owner. This information is gathered by utilizing Lagrange interpolation or similar technique.

Multiple security measures are offered by Shamir's Secret Share. One person cannot restore the secret even if they obtain it, for instance, if a secret requires the merging of at least three persons. This can be used for a variety of purposes, including safely exchanging encryption keys or safeguarding information. This protocol is utilized in a wide range of application domains and plays a significant role in the fields of cryptography and information security. Shamir's Sharing Secret's fundamental concepts are widely applied in industries including cybersecurity, data security, and safe multiparty computing.

# Related works on secret sharıng

## Proactive Secret Sharing Scheme Suitable for Asymmetric Secret Sharing Scheme

Because it generates up to k-1 shares from a single key belonging to the secret owner, an asymmetric secret sharing scheme (A-SSS) can limit the number of servers to fewer than k. Thus, even in the event that every server is compromised, the secret remains hidden. Shares could, however, leak if the owner's key is taken and compromised. Consequently, a proactive secret sharing plan appropriate for an A-SSS is proposed in this work. Comparing this system to traditional proactive secret sharing techniques, a significant decrease in communication volume is achieved.

This work addresses a proactive secret sharing method that is suggested in line with an asymmetric secret sharing scheme that was created for usage in secure cloud systems. The utilization of a key chosen by the owner of the secret information allows for the implementation of asymmetric secret sharing schemes. In order to prevent the disclosure of all secret information, the plan put out in this study makes sure that the secret key is split, saved, and then combined as needed. The study discusses a scenario in which shares could be compromised if the owner of the secret's key is lost, stolen, or compromised. A proactive secret sharing plan appropriate for an asymmetric secret sharing scheme (A-SSS) is suggested as a solution to this problem. This preemptive plan provides a framework that can greatly lower communication traffic and boost security. The study highlights that, in comparison to conventional proactive secret sharing schemes, the suggested scheme reduces communication volume and boosts security. This plan offers a fresh method of reducing security risks in cloud systems while addressing current worries about data security and privacy. The proactive secret sharing strategy proposed by Herzberg and popular secret sharing schemes like Shamir's scheme are reviewed and contrasted in this paper. According to the statement, Herzberg's approach has some security flaws and a higher communication volume growth. According to the study, this proactive secret sharing strategy that has been suggested is a significant step in lowering communication traffic and resolving security issues with cloud systems. The purpose of this study was to increase public awareness of data security and aid in the creation of safe cloud computing infrastructure.

## Boolean-Based Multi Secret Sharing Scheme Using Meaningful Shares

Meaningless shares, which resemble noise, are created by encoding a secret image using the classic visual secret sharing (VSS) scheme. Sharing numerous secret images with multiple secret sharing (MSS) schemes increases the sharing capability of VSS schemes. The application of a universal commonality shared by all participants in MSS programs constitutes diversity. Making relevant posts to lower the suspicion when sharing hidden photographs is a recent trend in MSS systems. However, this technique is ineffectual for the CNS due to the low visual quality of relevant postings. A Boolean-based MSS system is suggested in this study to enhance the meaningful postings' visual quality. Using n+1 cover images, the suggested approach encodes n grayscale secret images into a meaningful universal share and n meaningful shares. N number of hidden photos are recovered using a boolean XOR method. The suggested method's efficiency is demonstrated by the experimental findings.

