Received: 20 March 2023 | Revised: 20 May 2023 | Accepted: 07 June 2023

Research Article
Journal of Research and Review in Science
35-42, Volume 10, June 2023.
DOI: 10.36108/jrrslasu/3202.01.0130

ORIGINAL RESEARCH

(10,10)-Threshold Secret-Sharing Scheme using Equivalence Classes of Integers Modulo a Prime

Aidanwosa Aiwanose P.[1], Abdulkareem Abdulafeez O.[2]

[1]*Department of Mathematics, Faculty of Science, Lagos State University, Nigeria*

Correspondence
Abdulkareem Abdulafeez Olalekan, Department of Mathematics, Faculty of Science, Lagos State University, Nigeria.
Email:abdulafeez.abdulkareem@lasu.edu.ng

Abstract:
Introduction: The quest for increasing the security of data in secret-sharing schemes has attracted much attention in the world of cryptography. Several methods have been applied, and the application of the new technique, (n,n)-threshold secret-sharing scheme based on equivalence classes, will be a perfect solution.
Aims: The aim is to explore and construct strong knowledge in the theory and structure of the secret-sharing scheme on (n,n)-threshold secret-sharing scheme based on equivalence classes; $(X) = (y \in X: (x, y) \in \mathbb{R})$ And achieve the following objectives:
i. To investigate an (n, n)-threshold secret-sharing scheme based on the equivalence classes of the prime over $\mathbb{Z}$.
ii. Investigation of the accuracy of such a scheme.
Materials and Methods: The study uses the set of integers modulo a prime and modulo arithmetic on the set of integers.

Results: The statistics on the coalition, security analysis, and information-theoretic efficiency are also discussed.
Conclusion: The secret sharing scheme on (10,10)-threshold secret-sharing scheme based on equivalence classes of integers modulo a prime is perfect in terms of only qualified coalitions can obtain the secret and it is reliable by means of security. We have used the property of these classes to provide the reconstruction algorithms, and access structures and calculated the number of minimal coalitions of the scheme. This new system is ideal in that the size of the secret is equal to the size of the share.
Keywords: Secret Sharing, Threshold Secret Sharing Scheme, Equivalence relation.

1. INTRODUCTION

The quest for increasing the security of data in secret sharing schemes has attracted much attention in both the physical and digital worlds. In cryptographic problems, several methods have been introduced to address different problems. It is the purpose of this study to investigate a new technique, (n,n)-Threshold scheme, based on equivalence classes on integers.

Secret-sharing schemes are a tool used in many cryptographic protocol. A secret-sharing scheme involves a dealer who has a secret, a set of n parties and a collection $\mathcal{A}$ of subset of parties called the access structure.
A secret-sharing scheme for $\mathcal{A}$ is a method by which the dealer distributes shares to the parties such that:

(1) any subset in $\mathcal{A}$ can reconstruct the secret from its shares, and

(2) any subset not in $\mathcal{A}$cannot reveal any partial information on the secret.

Originally motivated by the problem of secure information storage, secret-sharing schemes have found numerous other applications in cryptography and distributed computing, e.g., Byzantine agreement, secure multiparty computations, threshold cryptography, access control, and attribute-based encryption [5,10].

Public-key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information. Nowadays, in many applications, there is a provider that wants to share data according to some policy based on user's credentials. In [5,10], it is shown that if the predicate can be described by an access structure that can be implemented by an efficient linear secret-sharing scheme, then there is an efficient attribute-based encryption system for this predicate.

Secret-sharing schemes were introduced by Blakley [3] and Shamir [8] for the threshold case, that is, for the case where the subsets that can reconstruct the secret are all the sets whose cardinality is at least a certain threshold. Secret-sharing schemes for general access structures were introduced and constructed by Ito, Saito, and Nishizeki [6]. More efficient schemes were presented in, e.g., [8,9,11,2]. Specifically, It is known that if an access structure can be described by a small monotone formula then it has an efficient perfect secret-sharing scheme. This was generalized by Karchmer and Wigderson [7] who showed that if an access structure can be described by a small monotone span programme then it has an efficient scheme.

