On Threshold secret sharing schemes with primary classes

Cenap Ozel[1] and Hanifa Zekraoui[2]

[1]Department of Mathematics, Faculty of Science,King Abdulaziz University, Kingdom of Saudi Arabia
[2]Department of Mathematics, Faculty of Exact Sciences and SNV, University of Oum El Bouaghi, Oum El Bouaghi, Algeria.

E-mail: cozel@kau.edu.sa[1], hzekraoui421@gmail.com[2]

Abstract

The aim of this paper is to study some specific classes of Threshold schemes. Our study is based on modular arithmetic and equivalence classes modulo a prime number. For this purpose we construct a secret sharing scheme by using these classes. This scheme is efficient by means of security.

2020 Mathematics Subject Classification. **94A62**. 11F06, 03E99, 37A99.
Keywords. Threshold secret sharing scheme, equivalence relation, equivalence classes modulo a prime.

1 Introduction

Highly sensitive and important information needs the cryptographic protocol of secret sharing to keep it confidential. In a secret sharing scheme there are some participants and a dealer. The dealer has a secret and dsitributes it to participants such that a minimal $t-$ subset of participants can recover the secret while combining their shares. These subsets are called the minimal access sets [5]

Secret sharing schemes were envented by Blakley [3] and Shamir [11] in 1979. A $(t;n)-$threshold secret sharing scheme is a method of the distribution of information among n participants such that $t>1$ of them can reconstruct the secret while $(t-1)$ participants cannot.

Shamir's scheme is a $(t;n)-$ secret sharing scheme. This scheme was based on polynomial interpolation and then Mc Eliece and Sarwate were obtained an application of Massey scheme, a scheme based on codes [9][, to Reed-Solomon Codes [8].

Blakley's scheme is also a $(t;n)-$ threshold scheme. It was based on finite geometry [1]. This scheme uses hyperplane geometry as a solution of the secret sharing problem.

Secret sharing schemes have been applied to different areas. Some of them are Information Security, Threshold Cryptography, Key Recovery Mechanism, Information Hiding, Electronic Voting and many others [1] [10], [7]. Another $(t;n)-$ threshold secret sharing scheme was created by Asmuth and Bloom [2]. Their scheme was based on the Chinese Remainder Theorem.

In the present work, we present an $(n;n)-$ threshold scheme based on the equivalence classes of primes over $\mathbb{Z}$. Since the construction of our scheme is based on a finite field, it is very reliable in terms of security. Because in a finite field, the size of a such number stays in a specified range , no matter how many operations we apply to the number. So finite fields are more suitable to explain a crypto application.

We suppose that the reader is familiar with sets, equivalence relation, classes modulo a natural number and some basic notions of group theory.

The paper is organized as follows. In Section 2, we present the new threshold secret sharing scheme and explain its security while in Section 3 we conclude our work.

Advanced Studies: Euro-Tbilisi Mathematical Journal 17(4) (2024), pp. 33–37.
DOI: 10.32513/asetmj/1932200824037

Tbilisi Centre for Mathematical Sciences.

Received by the editors: 13 June 2024.
Accepted for publication: 30 September 2024.

In a finite abelian group, by regrouping elements and their inverses together (xx^{-1} in case of multiplication and $x + (-x)$ in case of addition), we can obtain the following proposition:

Proposition 1.1. Let G be a finite abelian group of order n and let x_1,..., x_k be all elements in G which are equal to their inverses for some $k \leq n$. Then the combination of all elements in G is equal to the combination of the mentioned elements.

For example, the sum of all elements in $\mathbb{Z}_4$ is 2, in $\mathbb{Z}_6$ the sum is equal to 3. While the sum of all elemnts in $\mathbb{Z}_p$ vanishes, for some prime number p. In fact, there is no element in $\mathbb{Z}_p$ equal to its inverse, because if there exists an x which is its own inverse, then we get $x = p - x$ which yields to $p = 2x$, even number, while p is supposed to be a prime.

