ALTERNATIVE TO SHAMIR'S SECRET SHARING SCHEME LAGRANGE INTERPOLATION OVER FINITE FIELD

Vanashree Gupta¹, Smita Bedekar²

E-Mail Id: ¹vanashreegupta@gmail.com, ²smitab@unipune.ac.in

Interdisciplinary School of Scientific Computing, Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract- Secret Sharing is a robust key management method in which shares are distributed to parties and only authorized subsets of parties can reconstruct the secret. Secret sharing schemes are the tool used in cryptography and security. There are different methods of secret sharing. Threshold secret sharing is a method in which out of all the parties only predefined or certain number of parties can reconstruct the secret. In this paper we will describe a threshold secret sharing scheme, the Shamir's secret sharing scheme and proposing an alternative approach for secret recovery instead of Lagrange interpolation over finite field. Based on this study we can use it in different applications such as secret data hiding and authentication, audio secret management, medical image security and EPR hiding, in storing credit card information securely.

Keywords: Credit card, Secret sharing, Security, Shamir's secret sharing, Threshold secret sharing.

1. INTRODUCTION

Secrets are the important messages or things, which should be always preserved and protected. Handling of secret is very important task. Sometimes we think that it is secure in single hand but at other time it is thought to be secure in many hands [15]. All this depends upon situation. Consider the case that you are managing a bank's vault which works with key. Now your job is to securely manage the key. For this you should be physically present whenever the vault needs to be opened. What will happen on vacation days you have? Also, in worst case, what if you lost the one and only key [18]? So there is need of sharing secret among more than one person.

Therefore secret is divided into pieces and distributed to that many people. This is called share distribution. When these pieces joined together will get the complete secret. This is called secret recovery. There are different methods for share distribution as well as secret recovery. Here we proposed a secret recovery method. Banking system uses the concept of secret sharing. To open the locker both the keys are required either of them cannot open the locker.

1.1 Organization

The rest of the paper is organized as follows: Section 2 some definitions are discussed. Section 3 covers related work based on Shamir's threshold secret sharing schemes and highlights details of how method were implemented. Section 4 gives an idea of the proposed method for secret recovery. Section 5 discusses the comparative study analysis of existing secret sharing schemes and proposed one. Section 6 concludes with final remarks .

2. SOME DEFINITIONS

2.1 Share/Shadow

Information held by each participant is called share.

2.2 Dealer

Special participant who choose secret is the dealer and is responsible for computing and distributing shares.

2.3 Combiner

Process by which recovery of secret information from authorized set is done [15].

2.4 Access Structure

The collection of subsets of participants that can reconstruct the secret.

2.5 Information Rate

It is ratio of the length of the secret (in bits) to the maximum length of share given to participants. In Shamir's scheme the share size is same as the secret size. However in generalized scheme which is other way of secret sharing, the share size is larger than the secret size.

2.6 Optimal Information Rate

The maximal information rate over all secret sharing scheme that realize that structure.

DOI Number: <https://doi.org/10.30780/IJTRS.V06.I03.002>

pg. 6

www.ijtrs.com, www.ijtrs.org

Paper Id: IJTRS-V6-I3-002

Volume VI Issue III, March 2021

@2017, IJTRS All Right Reserved

2.7 Secret Sharing Scheme (SSS)

A secret sharing scheme is a method by which a dealer distributes shares to parties such that only authorized subsets of parties can reconstruct the secret [7].

2.8 Ideal Secret Sharing

Secret sharing schemes having information rate 1 are called ideal. Scheme is ideal if share has the same length as secret [8]. This secret sharing scheme have high efficiency.

2.9 Perfect Secret Sharing

Secret sharing scheme in which no information about the secret is obtained on pooling of shares of any unauthorized set of participants [15].

2.10 Principal of Secret Sharing

2.10.1 Initialization /Division Phase

In this a secret is divided among a group of participants. Each of the participant get a share of the secret.

2.10.2 Reconstruction Phase

This phase uses combiner algorithm. Sufficient number of shares combined reveals secret. Based on the principal there are different kinds of secret sharing schemes e.g. threshold secret sharing, general access structure and verifiable secret sharing [8]. Here we are going to discuss only threshold secret sharing scheme.