A major problem with secret-sharing schemes is that the shares' size in the best known secret-sharing schemes realizing general access structures is exponential in the number of parties in the access structure. Thus, the known constructions for general access structures are impractical. This is true even for explicit access structures (e.g., access structures whose characteristic function can be computed by a small uniform circuit). On the other hand, the best known lower bounds on the shares' size for sharing a secret with respect to an access structure are far from the above upper bounds. The best lower bound was proved by Csirmaz [4], proving that, for every n, there is an access structure with n parties such that sharing ℓ-bit secrets requires shares of length Ω(\ln / log n). The question if there exist more efficient schemes, or if there exists an access structure that does not have (space) efficient schemes remains open. The statement below is a widely believed conjecture:

Conjecture 1.1
There exists an $\varepsilon > 0$ such that for every integer n there is an access structure with n parties, for which every secret-sharing scheme distributes shares of length exponential in the number of parties, that is, $2^{\epsilon n}$.

Proving (or disproving) this conjecture above is one of the most important open questions concerning secret sharing. No major progress on proving or disproving this conjecture has been obtained in the last 16 years. It is not known how to prove that there exists an access structure that requires super-polynomial shares (even for an implicit access structure).

Most previously known secret-sharing schemes are linear. In a linear scheme, the secret is viewed as an element of a finite field, and the shares are obtained by applying a linear mapping to the secret and several independent random field elements. For many applications, linearity is important, e.g., for secure multiparty computation. Thus, studying linear secret-sharing schemes and their limitations is important. Linear secret-sharing schemes are equivalent to monotone span programs. Super-polynomial lower bounds for monotone span programs and, therefore, for linear secret-sharing schemes.

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.

Another (t, n) - threshold secret sharing scheme was created by Asmuth and Bloom [1]. Their scheme was based on the Chinese Remainder Theorem.

In the present work, we present an (10, 10) - threshold scheme based on the equivalence classes of prime order over $\mathbb{Z}$. Since our scheme is constructed based on a finite field, it is very reliable in terms of security. Because in a finite field, the size of a number stays in a specified range, no matter how many operations we apply to the number. So the finite fields are more suitable to explain a cryptography application.

We should have the following notations to define secret sharing schemes:

1. The secret could be a password, a chemical formula, or any private information.

2. The dealer who selects the secret and distributes it among participants.

3. Shares which are pieces of the secret information. The eligible group of shares can reach the secret and the other group of shares cannot.

4. The participants who receive the secret shares.

5. 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 be recovered the secret.

In a secret sharing scheme there are two fundamental grades:

i) Distribution: The secret is broken into N pieces $y_1, y_2, \ldots, y_N$ 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.

2. PRELIMINARIES

We begin with some necessary information about equivalence relations on $\mathbb{Z}$ and secret sharing schemes.

2.1 Equivalence Relations

An important main concept in algebra is the notion of an equivalence relation. We will use the idea in the next section, where we remind the equivalence classes.

Definition 2.1 Let X be a non-empty set. A relation on X is a subset of $X \times X$.

Example 2.2 Let X be the set of real numbers. Let R be the relation defined by $(x, y) \in R$ iff $x \leq y$. R contains elements such as $(1,1), (\pi, 4)$ and $(-7/3, 0)$ but does not contain (2,1), since \$2 $\not\leq$ 1\$. Note that (x, x) in R for each $x \in X$, so we say that R is a reflexive relation. Also if $x \leq y$ and $y \leq z$, then $x \leq z$. Especially if $(x, y), (y, z) \in R$, then $(x, z) \in R$. We say that the relation R is transitive. On the other hand, $(1,2) \in R$ but $(2,1) \notin R$, so R is not symmetric.

Definition 2.3 Let X be a non-empty set. A relation R on X is called an equivalence relation if

- $(x, x) \in R$ for every $x \in X$ (R is reflexive)
- if $(x, y) \in R$, then $(y, x) \in R$ (R is symmetric)
- if $(x, y), (y, z) \in R$, then $(x, z) \in R$ (R is transitive).

If R is an equivalence relation on a set X, then the equivalence class of an element $x \in R$ is defined as the set of all elements in X that are equivalent to x. We write

$$[x] = \{y \in X : (x, y) \in R\}$$

2.2 The Ring of Integers Modulo n

Let n be a fixed positive integer. Define a relation on $\mathbb{Z}$ by $a \sim b$ if and only if $n|(b - a)$. Clearly $a \sim a$ and $a \sim b$ implies b$\sim a$ for any integers a and b, so this relation is trivially reflexive and symmetric. If $a \sim b$ and $b \sim c$, then n divides (a-b) and n divides (b-c) so n also divides the sum of these two integers, i.e. n divides $(a - b) + (b - c) = a - c$, so $a \sim c$ and the relation is transitive. Hence this is an equivalence relation. Write $a \equiv b (mod\ n)$ if $a \sim b$. For any $k \in \mathbb{Z}$ we shall denote the equivalence class of a by $\bar{a}$. This is called the congruence class of $a\ mod\ n$ and consists of the integers which differ from a by an integral multiple of n, i. e.

