Sigma J Eng & Nat Sci 37 (2), 2019, 489-494

Sigma Journal of Engineering and Natural Sciences
Sigma Mühendislik ve Fen Bilimleri Dergisi

Research Article

THE BLAKLEY BASED SECRET SHARING APPROACH

Selda ÇALKAVUR*[1], Fatih MOLLA[2]

[1]*Mathematics Department, Kocaeli University, KOCAELI;* ORCID: 0000-0002-1502-123X
[2]*Information Technology, Kocaeli University, KOCAELI;* ORCID: 0000-0003-0164-330X

Received: 18.02.2019 Revised: 14.03.2019 Accepted: 21.03.2019

ABSTRACT

Hiding a secret is needed in many situations. One might need to hide a password, an encryption key, a secret recipe and etc. Information can be secured with encryption, but the need to secure the secret key used for such encryption is also important. Imagine you encrypt your important files with are secret key and if such a key is lost, then all the important files will be inaccessible. Thus, secure and efficient key management mechanisms are required. One of them is secret sharing scheme that lets you split your secret into several parts and distribute them among selected parties. The secret can be recovered once these parties collaborate in some way. In this paper we propose a new approach to construct Blakley's scheme by using the finite fields.

Keywords: Secret sharing, threshold scheme, finite fields.

1. INTRODUCTION

Secret sharing schemes are one of the key management or establishment scheme invented separately in 1979 by both Shamir [10] and Blakley [2] as a solution to safeguarding cryptographic keys. Secret sharing schemes are also used to protect other types of secrets, such as a secret recipe or a password to a bank vault, control access of nuclear weapons and others. We need these schemes because many cryptosystems that use a single master key have various vulnerabilities. For instance, if the master key is disclosed to the public by accident or by an attacker, this will compromise the entire system. Also, if the master key is lost, then all the other keys it protects become inaccessible. Additionally, if the owner of the master key turns out to be disloyal then all sensitive information will be leaked to the opponents [12]. In addition, these schemes are useful when we do not trust a single person owning a certain secret. Thus it is needed the secret sharing schemes.

Secret sharing schemes are a technique used to hide a piece of information called the secret by splitting this secret into several parts called shares and distributing them among participants. The secret can be recovered from certain subsets of the shares. The one who produces such shares and privately distributes them to the participants called a dealer [6].

Secret sharing schemes have been applied different applications such as Secure Multiparty Computation, Threshold Cryptography, Key Recovery Mechanism, Distributed Certificate Authorities, Distributed Information Storage, Location Privacy, Key Management in Ad-hoc

[*] Corresponding Author: e-mail: selda.calkavur@kocaeli.edu.tr, tel: (262) 373 28 02 / 117

Networks, Information Hiding, Fair Exchange, Secure Online Auctions, Electronic Voting and many others [8], [9].

In [7] Noura Al Ebri and et al. studied on secret sharing schemes and their applications.

In this paper we propose a new approach to construct Blakley's scheme by using the finite fields. Blakley's method [2] uses principles of geometry to share the secret. In [3], Blakley et al. only provide a guideline on how to design a matrix of linear systems for perfect secrecy, and no actual matrix was given. Recently, researchers began to use Blakley's geometry-based secret sharing approach in the area of secret image sharing [5], [11].

The rest of this paper is organized as follows. Section II overviews the secret sharing schemes and reminds Blakley's scheme. Section III proposes our new approach to construct a secret sharing scheme based on Blakley's method.

2. OVERVIEW OF SECRET SHARING SCHEMES

Secret sharing is a technique by which a dealer spreads shares, which are pieces of the secret, to participants in a way that only authorized subsets of participants can recover the secret. Secret sharing schemes are very important in cryptography and they are a key building block for many secure protocols. Such as threshold cryptography, access control, attribute-based encryption, Byzentine agreement, generalized oblivious transfer and general protocol for multiparty computation [1].

We will need the following notations to define secret sharing schemes:

- Shares or shadows which are pieces of information. In this secret sharing scheme these shares have the property that certain authorized group of shares can reconstruct the secret, and no other unauthorized group of shares can reconstruct the secret.
- Set of all possible shares called the share set.
- The secret, it could be a key or message or any valuable information.
- Set of participants who are the parties that will receive the shares.
- The dealer who chooses the secret key and distributes them to the participants.
- The access structure which is a subset of the participants set and the elements in this structure are the authorized combinations of participants whose shares can be used to retrieve the secret.

Thus, we can say that for any secret sharing scheme it has the following two process.

- Distribution Process: This process's input is the secret that gets portioned into n number of shares $s_1, s_2, \cdots, s_n$ that is privately delivered to the participants.
- Reconstruct Process: The secret can be reconstructed when a suitable set of shares is present using a certain algorithm.

2.1. Threshold Secret Sharing Schemes

These schemes are the first kind of schemes that were constructed individually by both Shamir who uses polynomial interpolation [10] and Blakley who uses finite geometry [2]. A (t, n)-threshold scheme is a method of distribution of information among n participants such that $t > 1$ can reconstruct the secret but $(t - 1)$ can not.