In view of Proposition 1.1 and the last explanation, we get the following result:

Corollary 1.2. For any prime number p, we have

$$\sum_{i=1}^{p-1} i \equiv 0 \, mod \, p. \tag{1.1}$$

2 Secret sharing schemes

Hiding the secret information is very important. Thus the secret sharing schemes are improved. The main problem is to divide the secret into pieces instead of storing the whole for a secret sharing. These schemes play an efficient role for several secure records. Some of them are threshold cryptography, attribute-based encryption, access control [4]. We should have the following notations to define secret sharing schemes:

- The secret could be a password, a chemical formula, or any private information.
- The dealer who selects the secret and distributes it among participants.
- Shares which are pieces of the secret information. The eligible group of shares can reach the secret and the other group of shares cannot.
- The participants who receive the secret shares.
- The access structure is the set of all minimal coalitions sets. The elements in this set are the competent associations of participants whose shares can recover the secret.

In a secret sharing scheme there are two fundamental grades:

i) Distribution: The secret is broken into N pieces $x_1, ..., x_N$ that are privately delivered to the participants.

ii) Reconstruction: The secret can be retrieved by using a special method for a suitable set of shares.

3 The scheme

3.1 Scheme description

In this section, we present a $(n; n)-$ threshold scheme based on the set of equivalence classes of a prime over $\mathbb{Z}$. We need the approximation space $(\mathbb{Z}, \sim)$.

- Let the approximation space $(\mathbb{Z}, \sim)$ be the secret space.
- Let our modulo be a prime $p \geq 5$. So we work on the field $\mathbb{F}_p$. it is our public set.

1) Secret Distribution:

- First the dealer pics a secret s from $\mathbb{F}_p^{\times} = \mathbb{F}_p - \{0\}$ (i.e. the multiplicative group).
- Then he distributes it over a secure channel to each participant P_j, where $1 \leq j \leq p-1$.

2) Secret Recovery: In view of Corollary 1.2, the participants can retrieve the secret by forming the sum $\sum_{j=1}^{p-1} x_j = 0$ where the sum of entries is taken by modulo p. Actually, we are recovering the secret by representatives of equivalence classes. We choose a random element from each of equivalence class to obtain the secret.

Theorem 3.1. Our scheme satisfying above conditions meets the following requirements:
i) The access structure consists of the equivalence classes of the prime p.
2) The size of access structure is $p-1$.

Proof. 1) Since the secret is reconstructed by representatives of equivalence calasses of a prime, the proof is clear.

2) In this scheme we are working on $\mathbb{F}_p$ and the order $|\mathbb{F}_p|$ as a group is $= p$: Any element of $\mathbb{F}_p^{\times}$ can be the secret. Moreover, we need the remaining $p-1$ elements to reach the secret. So the size of access structure is $p-1$. Q.E.D.

Theorem 3.2. This new scheme is also a $(p-1; p-1)-$ threshold secret sharing scheme.

Proof. The participants are elements of ${\mathbb{F}_p}^{\times}$. Hence $p-1$ elements of $\mathbb{F}_p$ (except the secret) can recover the secret together. Thus the new scheme is a $(p-1; p-1)-$ threshold secret sharing scheme. Q.E.D.

3.2 Statistics on coalitions

Theorem 3.3. In the new secret sharing scheme based on equivalence classes of a prime over $\mathbb{Z}$, the number of minimal coalitions is $p-1$.

Proof. A minimal coalition is a set of participants. The participants are elements of $\mathbb{F}_p^{\times}$, their number is $p-1$. The secret is any element of ${\mathbb{F}_p}^{\times}$. The remaining $p-2$ elements can recover the secret. So the number of minimal coalitions of this scheme is $\binom{p-1}{p-2} = \frac{(p-1)!}{(p-2)!} = p-1$. Q.E.D.

3.3 Security analysis

Assume that $h-(p-1)$ users have to guess the secret amongst $h+(p-1)$, where $h > p-1$. The probability of success of such an attack is $\prod_{i=1}^{h} \frac{1}{(p-1)+i}$. We have chosen $p \geq 5$ for our scheme. If $p < 5$, then it would be the worst case for security since it maximizes the probability of success. So it is clear that $h \geq 5$. If p is big enough, then this quantity can be made arbitrary small.

Another possible attack would be to isolate the other representative elements of ${\mathbb{F}_p}^{\times}$ which leads to recovering the secret. It is very difficult to guess them since it is chosen randomly. The scheme based on $\mathbb{F}_p$ is appealing against cheating and this scheme is more resistant to algebraic attacks in view of the reconstruction algorithm.

3.4 Information theoretic efficiency

If the size of the shares of all participants are less than or equal to the size of the secret, then this secret sharing scheme is said to be ideal. If a secret sharing scheme satisfies the following situations, then it is called perfect scheme:

- All eligible coalitions can obtain the secret and
- unskilled coalitions acquire no information about the secret [12]. So our scheme is both ideal and perfect.