$$\bar{a} = \{a + k\,n \,|k \in \mathbb{Z}\}$$
$$= \{a, a \mp n, a \mp 2n, a \mp 3n, \ldots.\}\,.$$

There are precisely n distinct equivalence classes $mod\ n$, namely $\bar{0}, \bar{1}, \bar{2}, \ldots, n - 1$ determined by the possible remainders after division by \$n\$ and these residue classes partition the integers $\mathbb{Z}$. The set of equivalence classes under this equivalence relation will be denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$ and called the integers modulo n (or the integers $mod\ n$).

$\mathbb{Z}_n = \{[0], [1], \ldots, n - 1]\}$.

The congruence class of x is given by

$$[x] = \{nk + x : k \in \mathbb{Z}\}$$

for each $x \in Z$ and $[x]$ has a unique representation as $[r]$, where r the remainder of x modulo n.

Theorem 5. *$\mathbb{Z}_n$ is a field if and only if n is prime.*

We remind an important definition associated with equivalence relation.

Definition 6. A pair (U, R) of a nonempty set U and on equivalence relation R is said to be an approximation space.

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 prime over $\mathbb{Z}$.

We need the approximation space $(\mathbb{Z}, \sim)$, where $\sim$ is a equivalence relation on $\mathbb{Z}$. - Let the approximation space $(\mathbb{Z}, \sim)$ be the secret space. We know that this relation splits $\mathbb{Z}$ into the equivalence classes.

1. Let our modulo be prime p, where $p \geq 5$. So we work on the equivalence classes of prime.
2. Consider the set of

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, p-1\} = \{x_0, x_1, \dots, x_{p-1}\}.$$

This set is public.

1. Secret Distribution:

- First the dealer picks a secret s from the set of $\{\mathbb{Z}_p - 0\}$.
- Then he distributes it over a secure channel to each participant P_j, where $1 \leq j \leq p-1$.

2. Secret Recovery: The participants can retrieve the secret by forming the sum

$$\overline{0} = \sum_{j=1}^{p-1} x_j,$$

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 7. *Our scheme satisfying above conditions meets the following requirements.*

1. *The access structure consists of the equivalence classes of prime.*
2. *The size of access structure is* $p-1$.

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

3. In this scheme we are working on Z_p and $|\mathbb{Z}_p| = p$. Any element of $\{\mathbb{Z}_p - 0\}$ can be the secret. Moreover, we need the remaining $p-1$ elements to reach the secret. So the size of access structure is $p-1$.

Theorem 8. *This new scheme is also a* $(p-1, p-1)$ *- threshold secret sharing scheme.*

Proof. The participants are elements of $\mathbb{Z}_p^* = \{\mathbb{Z}_p - 0\}$ and $|\mathbb{Z}_p^*| = p-1$. Hence $p-1$ elements of $\mathbb{Z}_p$ (except the secret) can recover the secret together. Thus the new scheme is a $(p-1, p-1)$ - threshold secret sharing scheme. □

3.2 Statistics on Coalitions

Theorem 9. *In the new secret sharing scheme based on equivalence classes of prime over $\mathbb{Z}$, the number of minimal coalitions is* $\binom{p-1}{p-2} = p-1$.

Proof. A minimal coalition is a set of participants. The participants are elements of $\mathbb{Z}_p^* = \{\mathbb{Z}_p - 0\}$ and their number is $p-1$. The secret is any element of $\mathbb{Z}_p^*$. The remaining $p-2$ elements can recover the secret. So the number of minimal coalitions of this scheme is $\binom{p-1}{p-2} = p-1$. □

3.3 Security Analysis

Assume that $h-(p-1)$ users has to guess the secret amongst $(p-1)+h$, 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 $h > 5$. 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 $\{\mathbb{Z}_p - 0\}$ which is recovered the secret. It is very difficult to guess them since it is chosen randomly.

The scheme based on $\mathbb{Z}_p$ over $\mathbb{Z}$ 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.

1. all eligible coalitions can obtain the secret and
2. unskilled coalitions acquire no information about the secret. So our scheme is both ideal and perfect.