In order to share secret information, a new encryption system called Boolean-based multiple secret sharing scheme is introduced in this work. With this new scheme, the authors of the study concentrate on creating a more efficient and secure sharing system by solving the shortcomings of current privacy technologies. The first section of the study discusses the drawbacks and restrictions of conventional visual secret sharing (VSS) techniques. He underlines that these tactics frequently result in sharing that is meaningless and noise-like and lower the appearance of secret information. The various secret sharing (MSS) systems that have been created to get around these drawbacks are then covered. He claims that these designs' significant posts don't have enough visual appeal, nevertheless. The paper suggests a novel Boolean-based MSS approach to address these issues and enhance the significance of posts' visual appeal. By evenly integrating cover and private photographs into posts, the suggested technique enhances the visual appeal of postings. It seeks to enhance the visual experience while safeguarding the security and privacy of shared photos in this way. The study also compares the suggested strategy with other schemes of a similar nature in order to examine it. This comparison demonstrates that the suggested strategy outperforms the other alternatives in terms of visual quality and meaningful share production. The great degree of similarity between encrypted and unencrypted photos lends more credence to this. Therefore, the study can be seen as a crucial step towards creating a new multiple secret sharing scheme and fixing the flaws in the ones that now exist. By attempting to improve the visual experience while preserving the security and privacy of shared information, the suggested strategy advances research in this area.

## Multi Secret Sharing Based on Hill Cipher and Blakley Secret Sharing

This work uses Blakley secret sharing and the Hill cipher to present a multi-secret sharing technique. With one or more shadow images, the suggested approach can reconstruct k-secret images. We compare the suggested approach for grayscale images with a (n, n)-threshold with existing relevant visual secret sharing schemes. In comparison with the other work, the threshold is lowered to (k, n) by the suggested technique. Additionally, the suggested strategy uses the Hill Cipher algorithm to share several secrets without relying on a random grid that is used as a share picture in another work scheme. using no pixel enlargement and lossless picture recovery, sharing more than one secret image using Hill Cipher and Blakley improves the security of those photos. The scheme's efficiency is demonstrated by the experimental findings.

This study presents a novel top secret sharing technique based on a hybrid of Blakley secret sharing and Hill cipher. With just a small number of shadow images, the suggested system can reconstruct many secret images, offering a high degree of security. The lowered threshold requirement and enhanced security of the suggested methodology are positioned it as an advance over earlier methods. It gives a thorough explanation of the sharing and recuperation phases of the plan and emphasizes the benefits of the suggested strategy over earlier strategies. According to study findings, several secret photos can be successfully shared and recovered without any pixel enlargement. The paper offers a thorough and organized analysis of a brand-new top-secret sharing plan that combines two well-known encryption methods. By offering important details on the conception, execution, and assessment of the suggested system, it significantly advances the fields of secure information transfer and cryptography. This work presents a multiple secret sharing technique. This plan makes use of Blakley secret sharing and Hill encryption. The suggested plan is limited to reconstructing mean-latent images that have one or more average shadow images. The suggested plan has lowered the threshold value and been compared to other pertinent visual secret sharing plans for grayscale photos. Furthermore, instead of depending on a random grid to serve as the sharing image for a different business plan, the suggested technique uses the Hill Cipher algorithm to communicate additional secrets. Multiple secret photos can be shared using Hill Cipher and Blakley, which increases the security of secret images while achieving lossless image recovery with no pixel enlargement. The scheme's efficiency is demonstrated by the outcomes of the experiments. The security is improved by the plan this study presents. Secrecy and protection of secret photos were further ensured by the use of Blakley secret sharing and Hill encryption. The plan avoids pixel inflation in shared photographs while offering safe multi-secret sharing. Furthermore, it provides acceptable quality in terms of qualities related to diffusion and confusion. Future developments in this area of study could lead to the development of less computationally complex methods for enhancing the security of multi-image secret sharing. It is also possible to investigate how well this strategy works with color photographs.