2.11 Threshold (t,n) Secret Sharing

In secret sharing there is one dealer and n players. The dealer gives each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of fewer than t players can. Such a system is called a (t,n) - threshold scheme [19].

3. RELATED WORK

There is an application scenarios where controlled access is necessary. For example in a bank three tellers are employed to open a vault. Combination of any two or all three can open the vault but a single person is not allowed to do so. These problems can be solved by means of threshold secret sharing schemes. This example is a (2; 3) threshold secret sharing scheme. The unanimous consent control is a (n; n) threshold scheme. These threshold schemes help to achieve both availability and confidentiality.

There are mainly 4 methods used to do threshold secret sharing: Shamir's secret sharing [1] which is polynomial interpolation based, Blakley's Secret Sharing [2] which is hyperplane based, Asmuth Bloom Secret Sharing [3][23] based on Chinese remainder theorem, Mignotte Secret Sharing [5] based on Chinese remainder theorem [4].

3.1 Shamir's Secret Sharing [1][16]

In this scheme each participant has to keep only one share which is of same size as the secret (ideal) and also less than t participant cannot deduce any information about the secret (perfect). This scheme is called (t; n) threshold schemes. Adi- Shamir idea for secret scheme was to define a line 2 points are sufficient, to define a parabola 3 points are sufficient, 4 points to define a cubic curve and so forth [22]. k points are sufficient to define a polynomial of degree (k-1). Shamir's secret sharing is linear approach based on Lagrange's polynomial interpolation. The correctness and privacy of Shamir's scheme follow from this [7]. It has two parameters: t, the threshold and n, the number of participants / players. The main idea of the scheme is that t points are sufficient to define a polynomial of degree t-1.

Given (t,n) secret sharing with secret information k and n shareholders { P₁, P₂, P₃, ..., P_n }. Using t-1 degree random polynomial with random coefficient.

Step 1: Polynomial construction

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \pmod{p}$$

Step 2: Share distribution

$$\text{Share}_i(s) = (x_i, f(x_i))$$

Step 3: Secret recovery

Using Lagrange Interpolation formula, the polynomial f(x) can be written in the form

$$f(x) = \sum_{i=0}^{t-1} f(x_i) * L_i(x)$$

where L_i(x) is the Lagrange Polynomial.

$$L_i(x) = \prod_{j=0, j \neq i}^{t-1} \frac{x - x_j}{x_i - x_j}$$

$L_i(x)$ has value 1 at x_i , and 0 at every other x_j .

3.2 Algorithm for Shamir's Secret Sharing Scheme

Share generation and share reconstruction-Create a group, group size n to share a secret.

- Select group size n , threshold t , prime number p (length of p depends on the security level required), m - minimum number of secret.
- Generate secret randomly between m and $p-1$.

3.3 Shamir's Secret Split or Share Generation

Build unique polynomial $f(x)$ with input n, t, p, s .

- Select n random distinct evaluation points on polynomials which are secret shares $sh_1, sh_2, \dots, sh_n$.
- Dealer distributes secret shares to group.
- This builds the polynomial and generates n shares $sh_1, sh_2, \dots, sh_n$.

3.4 Shamir's Secret Reconstruction

- Collect threshold number of secret shares t from any of the group members $sh_0, sh, \dots, sh_{t-1}$.
- Using Lagrange interpolation formula, compute Lagrange Polynomial $L_i(x)$.
- Reconstruct unique polynomial $f(x)$ from Lagrange polynomial.
- Secret (reconstructed)- constant a_0 in unique polynomial $f(x)$ in the secret s .

3.5 Properties of Shamir's Secret Scheme

- Secure - The secret will be kept secure and confidential from participants.
- Minimal- Size of secret does not exceed size of share.
- Extensible
- Dynamic - Security can be increased.
- Flexible
- Convenience
- Reliability

3.6 Limitations of Shamir's Secret Scheme

- Verifiable Shares Verifiable shares are not produced by Shamir's Scheme, i.e. individuals can prevent correct share being reconstructed by submitting fake one. An adversarial shareholder with enough information can even produce a different share such that secret S is reconstructed to a value of their choice. This issue is addressed by verifiable secret sharing schemes such as Feldman's scheme and Pedersen's scheme [18].
- The length of a secret is easily leaked since the length of any given share is equal to the length of an associated secret. This issue is trivial to fix by simply padding the secret to a fixed length [18].
- It is computationally hard & becomes impractical with large number of shares. Stack overflow will occur.
- In Shamir's (k, n) threshold scheme, Lagrange interpolation requires $O(k \log^2 k)$ steps. The complexity can be reduced from $O(k \log^2 k)$ to $O(k(\log k - \log j)^2)$ if instead of sharing a single long s , divide s into j smaller pieces and share every piece [21].
- Larger the share size, more memory is required which lowers the efficiency.