2.2. Blakley Secret Sharing Scheme

This is one of the very first secret sharing scheme and is based on finite geometry [7]. This scheme uses hyperplane geometry as a solution to the secret sharing problem. To generate a (t, n)-threshold scheme each of the n participants is given hyperplane equation in a t-dimensional space over a finite field. In some cases, each hyperplane passes through a certain point. The secret is the intersection point of the hyperplanes. Once participants need to reconstruct the secret by solving the system of equations [4].

2.3. A New Approach to Construct a Secret Sharing Scheme Based on Blakley's Method

In this section, we propose a new approach to construct Blakley's scheme by using the finite fields.

Let the number of elements of finite field be $q = p^m$, where p is a prime number and $m \in \mathbb{Z}^+$.

We choose the secret and IDs of participants from the following set.

$$M_q = \{ a \mid 0 \leq a \leq q-1, a \in \mathbb{Z} \} \tag{1}$$

We transform the selected integers to the polynomials of $\mathbb{F}_q[x]$ by Algorithm 1.

Algorithm 1.
input: $a \in M_q$
output: $b \in \mathbb{F}_q$

Step 1. a is transformed into vectors of length m with respect to base p.
Step 2. these vectors are written as a polynomial in $\mathbb{F}_q[x]$.

Example 1.
Consider $4 \in M_8 \Rightarrow 4 = (100)_2 = \theta^2 \in \mathbb{F}_8$, where θ is a primitive element of $\mathbb{F}_8$.

We transform the obtained polynomials to the integers by Algorithm 2.

Algorithm 2.
input: $b \in \mathbb{F}_q$
output: $a \in M_q$
Step 1. b is transformation into vectors of length m with respect to base p.
Step 2. these vectors are written with respect to base 10.

Example 2.
Consider $\theta^2 \in \mathbb{F}_8 \Rightarrow \theta^2 = (100)_2 = 4 \in M_8$.

2.4. Proposed Scheme

We consider the finite field $\mathbb{F}_q$ is the secret space. We try to construct a (k,n)-threshold scheme based on Blakley's method. ($n \leq q$, the size of k participants is m)

We choose any vector $x = (x_1, x_2, \cdots, x_m) \in M_q$ whose first coordinate is the secret.

Since the scheme will be a (k,n)-threshold scheme, at least k participants out of n will be recovered the secret.

Consider n vectors of length m to find the secret pieces for all n participants. Let these be $A_{u_1}, A_{u_2}, \cdots, A_{u_n}$.

Then calculate the secret pieces for each n participants such that

$$\begin{gathered} y_{u_1} = A_{u_1} \cdot x^T \\ y_{u_2} = A_{u_2} \cdot x^T \\ \vdots \\ y_{u_n} = A_{u_n} \cdot x^T \end{gathered}$$

These values of y_{u_i} $(1 \leq i \leq n)$ transform to the elements of $\mathbb{F}_q$.

Assume that $u_1, u_2, \cdots, u_k$ participants can recover the secret. In this case it is constructed the following linear equation system.

$$A \cdot x^T = y \tag{2}$$

$$\begin{pmatrix} A_{u_1} \\ A_{u_2} \\ \vdots \\ A_{u_k} \end{pmatrix}_{k\times k} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix}_{k\times 1} = \begin{pmatrix} y_{u_1} \\ y_{u_2} \\ \vdots \\ y_{u_k} \end{pmatrix}_{k\times 1} \tag{3}$$

The secret can be reached by solving above equation system.

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

Example 3. Assume that $\mathbb{F}_8$ is the secret space. Let the number of participants be $n = 5$, the threshold value be $k = 3$ and the secret be $s = 4$. We construct a secret sharing scheme based on $\mathbb{F}_8$ with these parameters by using Blakley's method.

Consider the polynomial $f(x) = x^3 + x^2 + 1$ which is irreducible over $\mathbb{F}_2$. Let θ be a root of f. We know that if $f \in \mathbb{F}_2[x]$ is an irreducible polynomial over $\mathbb{F}_2$ degree d, then by adjoining a root of f to $\mathbb{F}_2$, we get a finite field with 2^d elements.

Let θ be a root of $f(x)$. So the elements of $\mathbb{F}_8$ are the following.

$$\mathbb{F}_8 = \{ 0, 1, \theta, \theta+1, \theta^2, \theta^2+1, \theta^2 + \theta, \theta^2 + \theta + 1 \}$$

$$\theta^1 = \theta$$
$$\theta^2 = \theta^2$$
$$\theta^3 = \theta^2 + 1$$
$$\theta^4 = \theta^2 + \theta + 1$$
$$\theta^5 = \theta + 1$$
$$\theta^6 = \theta^2 + \theta$$
$$\theta^7 = 1$$

The transformation between M_8 and $\mathbb{F}_8$ 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 $x = (6, 3, 4) \in M_8$ whose first coordinate 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

$$\mathrm{A}_{\mathrm{u}_1} = (0, 2, 2)$$
$$\mathrm{A}_{\mathrm{u}_2} = (1, 3, 3)$$
$$\mathrm{A}_{\mathrm{u}_3} = (1, 5, 5)$$
$$\mathrm{A}_{\mathrm{u}_4} = (0, 3, 2)$$
$$\mathrm{A}_{\mathrm{u}_5} = (5, 2, 5)$$

