A NEW APPROACH TO CONSTRUCT (K, N) THRESHOLD SECRET SHARING SCHEMES BASED ON FINITE FIELD EXTENSION

[1]*Vanashree Gupta* & [2]*Smita* Bedekar

Interdisciplinary School of Scientific Computing,
Savitribai Phule Pune University, Pune , Maharashtra, India
Email: [1]vanashreegupta@gmail.com ,[2]smitab@unipune.ac.in

Abstract
With increase in use of internet there is need to keep passwords, secret keys, important information secret. One way to do this is encryption. But it also need key which should be kept secure. Sometimes key is secure. But what will happens if the key is lost, forgotten etc. This problem can be solved using secret sharing. Instead of sharing whole secret, it is divided into pieces and distributed to finite set of pieces and some subset of pieces called access structure of scheme, which can recover secret. Here we propose a new way to construct threshold secret sharing schemes based on finite field extension using Blakley's secret sharing as a base. It is useful in many cryptographic applications and security. Because of finite fields the size of numbers stays within a specified range, doesn't matter how many operations we apply on number.

Keywords: *Finite Field extension, Secret Sharing Scheme, Blakley's secret sharing, Access structure, Security*

1. Introduction
A secret sharing is useful in hiding information among certain pieces called shares\shadows and distributed to those many people. This is called share distribution. When particular subset of pieces called access structure joined together will get the complete secret. This is called secret recovery. There are lots of studies about secret sharing schemes. Shamir's secret sharing [1] which is polynomial interpolation based, Blakley's Secret Sharing [2] is hyperplane based, Asmuth Bloom Secret Sharing [3][23] based on Chinese remainder theorem, Mignotte Secret Sharing [5] based on Chinese remainder theorem [4] . Beimel [7] gave detail study about construction of secret sharing schemes. Shalini et al [23] proposed secret sharing scheme based on elliptic curve and gave a comparative analysis of secret sharing schemes with special reference to e-commerce applications. [8] explains about various multifarious secret sharing schemes, their applications and the comparison based on various extended capabilities.In [25] an alternative way to Shamir's secret sharing scheme lagrange interpolation over finite field is proposed.

Here we proposed a new way to construct a threshold secret sharing scheme. We use Blakley's secret sharing as a base and same technique of finite field can be used to construct new scheme using Shamir's secret sharing as base.

1.1 Our Contribution

In this work, we provide a brief overview of existing threshold secret sharing schemes Shamir's secret sharing [1] and Blakley's Secret Sharing [2] .The proposed secret sharing is based on finite field extension and Blakley secret sharing. Based on different parameters the proposed method is compared with existing ones. Here we also claim that same finite field extension method can be used over Shamir's secret sharing to improve the results.

1.2 Organization

The rest of the paper is organized as follows: Section 2 covers required background and preliminaries. Section 3 gives an idea of proposed method. Section 4 is about analysis and discussion of proposed scheme. Section 5 concludes with final remarks.

2. Background & Preliminaries

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

2.1 Threshold secret sharing scheme

In secret sharing there is one dealer and n players. The dealer distributes shares to each player 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(perfect) . Such a system is called a (t,n) - threshold scheme [19].

2.2 Shamir's secret sharing scheme [1]

Adi- Shamir idea for secret scheme was 2 points can define a line, 3 points can define a parabola, 4 points 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 is due to 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 k as secret and n shareholders { P_1,P_2,P_3, …..,P_n}. Using t-1 degree random polynomial with random coefficient.

Step 1: Polynomial construction

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

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 .

This scheme have some limitations like computationally hard, larger the share size, more memory is required which lowers the efficiency etc [25].

2.3 Blakley's secret sharing scheme [2]

As per [2][16] Blakley is based on hyper plane geometry.To solve a (t, n) threshold secret sharing scheme problem,each of the participant is given a hyper-plane equation in a t dimensional space over a finite field such that each hyper plane passes through a certain point. When t participants come together, they can solve the system of equations to find the secret.The point of intersection of the hyper planes is the secret in t dimensional space.An affine hyper plane in a t-dimensional space with coordinates in a field F can be described by a linear equation of the following form:

$a_1 x_1 + a_2 x_2 + ... + a_t x_t = b$

Reconstruction or recovery of original secret is simply by solving a linear system of equations.By finding the inter-section of any t of these hyper planes will get intersection point(secret). The secret can be any of the coordinates of the intersection point or any function of the coordinates. The most common application of Blakley's scheme is in distributing a key between different participants and reconstructing the key based on each share. Due to large space states this method is not efficient enough.

3. MATHEMATICAL FORMULATION OF THE PROBLEM

Assume the number of elements of field extension be $q = p^m$ (p is prime and $m \in Z+$). We choose the secret and IDs of participants from the following set.

$Mq = \{u \mid 0 \leq u \leq q\ 1, u \in Z\}$……(1)

One way to define Galois field or Finite fields is to transform the selected integers to the polynomials of (GF(q))[x] by Algorithm 1 as follows :

Algorithm 1.

Input: $u \in Mq$

Output: $v \in GF(q)$ or F(q) [Finite fields are also called as Galois fields].