## QR Shares Based Secret Sharing Scheme Using DWT, Random Permutation and Arithmetic Modulo Operation for QR Secret

Because of its shared images that resemble noise, the conventional method of sharing secret images through Secret Image Sharing (SIS) has grown more vulnerable to malevolent individuals. Hence, it is imperative to explore novel methodologies that offer a secure means of disseminating covert photos as significant shares. In order to achieve this, scholars have been investigating various encryption techniques, safe communication protocols, and intricate patterns for exchanging secrets in meaningful ways that can impede identification by malevolent actors. With the use of the Discrete Wavelet Transform (DWT), Random Permutation (RP), and Arithmetic Modulo (AM) operation, this suggested method presents a secret sharing strategy based on QR shares. The suggested (n, n) perfect secret sharing system is computationally efficient due to its lightweight operations, and it only needs n shares to reconstruct the secret. Since malicious attackers cannot reverse or restore the data, this technique offers a high level of protection even though it might not be the most robust. The testing findings show that the suggested approach yields higher-quality QR shares and a visually superior, lossy-natured restored QR secret. When the scheme's performance is assessed using metrics like correlation, RMSE, PSNR, NPCR, and UACI, it performs better for QR secrets. The topic of this study is secret sharing systems based on QR codes. Due to its many benefits, including their quick reading speed, error correction capability, and capacity to represent a large range of data types, QR codes have gained popularity in recent years. The goal of this research is to offer a safe way of distribution that can turn personal photos into valuable exchanges. Making secret photos into insightful posts makes it more difficult for hostile people to decrypt and comprehend the images. The suggested method makes use of the Random Permutation (RP), Arithmetic Modulation (AM), and Discrete Wavelet Transform (DWT) operations. Images can be transformed into secret shares and the secret image can be recreated using these processes. In essence, the hidden image is used to create QR codes, which are then transformed into shares that have meaning. This procedure guarantees meaningful communication while safeguarding sensitive information. In contrast to earlier research, the proposed method is more computationally efficient and lighter. Because of its lossy character, this method results in better quality sharing of QR codes and QR secret data with greater visual quality.The report also mentions earlier research in the areas of hidden picture sharing and QR codes. Many of these research' shortcomings and merits are also covered. It is highlighted that the suggested method performs better and provides answers to these drawbacks. Statistical analysis and experiments are also included in the paper. These analyses show the performance of the suggested method on real data and its comparison with other similar studies. These analyses demonstrate that, for QR secret shares, the suggested strategy works better and yields better results.

## Verifiable Image Secret Sharing with Cheater Identification

The cryptographic technique for communicating private information is called secret sharing. N participants, resulting in N as the total number of participants. Participants must assemble in huge numbers in order to divulge any one of the k secrets. When it comes to secret sharing, it's generally accepted that both the participants who receive the secret shares and the seller who divides and distributes them in secret are sincere. They promise not to act inappropriately or dishonestly. In the actual world, nevertheless, it might be conceivable for participants and the dealer to cheat. During the restructuring, the participant may offer the incorrect share, or the dealer may offer the incorrect share to the participant. Verifiable secret sharing is therefore required, as is the identification of the cheater. We offered a novel method for identifying and verifying image secret sharing cheaters in our suggested work. It is a generic scheme that may be used with any scheme for sharing secret images. There have been four distinct secret sharing schemes tested through experiments. The outcome of the experiment demonstrates that the suggested method is effective in confirming image secret sharing and spotting fraud. Shares by themselves are useless. There are N participants and one dealer in the covert sharing plan. Participants receive shares that the seller issues to them once hidden shares are created, but only under specific circumstances. This study presents a novel method for sharing private data. In essence, the paper suggests a way to exchange private information safely. This approach seeks to protect against and identify potential fraud scenarios when exchanging sensitive information. The process of breaking up private information into smaller chunks and giving it to various individuals is known as "secret sharing." It is possible to reconstitute private information by piecing these parts together. On the other hand, dishonesty and fraud could happen throughout this procedure. To guard against such frauds, the paper discusses the ideas of "verifiable secret sharing" and "scammer identification." One technique to make sure participants are comfortable with the accuracy of supplied data is verified confidential sharing. On the other hand, fraud identification looks for participant deception in order to safeguard the accuracy of shared data. The study looks at earlier research on this topic that has been done in the literature and talks about its shortcomings and achievements. It is specifically highlighted how the suggested approach addresses these drawbacks and what benefits it offers over current approaches. The suggested approach has been tested with several secret data sharing methods and has been demonstrated to function well with a variety of image formats, including color images. Furthermore, MATLAB platform studies have demonstrated the efficacy and dependability of the suggested approach.