4. PROPOSED METHOD

The proposed secret sharing is linear approach based on Variable elimination.

Given (t, n) secret sharing with secret information k and n shareholders $\{P_1, P_2, P_3, \dots, P_n\}$. Using $t-1$ degree random polynomial with random coefficient. First two steps i.e. polynomial construction and share distribution are similar to Shamir secret sharing explained above. Difference lies in the share recovery step.

Step 1: Polynomial construction

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1} \pmod{p}$$

Step 2: Share distribution

$$\text{Share}_i(s) = (x_i, f(x_i))$$

Step 3: Secret recovery

Here instead of Lagrange interpolation we are using variable elimination.

4.1 Algorithm for Proposed Secret Sharing Scheme

Share generation and share reconstruction- Create a group , group size n to share a secret.

- Select group size n, threshold t, prime number p (length of p depends on the security level required), m- minimum number of secret.
- Generate secret randomly between m and p-1.

4.2 Secret Split

Build unique polynomial $f(x)$ with input n,t,p,s.

- Select n random distinct evaluation

points on polynomials which are secret shares $sh_1, sh_2, \dots, sh_n$.

- Dealer distributes secret shares to group.
- This builds the polynomial and generates n shares $sh_1, sh_2, \dots, sh_n$.

4.3 Secret reconstruction

- Collect threshold number of secret shares t from any of the group members $sh_0, sh_1, \dots, sh_{t-1}$.
- Write polynomial equations $f(x_i)$ for respective share x_i of threshold t.
- Using variable elimination method compute values of constants.
- Reconstruct unique polynomial $f(x)$.

Secret (reconstructed)- constant a_0 in the unique polynomial $f(x)$ in the secret S.

4.4 A Method of Solution

Example 1: Consider $a(3,6)$ over Z_7

Let $x_i=1,2,3,4,5,6$. Secret is 3.

$$f(x)=3+3x+3x^2$$

Share	S1	S2	S3	S4	S5	S6
Value	2	-	4	-	-	3

$$f(x)=a_0+a_1x^1+a_2x^2+a_3x^3+\dots$$

Here $t=3$ so computing p_1, p_3 & p_6 as follows

$$2=a_0+a_1+a_2$$

$$4=a_0+3a_1+2a_2$$

$$3=a_0+6a_1+a_2$$

4.5 Finding Secret a_0 using Lagrange Interpolation

$$f(0) = \frac{(-x_3)(-x_6)}{(x_1-x_3)(x_1-x_6)} * y_1 + \frac{(-x_1)(-x_6)}{(x_3-x_1)(x_3-x_6)} * y_3 + \frac{(-x_1)(-x_3)}{(x_6-x_1)(x_6-x_3)} * y_6$$

$$f(0) = \frac{(-3)(-6)}{(1-3)(1-6)} * 2 + \frac{(-1)(-6)}{(3-1)(3-6)} * 4 + \frac{(-1)(-3)}{(6-1)(6-3)} * 3$$

$$f(0) = \frac{18}{(-2)(-5)} * 2 + \frac{6}{(2)(-3)} * 4 + \frac{3}{(5)(3)} * 3$$