Step 1: u is transformed into vectors of length with respect to base .

Step 2: All these vectors can be written as a polynomial in $F_q[x]$.

Example 1. Consider $7 \in M_8 \Rightarrow 7 = (111)_2 = \theta^2 + \theta + 1 \in GF(8)$, where θ is a primitive element of GF(8).

Example 2. Consider $5 \in M_9 \Rightarrow 5 = (12)_3 = \theta + 2 \in GF(9)$, where θ is a primitive

element of GF(9).

Then obtained polynomials can be transformed to integers by Algorithm 2 as follows:

Algorithm 2.

Input: $v \in GF(q)$

Output: $u \in Mq$

Step 1: v is transformed into vectors of length m with respect to base p.

Step 2: These vectors are written with respect to base 10.

Example 3. Let $\theta^2+\theta+1 \in GF(8) \Rightarrow \theta^2+\theta+1 = (111)_2 = 7 \in M_8$, where θ is a primitive element (root) of GF(8).

Example 4. Let $2\theta + 1 \in GF(9) \Rightarrow 5 = (21)_3 = 7 \in M_9$, where θ is a primitive element of GF(9).

3.1 Proposed Scheme using Blakley's secret sharing scheme as base

Consider the finite field F_q is the secret space. Here we are proposing a (k,n) threshold scheme based on Blakley's method i.e. at least k participants out of n will recover the secret.

Steps for Share Distribution :

1) Choose any vector $x=(x_1,x_2,x_3,\ldots x_m) \in Mq$ whose first coordinate (here x_1) is the secret.

2) Consider n vectors of length m to find the secret pieces for all n participants.

3) Let these be A_{u1} , A_{u2} , A_{u3} ,…., A_{un} .

4) Then calculate the secret pieces for each n participants such that

$Y_{u\,1} = A_{u1} \,.\, x^T$

$Y_{u\,2} = A_{u2} \,.\, x^T$

$Y_{u\,3} = A_{u3} \,.\, x^T$

…..

$Y_{u\,n} = A_{un} \,.\, x^T$

5) Transform values of $Y_{u\,i}$ $(1 \leq i \leq n)$ to the elements of Fq .

Steps for Secret Recovery:

Assume that $u_1,u_2,u_3,\ldots,u_k$ participants can recover the secret.Here it is the following linear equation system.

$Y = A \cdot x^T$

$$\begin{pmatrix} A_{u1} \\ A_{u2} \\ A_{u3} \\ \ldots\ldots \\ A_{uk} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \ldots\ldots \\ x_k \end{pmatrix} = \begin{pmatrix} Y_{u1} \\ Y_{u2} \\ Y_{u3} \\ \ldots\ldots \\ Y_{uk} \end{pmatrix}$$

The secret can be reached by solving above system of equation.

If the matrix A is non-singular, then the secret can be recovered. Otherwise it cannot be recovered.

Example 5. Let F_8 be the secret space, the number of participants n= 5, the threshold value k=3 and the secret s = 4. Construct a secret sharing scheme based on F_8 with these parameters by using Blakley's method.

Consider the polynomial $f(x) = x^3+x^2+1$ which is irreducible over F_2. Let Θ be a root of f. We know that if $f \in F_2[x]$ is an irreducible polynomial over F_2 degree , then by adjoining a root of f to F_2, we get a finite field with 2^d elements[24].

Assume θ to be a root of irreducible polynomial f(x). The elements of F_8 are as following.

$F_8 = \{ 0, 1, \theta, \theta+1, \theta^2, \theta^2+1, \theta^2+\theta, \theta^2+\theta+1\}$

$\theta^1 = \theta$

$\theta^2 = \theta^2$

$\theta^3 = \theta^2+1$

$\theta^4=\theta^2+\theta+1$

$\theta^5=\theta+1$

$\theta^6=\theta^2+\theta$

$\theta^{7=} \theta^0 =1$

The transformation between M_8 and F_8 is as follows.

$0 \longrightarrow 0$

$1 \longrightarrow 1$

$2 \longrightarrow \theta$

$3 \longrightarrow \theta + 1$

$4 \longrightarrow \theta^2$

$5 \longrightarrow \theta^2 + 1$

$6 \longrightarrow \theta^2 + \theta$

$7 \longrightarrow \theta^2 + \theta + 1$

We choose the vector $(5, 2, 3) \in M_8$ whose first coordinate $x_1=5$ is the secret.

Since the scheme will be (3, 5)-threshold scheme, we consider the five vectors as the participants.

Let us these vectors be

$A_{u1} = (0, 2, 2)$

$A_{u2} = (1, 3, 3)$

$A_{u3} = (1, 5, 5)$

$A_{u4} = (0, 3, 2)$

$A_{u5} = (5, 2, 5)$

These vectors correspond to the following vectors in $F_8[x]$.