The following succinctly describes the main points of the study's solution:

Verifiability of Shares: Every share is verified through the use of the MD5 algorithm. By generating a distinct hash for every post, this technique guarantees the precision and consistency of every one.

Cheater Identification: The algorithm is able to identify the fraudster if one or more of the posts are erroneous or cannot be validated. This makes it possible to identify the fraudster and identify any fraudulent attempts made during the transfer of personal data.

Support for Color Images: The suggested solution is capable of handling several image formats, including color images. This demonstrates that there are more applications for private data sharing than just sharing black-and-white photos.

General Applicability: Any private data exchange algorithm can be used with the study's solution. This guarantees the solution's broad applicability and usability in various circumstances involving the sharing of confidential data.

# Project Detaıl

Pseudo-random secret sharing (PRSS) is a method designed to increase security by adding random values to traditional secret sharing algorithms. This approach aims to make the secret sharing system more resistant to certain security attacks. Let's talk about the usage scenarios and advantages of PRSS.

I) Security Reinforcement:

PRSS can make some attacks difficult against information theory-based secret sharing algorithms, thanks to random values added to the shared secrets. This provides an additional layer of security, especially for situations such as "active attacks".

II)Crypto-Analysis Resistance:

Although secret sharing algorithms are built on mathematical foundations, they may be subject to attacks from crypto-analysts due to the random numbers used or certain features of the algorithms. PRSS may provide additional resistance to such analysis.

III)Privacy Protection:

Adding random values can make it difficult to attribute shares to previous values. This can contribute to more secure protection of shared secrets and ensure confidentiality.

IV)Use in Security Protocols:

PRSS can be integrated to increase security by using it in multiparty security protocols or distributed systems. For example, by using it in multi-participant crypto protocols, it can contribute to making shares more secure in case of an error or attack in the protocol.

V)Second Layer Security:

PRSS can be used as an additional layer of security in cases where the basic secret sharing algorithm is insufficient in terms of security. Thus, even if the first layer algorithm security is compromised, the second layer (random value addition) can protect the system.

metin, ekran görüntüsü, diyagram, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu

Fig. 1: Design Scheme of Project

##### tests Results of project

1. Checking The Accuracy of The Secret:

Scenario: A specific secret is created and divided into shares.

Test: Combining the shares to obtain the original secret.

Expected Result: The resulting secret should be equal to the original secret.

metin, ekran görüntüsü, yazı tipi, sayı, numara içeren bir resim

Açıklama otomatik olarak oluşturuldu

Fig. 2: Checking The Accuracy of The Secret Table

1. Experiment with Different Sharing Numbers:

Scenario: Sharing the secret using different number of shares.

Test: Checking the accuracy of the secret by changing the number of shares.

Expected Result: In all cases, the secret is shared correctly.

metin, ekran görüntüsü, yazı tipi, sayı, numara içeren bir resim

Açıklama otomatik olarak oluşturuldu

Fig. 3: Experiment with Different Sharing Numbers Table

C. Creating and Reading QR Codes:

Scenario: QR codes are created for each shared and merged secret.

Test: Reading the generated QR codes and checking the data they contain.

Expected Result: Each QR code contains the correct data.

Example Test Result:

Share Number: 3

Original Secret: 121314

Generated Shares: [72849829242927097159252216673239543687586326520540555189471767432729055389113, 101439742920415855365274484743805339717577175607580167098198107629459001965153, 29533447971840188450912014000238358383525511969190136790393279295990961194554]

Combined Secret: 121314

Secrets match! Success.