$$f(0) = \frac{36}{10} + \frac{24}{-6} + \frac{9}{15}$$

$$f(0)=36*10^{-1} - 24*6^{-1} + 9*15^{-1} \pmod{7}$$

$$f(0)=36*5 - 24*6 + 9*8 \pmod{7}$$

$$f(0)=180-144+72 \pmod{7}$$

$$f(0)=108 \pmod{7}$$

$$f(0)=3$$

4.6 Finding Secret a_0 using Variable Elimination Method

$$2=a_0+a_1+a_2$$

$$a_0=2-a_1-a_2$$

$$4=a_0+3a_1+2a_2$$

Substitute value of a_0 in above equation, we get

$$4=2-a_1-a_2+3a_1+2a_2$$

DOI Number: <https://doi.org/10.30780/IJTRS.V06.I03.002>

pg. 9

www.ijtrs.com, www.ijtrs.org

Paper Id: IJTRS-V6-I3-002

Volume VI Issue III, March 2021

@2017, IJTRS All Right Reserved

$$a_2 = 2 - 2a_1$$

$$3 = a_0 + 6a_1 + a_2$$

Substitute value of a_0 and a_2 in above equation

$$3 = 2 - a_1 \cdot a_2 + 6a_1 + 2 - 2a_1$$

$$1 = 5a_1$$

$$1 \cdot 5^{-1} \bmod 7 = a_1$$

$$10 \bmod 7 = a_1$$

$$3 = a_1$$

$$a_0 = 2 - 3 + 4 \bmod 7$$

$$a_0 = 6 - 3 \bmod 7$$

$$a_0 = 3 \text{ which is a secret.}$$

From above methods we can reconstruct the same secret.

Example 2:

We will consider the example given in [15][20], a secret is shared by computing points on a random polynomial in $(\mathbb{Z}/p\mathbb{Z})[X]$. Assume “plaintext” secret contains only words in uppercase letters which is a sequence of letters and blank spaces. Replace each letter of the secret by a number, using the following correspondence:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

The blank space is replaced by 99. Finally we obtain a very large number, if the secret is large. Then break the secret into a sequence of positive integers, each smaller than p . These are called the *blocks* of the secret.

For example, the numerical representation of the proverb

“A SMALL LEAK WILL SINK A GREAT SHIP” is

1099282210212199211410209932182121992

818232099109916271410299928171825

We choose the prime $p = 9973$, break above large number into blocks smaller than 9973.

Like 1099-2822-1021-2199-2114-1020-9932-1821- 2199-2818-2320-9910-9916-2714-1029- 9928 -1718 - 25

When secret is reconstructed, one obtains a sequence of blocks. The blocks are then joined together to give the numerical representation of the secret. It is only after replacing the numbers by letters, according to the table above, that one obtains the original secret [20].

We choose $p = 9973$. To construct a $(3,5)$ - threshold scheme, dealer chooses $x_i = i$, $1 \leq i \leq 5$, randomly selected coefficients $b_2 = 1572$ and $b_1 = 7583$ are 1.

For the first block of the secret, we must compute the polynomial,

$$f(x) = 1572x_2 + 7583x + 1099 \pmod{9973}$$

at each x_i . Thus the five shares of the first block are:

$$s_1 = f(1) = 1572 \cdot 1 + 7583 \cdot 1 + 1099 \equiv 281 \pmod{9973}$$

$$s_2 = f(2) = 1572 \cdot 2 + 7583 \cdot 2 + 1099 \equiv 2607 \pmod{9973}$$

$$s_3 = f(3) = 1572 \cdot 3 + 7583 \cdot 3 + 1099 \equiv 8077 \pmod{9973}$$

$$s_4 = f(4) = 1572 \cdot 4 + 7583 \cdot 4 + 1099 \equiv 6718 \pmod{9973}$$

$$s_5 = f(5) = 1572 \cdot 5 + 7583 \cdot 5 + 1099 \equiv 8503 \pmod{9973}$$

Sharing the whole secret, we have the following sequence of blocks:

$s_1 = 281-2004-203-1381-1296-202- 9114-1003-1381- 2000-1502-9092- 9098-1896-211-9110-900-9180.$

$s_2 = 2607-4330-2529-3707-3622- 2528- 1467-3329-3707-4326-3828-1445- 1451 - 4222-2537-1463-3226-1533.$

$s_3 = 8077-9800- 7999-9177-9092- 7998 -$

$6937- 8799-9177- 9796-9298-6915 -6921 -$

$9692 -8007 - 6933-8696-7003.$

$s_4 = 6718-8441-6640-7818-7733 - 6639-$

$5578-7440-7818-8437-7939-5556-5562-8333$

$-6648- 5574-7337-5644.$

$s_5 = 8503-253-8425-9603- 9518-8424- 7363-9225-9603- 249-9724-7341- 7347- 145-8433-7359-9122-7429.$

DOI Number: <https://doi.org/10.30780/IJTRS.V06.I03.002>

pg. 10

www.ijtrs.com, www.ijtrs.org

Let us see how a block of a secret can be reconstructed from the three shares using both methods.