$A_{u1}' = (0, \theta, \theta)$

$A_{u2}' = (1, \theta + 1, \theta + 1)$

$A_{u3}' = (1, \theta^2 + 1, \theta^2 + 1)$

$A_{u4}' = (0, \theta + 1, \theta)$

$A_{u5}' = (\theta^2 + 1, \theta, \theta^2 + 1)$

Now we calculate the secret pieces as below.

$Y_{u\,1} = (0, \theta, \theta) .(\theta^2 + 1, \theta, \theta+1)^T = \theta$

$Y_{u2} = (1, \theta + 1, \theta + 1) .(\theta^2 + 1, \theta, \theta+1)^T$

$= \theta^2+\theta=\theta^6$

$Y_{u3} = (1, \theta^2 + 1, \theta^2 + 1) \cdot(\theta^2 + 1, \theta, \theta+1)^T = 0$

$Y_{u4} = (0, \theta + 1, \theta) (\theta^2 + 1, \theta, \theta+1)^T = 0$

$Y_{u5} = (\theta^2 + 1, \theta, \theta^2 + 1) .(\theta^2 + 1, \theta, \theta+1)^T = 0$

When three participants combine their shares the secret will be recovered since the scheme is a (3, 5)-threshold scheme. Assume that the participants with number 2, 4, 5 can recover the secret.

$$\left(\begin{array}{ccc|c} 1 & \theta^5 & \theta^5 & \theta^6 \\ 0 & \theta^5 & \theta & 0 \\ \theta^3 & \theta & \theta^3 & 0 \end{array}\right) \xrightarrow[l_3 \to \theta^4 l_3 + l_1]{l_2 \to \theta^2 l_2}$$

$$\left(\begin{array}{ccc|c} 1 & \theta^5 & \theta^5 & \theta^6 \\ 0 & 1 & \theta^3 & 0 \\ 0 & 0 & \theta & \theta^6 \end{array}\right) \xrightarrow{l_3 \to \theta^6 l_3}$$

$$\left(\begin{array}{ccc|c} 1 & \theta^5 & \theta^5 & \theta^6 \\ 0 & 1 & \theta^3 & 0 \\ 0 & 0 & 1 & \theta^5 \end{array}\right) \xrightarrow{l_2 \to l_2 + \theta^3 l_3}$$

$$\left(\begin{array}{ccc|c} 1 & \theta^5 & \theta^5 & \theta^6 \\ 0 & 1 & 0 & \theta \\ 0 & 0 & 1 & \theta^5 \end{array}\right) \xrightarrow{l_1 \to l_1 + \theta^5 l_2 + \theta^5 l_3}$$

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & \theta^3 \\ 0 & 1 & 0 & \theta \\ 0 & 0 & 1 & \theta^5 \end{array}\right)$$

$x_1 = \theta^3 = \theta^2 + 1 \Rightarrow x_1 = 5 \in M_8$

$x_2 = \theta \Rightarrow x_2 = 2 \in M_8$

$x_3 = \theta^5 = \theta + 1 \Rightarrow x_3 = 3 \in M_8$

$x = (5, 2, 3)$

It is seen that the secret $s = x_1 = 5$ recovered.

4. Analysis & Discussion

4.1 Security Analysis

In the proposed sharing algorithm the secret is split into shares and it is reconstructed by collecting pieces. Secret is computed by doing computations in field extension. To do so a new approach in the elements of the field extension is used. The secret can be reached every element of field extension F_q ($q = p^m$) can be uniquely expressed l in θ over Fp . So, this scheme is very strong and reliable.

4.2 Performance Analysis

The access structure of this scheme consists of the *k* elements. So the performance of the system will increase.

4.3 Comparative study analysis

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

Table I. Comparison of different threshold secret sharing schemes [25][8]

Parameters	**Secret Sharing Scheme**				
	Shamir[1]	**Blakley**[2]	**Mignotte**[5]	**Asmuth-Bloom**[3]	**Proposed**
Techniques used	Polynomial interpolation	Vector space (Hyper plane)	Chinese reminder theorem	Chinese reminder theorem	Vector space and finite fields
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
Security	Low	Low	Low	Low	High

5. Conclusion

Here we proposed a new approach of threshold secret sharing over finite field extension based on Blakely secret sharing. Due to the finite fields the security of the scheme is increased. This scheme is reliable. Using this technique of finite field extension we can create a secret sharing scheme over finite field extension based on Shamir secret sharing in similar fashion. This method has lots of application in image secret sharing.

REFERENCES

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

[2] G. Blakely, "Safeguarding cryptographic keys", Proceedings of the AFIPS 1979 National Computer Conference, vol. 48, Arlington, VA, June 1997, pp. 313–317.

[3] C. Asmuth and 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 and 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 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

[24]Selda Calkavur , Fatih Molla ,"The Blakely based secret sharing approach", Sigma Journal of Engineering and Natural Sciences,37 (2), 2019, pp.489-494

[25]Vanashree Gupta,Smita Bedekar,"Alternative to Shamir's Secret Sharing Scheme Lagrange Interpolation over Finite Field",International Journal of Technical Research & Science (IJTRS) ,V6-I3-002 , March 2021, ISSN: 2454-2024 , https://doi.org/10.30780/IJTRS.V06.I03.002