These vectors correspond to the following vectors in $\mathbb{F}_8[x]$.

$$\mathrm{A}'_{\mathrm{u}_1} = (0, \theta, \theta)$$
$$\mathrm{A}'_{\mathrm{u}_2} = (1, \theta + 1, \theta + 1)$$
$$\mathrm{A}'_{\mathrm{u}_3} = (1, \theta^2 + 1, \theta^2 + 1)$$
$$\mathrm{A}'_{\mathrm{u}_4} = (0, \theta + 1, \theta)$$

$$\mathrm{A}'_{\mathrm{u}_5} = (\theta^2+1,\theta,\theta^2+1)$$

Now we calculate the secret pieces as below.

$$y_{u_1} = (0,\theta,\theta)\cdot(\theta^2+\theta,\theta+1,\theta^2)^T = \theta+1 = \theta^5$$
$$\mathrm{y}_{\mathrm{u}_2} = (1,\theta+1,\theta+1)\cdot(\theta^2+\theta,\theta+1,\theta^2)^{\mathrm{T}} = \theta$$
$$\mathrm{y}_{\mathrm{u}_3} = (1,\theta^2+1,\theta^2+1)\cdot(\theta^2+\theta,\theta+1,\theta^2)^{\mathrm{T}} = \theta^2+\theta+1 = \theta^4$$
$$\mathrm{y}_{\mathrm{u}_4} = (0,\theta+1,\theta^2)\cdot(\theta^2+\theta,\theta+1,\theta^2)^{\mathrm{T}} = 0$$
$$\mathrm{y}_{\mathrm{u}_5} = (0,\theta+1,\theta^2)\cdot(\theta^2+\theta,\theta+1,\theta^2)^{\mathrm{T}} = 1$$

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

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

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

$$x_3 = \theta^2 \Rightarrow x_3 = 4 \in M_8$$
$$x_2 = \theta^5 = \theta+1 \Rightarrow x_2 = 3 \in M_8$$
$$x_1 = \theta^6 = \theta^2+\theta \Rightarrow x_1 = 6 \in M_8$$
$$x = (6,3,4)$$

It is seen that the secret $s = x_1 = 6$.

4. SECURITY ANALYSIS

Finally, the security of the proposed approach is analyzed. The proposed sharing algorithm shares the secret is splitted to n shares and it is reconstructed by collecting k pieces. The secret any the pieces are elements of a finite field. We know that these elements are uniquely determined. So the proposed approach is very reliable since there are no shadows of them.

5. CONCLUSION

This study presents the Blakley based secret sharing approach. We obtain the finite fields. The security is increased thanks to the finite fields.

REFERENCES

[1] Beimel, A., Chee, Y. M., Gwo, I., Ling, S., Shao, F., Tang, Y., Wang, H., and Xing, C., (ed), Secret Sharing Schemes: A Study, Springer, 2011, 6639, pp. 11-46.

[2] Blakley, G. R., Safeguarding Cryptographic Keys, *AFIPS Conf. Proc., vol. 48*, pp. 313-317, 1979.

[3] Blakley, G. R. and Kabatianski, G. A., Linear Algebra Approach to Secret Sharing Schemes, *In Proc. of Error Control, Cryptology and Speech Compression, Lecture Notes in Computer Science, vol 229*, pp. 33-40, 1994.

[4] Bozkurt, I. N., Kaya, K., Selçuk, A. A., Güloğlu, A. M., Threshold Cryptography Based on Blakley Secret Sharing, *In Proc. of Information Security and Cryptology 2008*, Ankara, Turkey, Dec. 2008.

[5] Chen, C. C. and Fu, W. Y., A Geometry Based Secret Image Sharing Approach, *Journal of Information Science and Engineering, vol. 24, no. 5,* pp. 1567-1577, 2008.

[6] Csirmaz, L. and Tardos, G., On-line secret sharing, *Cryptology ePrint Archive*, Report 2011/174, 2011.

[7] Ebri, N. Al and Yeun, C. Y., Study on Secret Sharing Schemes (SSS) and Their Applications, *6th International Conference on Internet Technology and Secured Transactions*, 11-14 December 2011, Abu Dhabi, United Arab Emirates, pp. 40-45, 2011.

[8] Iftere, S., Secret sharing schemes with applications in security protocols, *Technical Report TR 07-01, University Alexandruloan Cuza of Iasi, Faculty of Computer Science*, January 2007.

[9] Martin, K., Challenging the Adversary Model in Secret Sharing Schemes, *In Coding and Cryptography II, Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts*, pp. 45-63, 2008.

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

[11] Tso, H. K., Sharing Secret Images Using Blakley's Concept, *Optical Engineering, vol. 47, no. 7,* pp. 21-23, 2008.

[12] Tso, R., A Study on Secret Sharing Schemes with Dishonest Dealers and Participants, *University of Tsukba*, January 2004.