Example 3.4. . We consider $p = 7$. Let us write the representatives set for each equivalence class.

$$\begin{aligned}
[0] &= \{..., 0, 7, 14, 28, ...,\} \\
[1] &= \{..., 1, 8, 15, 29, ...,\} \\
[2] &= \{..., 2, 9, 16, 30, ...,\} \\
[3] &= \{..., 3, 10, 17, 31, ...,\} \\
[4] &= \{..., 4, 11, 18, 32, ...,\} \\
[5] &= \{..., 5, 12, 19, 33, ...,\} \\
[6] &= \{..., 6, 13, 20, 34, ...,\}
\end{aligned}$$

Let the secret be $s = 2 \in \mathbb{F}_7$. The participants are all elements of $\mathbb{F}_7^{\times} = \{1, 2, 3, 4, 5, 6\}$. To recover the secret, we choose an element from each of representative set randomly. Let these elements be

$$8 \in [1], 17 \in [3], 4 \in [4], 26 \in [5], 13 \in [6] \tag{3.1}$$

These participants can recover the secret as follows

$$8 + 17 + 4 + 26 + 13 + x \equiv 0 \, (mod 7). \tag{3.2}$$

Therefore $x = 2 \in \mathbb{F}_7$ is obtained. Since $2 \in [2]$, the secret is recovered by solving above equation. This scheme is also a $(6; 6)-$ threshold secret sharing scheme, because if we take any $5 = 7 - 2$ participants, then the secret cannot be recovered.

4 Conclusion

In this paper, we present a new threshold secret sharing scheme based on the equivalence classes of a prime over $\mathbb{Z}$. We use the properties of these classes to explain the reconstruction algorithm. We determine the access structure and calculate the number of minimal coalitions of this scheme. We consider some possible attacks. The new scheme is ideal in the sense that the size of the secret equals the size of any share. Moreover, this scheme is perfect in terms of only qualified coalitions can obtain the secret. The new system is too reliable by means of security. We work on $\mathbb{F}_p$ over $\mathbb{Z}$, where p is prime. The advantage of this approach can be explained as follows. Since $\mathbb{F}_p$ is a field, the elements of $\mathbb{F}_p$ will be matched the previous elements after the certain processing steps. This situation increases the security. Thus our scheme cannot be constructed based on $\mathbb{Z}_m$, where m is any positive integer.

5 Acknowledgment

Thanks and appreciate to The Deanship of Scientific Research(DSR), King Abdulaziz University (KAU) supporting to our project with numbered "IFPIP:435-130-1443". This paper is written from that project.

References

[1] N. Al Ebri and C. Y. Yeun, *Proceedings of 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates* (2011) 40–45.

[2] C. Asmuth and J. Bloom, IEEE Trans. Information Theory **29 (2)** (1993) 208–210.

[3] G.R. Blakley, *Proceedings of National Computer Conference, New York, USA* (1979) 313–317.

[4] A. Beimel, Y. M. Chee, I, Gwo, S. Ling, F. Shao, Y. Tang, H. Wang, and C. Xing, (ed), *Secret Sharing Schemes: A Study* Springer (2011) 11–46.

[5] L. Csirmaz and G. Tardos, *Cryptology ePrint Archive* Report 2011/174 (2011).

[6] D. S. Dummit, R. M. Foote, *Abstract Algebra*, Prentice Hall International, Inc, University of Toronto (2004).

[7] S. Iftere, Technical Report TR 07-01, University Alexandruloan Cuza of Iasi, Faculty of Computer Science (2007).

[8] R. J. Mc Eliece, D. V. Sarwate, Commun. Assoc. Comp. Mach **24**(1981) 583–584.

[9] J. L. Massey, *Procedings of 6th Joint Swedish-Russian on Information Theory, M¨olle, Sweden* (1993) 276–279.

[10] K. Martin, *In Coding and Cryptography II*, Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts (2008) 45–63.

[11] A. Shamir, *Comm. of the ACM*, **22** (1979) 612–613.

[12] R. Yılmaz, *Some Ideal Secret Sharing Schemes, MSc Thesis*, Bilkent University, Turkey (2010).

[13] S. T. Almohammadi, C. Ozel, *General Letters in Math*, **6(1)** (2019) 1–9. DOI : https://doi.org/10.31559/glm2019.6.1.1