kalıp, desen, düzen, kare, simetri, bakışım, piksel içeren bir resim

Açıklama otomatik olarak oluşturuldu

Fig 4: Share 1

kalıp, desen, düzen, kare, piksel, tasarım içeren bir resim

Açıklama otomatik olarak oluşturuldu

Fig 5: Share 2

kalıp, desen, düzen, kare, simetri, bakışım, sanat içeren bir resim

Açıklama otomatik olarak oluşturuldu

Fig 6: Share 3

kalıp, desen, düzen, kare, simetri, bakışım, dikdörtgen içeren bir resim

Açıklama otomatik olarak oluşturuldu

Fig 7 : Combined Secret and Original Secret

##### Conclusion

The use of Pseudo-Random Secret Sharing (PRSS) is emerging as a pioneering approach to strengthen the security posture of traditional secret sharing algorithms. By introducing pseudo-random values into the sharing process, PRSS contributes to preventing possible attacks, improving privacy protection, and increasing the overall robustness of cryptographic protocols.

This project can be used in many places in daily life.

a) Sharing of Confidential Information: For example, a person who has critical information within a company wants to share this information with other colleagues only under certain conditions. This project allows secure sharing of information by dividing it into random shares.

b) Access Control: Situations where the contribution of more than one person is required for a group of people to perform a certain operation on a system. For example, different employees may be needed to open a bank vault. This project provides a secure access control mechanism for such situations.

c) Secure Data Transfer: This project can be used for situations that require secure data transfer. For example, shares can be created to securely transfer a private key to another device.

The project's implementation and testing results confirm the effectiveness of PRSS in achieving its goals. As the digital environment continues to evolve, the importance of innovative cryptographic methods becomes increasingly evident. PRSS represents a forward-looking solution that adapts to the dynamic nature of information security, demonstrating the potential for widespread adoption in a variety of applications. The successful integration of PRSS underscores the need for continued advances in cryptographic techniques, especially in the context of secret sharing. This report serves as a testament to the effectiveness and versatility of PRSS, offering a promising avenue for further research and application in the ever-changing information security landscape.

##### References

[1] A. Shamir, "How to Share a Secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[2] N. Kaneko and K. Iwamura, "Proactive Secret Sharing scheme suitable for asymmetric secret sharing scheme," in 2016 IEEE 5th Global Conference on Consumer Electronics.

[3] V. J. Kapadiya, L. S. Desai, and Y. K. Meghrajani, "Boolean-based Multi Secret Sharing Scheme using Meaningful Shares," in 2018 Second International Conference on Inventive Communication and Computational Technologies, 2018.

[4] A. A. Mervat, O. S. Younes, and H. S. Abdul-Kader, "Multi secret Sharing Based on Hill Cipher and Blakley Secret Sharing," in 2017 27th International Conference on Computer Theory and Applications, 2017.

[5] A. S. Rawat, M. Deshmukh, and M. Singh, "QR Shares based Secret Sharing Scheme using DWT, Random Permutation and Arithmetic Modulo Operation for QR Secret," in 2023 10th International Conference on Signal Processing and Integrated Networks, 2023.

[6] S. D. Patil and P. K. Ithape, "Verifiable Image Secret Sharing with Cheater Identification," in 2018 Second International Conference on Inventive Communication and Computational Technologies, 2018.

[7] R. Cramer, I. Damgård, and Y. Ishai, "Share conversion, pseudorandom secret-sharing and applications to secure computation," in Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2, pp. 342-362, Springer Berlin Heidelberg, 2005.

[8] F. Benhamouda, E. Boyle, N. Gilboa, S. Halevi, Y. Ishai, and A. Nof, "Generalized pseudorandom secret sharing and efficient straggler-resilient secure computation," in Theory of Cryptography: 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8–11, 2021, Proceedings, Part II, pp. 129-161, Springer International Publishing, 2021.

[9] A. Mayer and M. Yung, "Generalized secret sharing and group-key distribution using short keys," in Proceedings. Compression and Complexity of SEQUENCES 1997 (Cat. No. 97TB100171), pp. 30-44, IEEE, June 1997.

[10] M. Cerecedo, T. Matsumoto, and H. Imai, "Shared Pseudo-Random Secret Generation Protocols," in IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, vol. 77, no. 4, pp. 636-645, 1994.