4. APPLICATION OF THE SCHEME

We consider $Z_{11} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}\}$ over Z. Let us write the representatives set for each equivalence class.

$$\bar{0} = [0] = \{\dots,0,11,22,\dots\}$$
$$\bar{1} = [1] = \{\dots,1,12,23,\dots\}$$
$$\bar{2} = [2] = \{\dots,2,13,24,\dots\}$$
$$\bar{3} = [3] = \{\dots,3,1425,\dots\}$$
$$\bar{4} = [4] = \{\dots,4,15,26,\dots\}$$
$$\bar{5} = [5] = \{\dots,5,16,27,\dots\}$$
$$\bar{6} = [6] = \{\dots,6,17,28,\dots\}$$
$$\bar{7} = [7] = \{\dots,7,18,29\dots\}$$
$$\bar{8} = [8] = \{\dots,8,19,30\dots\}$$
$$\bar{9} = [9] = \{\dots,9,20,31,\dots\}$$
$$\bar{10} = [10] = \{\dots,10,21,32\dots\}$$

Let the secret be $s = \bar{3} \in Z_{11}$. The participants are

$$Z_p^* = \{\mathbb{Z}_p - 0\} = \{1,2,3,4,5,6,7,8,9,10\}.$$

To recover the secret, we choose an element from each of representative set randomly. Let these elements be

$$12 \in \bar{1}$$
$$24 \in \bar{2}$$
$$4 \in \bar{4}$$
$$38 \in \bar{5}$$
$$17 \in \bar{6}$$
$$18 \in \bar{7}$$
$$30 \in \bar{8}$$
$$9 \in \bar{9}$$
$$32 \in \bar{10}$$

These participants can recover the secret as follows.

$$12 + 24 + 4 + 38 + 17 + 18 + 30 + 9 + 32 + x \equiv 0(\bmod 11)$$

Therefore

$$x = 3 \in Z$$

is obtained. Since $3 \in \bar{3}$, the secret is recovered by solving above equation. This scheme is also a $(10,10)$-threshold secret sharing scheme.

5. CONCLUSION

The secret sharing scheme on $(10,10)$-threshold secret-sharing scheme based on equivalence classes of prime over $\mathbb{Z}$ is perfect in term of only qualified coalition can obtain the secret and it is reliable by means of security. We have used the property of these classes to explain the reconstruction algorithms, access structures and calculated the number of minimal coalitions of the scheme. This new system is ideal in that the size of secret equal to the size of any share.

AUTHORS' CONTRIBUTIONS

All authors participated actively in this research work and have read and approved the final manuscript.

CONSENT (WHERE EVER APPLICABLE)

Consent form has been approved by all authors.

REFERENCES

1. Asmuth, C. A. and Bloom, J. A modular approach to key safeguarding, IEEE Transactions on Information Theory IT-29. 1983;208–210.

2. Bertilsson M., Ingemarsson I. A construction of practical secret sharing schemes using linear block codes. In J. Seberry and Y. Zheng, editors, Advances in Cryptology – AUSCRYPT ’92, volume 718 of Lecture Notes in Computer Science. Springer-Verlag. 1993;67–79.

3. Blakley, G. R., Safeguarding cryptographic keys, in: National Computer Conference, American Federation of Information Processing Societies Proceedings. 1979;48:313–317.

4. Csirmaz, L. The size of a share must be large. Journal of Cryptology, 1997;10:223–231.

5. Goyal V., Pandey O., Sahai A., Waters B., Attribute-based encryption for fine-grained access control of encrypted data. In Proc. of the 13th ACM conferenceon Computer and communications security, 2006;89–98.

6. Ito, M., Saito, A., Nishizeki, T. Secret sharing scheme realizing any access structure. Proc. IEEE Globecom’87. 1987;99–102.

7. Karchmer M., Wigderson A., On span programs. Proceedings of the Eighth Annual Structure in Complexity Theory Conference, San Diego, CA. 1993;102–111.

8. Shamir A., How to share a secret, Communications of the ACM 22 1979;612–613.

9. Simmons G.J., Jackson W., K. M. Martin K.M., The geometry of shared secret schemes. Bulletin of the ICA. 1991;1:71–88.

10. Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Technical Report 2008/290, Cryptology ePrint Archive, 2008;http://eprint.iacr.org/.

11. Yilmaz, R., Some Ideal Secret Sharing Schemes, Master Thesis, Bilkent University, Ankara, Turkey, August, 2010.