4.7 Using Lagrange Interpolation Method to find Secret

The first block of S can be reconstructed from the first blocks of the shares s_2 , s_3 and s_5 by using the formula Lagrange interpolation formula:

$$b[0] = \frac{2607.3}{1.3} * 5 + \frac{8077.2}{-1.2} * 5 + \frac{8503.2}{-3.-2} * 5 \pmod{9973}$$

$$b[0] = 2607.5 + 8077.(-5) + 8503 \pmod{9973}$$

$$b[0] = -18847 \pmod{9973}$$

$$b[0] = 1099$$

Similarly each block can be reconstructed.

4.8 Using Proposed Variable Elimination Method

The first block of S can be reconstructed from the first blocks of the shares s_2 , s_3 and s_5 by using the variable elimination method:

$$p=9973, s(2)=2607, s(3)=8077, s(5)=8503$$

$$f(x)=a_0+a_1x+a_2x^2+\dots+a_{t-1}x^{t-1} \pmod{p}$$

Here 3 shares are given $t=3$, generate the polynomials as follows:

$$f(2)=a_0+a_12+a_22^2 \pmod{9973}$$

$$2607=a_0+2a_1+4a_2 \pmod{9973}$$

$$2607-2a_1-4a_2=a_0 \quad \text{----- (1)}$$

$$f(3)=a_0+a_13+a_23^2 \pmod{9973}$$

$$8077=a_0+3a_1+9a_2 \pmod{9973}$$

$$8077=2607-2a_1-4a_2+3a_1+9a_2 \pmod{9973}$$

$$5470=a_1+5a_2$$

$$5470-5a_2=a_1 \quad \text{----- (2)}$$

$$f(5)=a_0+a_15+a_25^2 \pmod{9973}$$

$$8503=a_0+5a_1+25a_2 \pmod{9973}$$

$$8503=2607-2a_1-4a_2+5a_1+25a_2 \pmod{9973}$$

$$5896=21a_2+3a_1$$

$$5896=21a_2+3(5470-5a_2)$$

$$5896=21a_2+16410-15a_2$$

$$-10514=6a_2 \pmod{9973}$$

$$-10514/6=a_2$$

$$-10514*6^{-1} \pmod{9973}=a_2$$

$$-10514*8311 \pmod{9973}=a_2$$

$$[\text{because } 6^{-1} \equiv 8311 \pmod{9973}]$$

$$-87381854 \pmod{9973}=a_2$$

$$-8401 \pmod{9973}=a_2$$

$$1572=a_2$$

Put $1572=a_2$ in equation (2)

$$5470-5a_2=a_1$$

$$5470-5*1572=a_1$$

$$5470-7860=a_1$$

$$-2390 \pmod{9973}=a_1$$

$$7583=a_1$$

Put $7583=a_1$ and $1572=a_2$ in equation (1)

$$2607-2a_1-4a_2=a_0$$

$$2607-2*7583-4*1572=a_0$$

$$2607-15166-6288=a_0$$

$$2607-21454=a_0$$

$$-18847 \pmod{9973}=a_0$$

$$-8874 \pmod{9973}=a_0$$

$$1099=a_0 \text{ which is a secret.}$$

From both methods we can reconstruct the same secret. Similarly each block can be reconstructed from either of the method. Our proposed scheme is fast because it depends on solving linear equations.

5. COMPARATIVE STUDY ANALYSIS

Table 5.1 shows comparative summary between Shamir, Blakley, Mignotte, Asmuth-Bloom and proposed secret sharing scheme.

Table-5.1 Comparison of Different Threshold Secret Sharing Schemes

Parameters	Secret Sharing Scheme				
	Shamir	Blakley	Mignotte	Asmuth-Bloom	Proposed
Techniques used	Polynomial interpolation	Vector space (Hyper plane)	Chinese remainder theorem	Chinese remainder theorem	Polynomial variable elimination
Perfect	Yes	No	No	No	Yes
Ideal	Yes	No	No	No	Yes
Multiple secret sharing	No	No	No	No	No
Threshold	Yes	Yes	Yes	Yes	Yes
Verifiable	No	No	No	No	No
Proactive	No	No	No	No	No

CONCLUSION

In this paper, we considered Shamir secret sharing as a basic tool in cryptography. Based on that proposed an alternative method for secret reconstruction. Applications for secret sharing schemes are becoming more important. Shamir secret sharing is fast, reliable, secure and most importantly it is applicable. Same is the case with the proposed approach.

FUTURE WORK

There are lot of applications for secret sharing scheme and day by day they are becoming more important. In our future work we are going to give the additional security to this new approach and will try to apply in other fields too. The comparative study shows that to add functionalities like multiple secret sharing, verifiability is difficult with threshold secret sharing. In future better threshold secret sharing can be implemented with all the capabilities.

REFERENCES

- [1] A. Shamir, "How to Share a Secret", Communications of the ACM, vol.22, no.11, 1979.
- [2] G. Blakely, "Safeguarding cryptographic keys", presented at Proceedings of the AFIPS 1979 National Computer Conference, vol. 48, Arlington, VA, June 1979, pp. 313–317.
- [3] C. Asmuth, J. Bloom, "A modular approach to key safeguarding", IEEE Transactions on Information Theory, Vol. 29, Issue 2, pp.208–210, March 1983.
- [4] Kamer Kaya and Ali Aydn Selcuk, "Threshold cryptography based on Asmuth Bloom secret sharing", Information Sciences, 2000, 177.
- [5] M. Mignotte, "How to Share a Secret, Cryptography", Lecture notes in Computer Science, Springer-Verlag, Germany, pp 371-375, 1983.
- [6] Cheng Gu, Chin-Chen Chang, "A Construction for Secret Sharing Scheme with General Access Structure", Journal of Information Hiding and Multimedia Signal Processing Ubiquitous International Volume 4-No.1, January 2013, ISSN 2073-4212
- [7] Amos Beimel, "Secret Sharing Schemes: A Survey", IWCC 2011, LNCS 6639, pp. 11-46, 2011, Springer-Verlag Berlin Heidelberg 2011.
- [8] Sonali Patil, Prashant Deshmukh, "An Explication of Multifarious Secret Sharing Schemes", International Journal of Computer Applications (0975 – 8887) Volume 46– No.19, May 2012.
- [9] D. R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton 1995.
- [10] E.D. Karnin, J.W. Greene, and M. E. Hellman, "On secret sharing systems," vol. IT-29, no. 1, pp. 35–41, Jan. 1983.
- [11] P. Giblin, "Primes and Programming: An introduction to Number Theory with Computing", Cambridge University Press/New York, pp. 79-82, 1993.

- [12] Levent Ertaul, William Marques Baptista, "Storing Credit Card Information Securely using Shamir Secret Sharing in a Multi-Provider Cloud".
- [13] J. Kleinberg and É. Tardos, "Algorithm Design", Pearson Education/Boston, 1st ed., pp. 234-242, 2006.
- [14] P. Choudhary, "A Practical Approach to: Linear Algebra", Oxford Book Company /India, 1st Ed, 2009.
- [15] A Sreekumar, "Secret sharing schemes using visual cryptography, Ph.D. thesis, Cochin University of Science and Technology, 2009.
- [16] V Binu, "Secret Sharing Schemes with Extended Capabilities and Applications", Ph.D. thesis, Cochin University of Science and Technology, 2016.
- [17] Janhavi Sirdeshpande, Sonali Patil, "Amended Biometric Authentication using Secret Sharing", International Journal of Computer Applications (0975 – 8887) Volume 98 – No.21, July 2014.
- [18] <https://ericrafaloff.com/shamirs-secret-sharing-scheme/>
- [19] https://en.wikipedia.org/wiki/Secret_sharing.
- [20] Neelam Yadav, Kanina Dhiraj Kumar, Ravi Yadav, "Key Sharing Schemes Using Visual Cryptography", International Journal of New Innovations in Engineering and Technology (IJNIET) Vol. 1 Issue 4 April 2013 ISSN: 2319-6319
- [21] T-79.159 Cryptography and Data Security, 24.03.2004 Lecture 9: Secret Sharing, Threshold Cryptography, MPC, Helger Lipmaa
- [22] https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing.
- [23] Shalini I S, Mohan Naik R, S V Sathyanarayana, "A comparative analysis of Secret Sharing Schemes with special reference to e-commerce applications", International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), 2015.