1st International Conference on Frontiers in Academic Research

https://www.icfarconf.com/

February 18-21, 2023, Konya, Turkey

Vector space multisecret-sharing scheme based on Blakley's method

Selda Çalkavur*, Patrick Solé [2]

[1]*Department of Mathematics/Faculty of Arts and Science, Kocaeli University, Turkey*
[2]*CNRS, I2M/Centrale Marseille, Aix Marseille University, France*

*(selda.calkavur@kocaeli.edu.tr) *Email of the corresponding author*

Abstract – Secret sharing schemes were introduced by Adi Shamir and George Blakley, independently, in 1979. In a (k, n)- threshold secret sharing scheme, any set of at least k out of n participants can retrieve the secret but no set of $(k-1)$ or less can. Shamir's secret sharing scheme is more popular than Blakley's, even though the former is more complex than the latter. The practical reason is that Blakley's scheme lacks determined, general and suitable matrices. In this paper, we present a multisecret-sharing scheme based on vector spaces over R^n and use Blakley's method. This scheme is ideal in the sense that the size of each secret equals the size of any share.

Keywords – Secret Sharing, Multisecret-Sharing Scheme, Ideal Scheme, Blakley Method, Vector Space

I. INTRODUCTION

The secure storage of the private keys of a cryptosystem is an important problem in cryptography and security. The possession of a highly sensitive key by an individual may not be desirable as the key can easily be lost or as the individual may not be fully trusted. Giving copies of the key to more than one individual increases the risk of compromise. A solution to this problem is to give shares of the key to several individuals, forcing them to cooperate to find the secret key. This not only reduces the risk of losing the key but also makes compromising the key more difficult. In threshold cryptography, secret sharing deals with this problem. The secret is shared among a group of n users so that only when a sufficient number k of them come together can the secret be reconstructed. In the literature well-known secret sharing schemes include Shamir [16] based on polynomial interpolation, Blakley [3] based on hyperplane geometry, and Asmuth-Bloom [2] based on the Chinese Remainder Theorem. These schemes are called (k, n)- threshold secret sharing.

In this paper, we use Blakley's scheme. Blakley's method [3] uses principles of geometry to share the secret. In [4], Blakley et al. only provided 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 [6], [17]. Chen et al. [6] and Tso [17] independently applied Blakley's scheme for secret image sharing. Ulutaş et al. [18] proposed an enhanced scheme for secret image sharing, which adopts Blakley's secret sharing method and Steganography together to share the secret and create meaningful shares. As for threshold cryptography, Bozkurt et al. [5] proposed the first threshold RSA signature scheme as the underlying secret sharing scheme. Hei, Du and Song [10] present two matrices that can be used for Blakley's secret sharing scheme.

Multisecret-sharing schemes form another family of secret sharing schemes. This scheme was proposed [11], [9], [13], [15], [19], [7]. Karnin et al. [12] examined the following situation. There are k secrets $s_1, s_2, \dots, s_k$ to be shared. Such systems are

called $[k, m, n]$- (multisecret-sharing) threshold schemes. Each $[k, m, n]$- threshold scheme for multisecret-sharing gives k single-secret (m, n)-threshold schemes [8].

In this work, we propose a new multisecret-sharing scheme based on vector spaces over R^n. We consider any basis elements of R^n. The proposed scheme is ideal by means of information rate and secure. We use Blakley's method to share and recover the secret. We determine the access structure of this scheme and anlayze its security.

The rest of the paper is organized as follows. In Section II we introduce Blakley's secret sharing scheme. In Section III we present a new multisecret-sharing scheme using Blakley's method and analyze its security. Section IV collects concluding remarks.

II. BLAKLEY'S SECRET SHARING SCHEME

Blakley's secret sharing scheme uses hyperplane geometry to solve the secret sharing problem. The secret is a point in a t- dimensional space and n shares are affine hyperplanes that pass through this point. An affine hyperplane in a t- dimensional space with coordinates in a commutative field F can be described by a linear equation of the following form.

$$a_1x_1 + a_2x_2 + \cdots + a_tx_t = b$$

The intersection point is obtained by finding the intersection of any t of these hyperplanes. The secret can be any of the coordinates of the intersection point or any function of the coordinates. We take the secret to be the first coordinate of the point of intersection.

A. *Dealing Phase*

Let F be the field we are working on. The dealer generates a secret point x in F, where the first coordinate x_1 is set to the secret value and sets the values of the other coordinates randomly from the field F. The ith user will get a hyperplane equation over F,

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{it}x_t = y_i \quad (1)$$

For a (t, n)- threshold scheme there will be n such hyperplane equations, and hence we will have an $n \times t$ linear system,

$$AX = Y. \quad (2)$$

The dealer then sends the secret value of y_i along with $a_{i1}, a_{i2}, \dots, a_{it}$ to user i. The coefficients a_{ij} are not sensitive and can be made publish if needed.

B. *Share Combining Phase*

Share combining step is simply finding the solution of a linear system of equations. Suppose that a coalition $S = \{i_1, i_2, \dots, i_t\}$ of users come together. They form a matrix A_s using their hyperplane equations and solve

$$A_sX = Y_s, \quad (3)$$

where Y_s is the vector of the secret shares of the users. The secret is found as the first coordinate of the solution [13].

III. MULTISECRET-SHARING SCHEMES BASED ON VECTOR SPACES

Consider a finite-dimensional vector space. We construct a multisecret-sharing scheme based on this space.

- Let the vector space F^n be the secret space.
- Let any vector of F^n be the secret.

We know that if vector addition is defined to be matrix addition and vector scalar multiplication is defined to be matrix scalar multiplication, then the set W of all $n \times n$ matrices with real entries is a vector space.

Definition 1 [1]. If W is any vector space and

$$V = \{v_1, v_2, \dots, v_n\}$$

is a set of vectors in W, then V is called a basis for W if the following two conditions hold:

i) V is linearly independent,

ii) V spans W.

Theorem 1 [1]. If $V = \{v_1, v_2, \dots, v_n\}$ is a basis for a vector space W, then every vector v in W can be expressed in the form

$$v = c_1v_1 + c_2v_2 + \cdots + c_nv_n$$

in exactly one way, where $c_1, c_2, \dots, c_n \in R$.

A. *Proposed Method*

Now we construct a multisecret-sharing scheme based on the vector space F^n. Let any vector of F^n be the secret $S = (s_1, s_2, \dots, s_n)$. First we find any basis of F^n is called $V = (v_1, v_2, \dots, v_n)$ and calculate the shares $y_i, 1 \le i \le n$.

$$V.S^T = Y^T,$$

where V is an element of W. We write the following linear equation system for each participant.

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} . \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}^T = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

It can reach by solving this equation system.

The dimension of matrix V is $n \times n$ and the elements are the basis elements of F^n. The transpose

of S is denoted by S^T. The dimension of S is $n \times 1$. Y is a sharing vector.

Theorem 2. If the matrix V is non-singular, then the secret can be recovered. Otherwise, it cannot be reached.

Proof. If the matrix V is singular, then the vectors of V will be linearly dependent. In this case, these vectors do not consist of a basis of F^n.

Theorem 3. In this multisecret-sharing scheme we have the following facts.

i) The qualified set in the access structure is the set of all n participants.

ii) No subset of less than n participants can recover the secret.

Proof.

i) The secret is recovered thanks to the basis elements of F^n and their number is n.

ii) The number of basis elements cannot be less than n. Only n elements can be used to recover the secret but $(n-1)$ cannot.

Corollary 1. The multisecret-sharing scheme satisfying the hypothesis of the above theorem is also a (n, n)- threshold secret sharing scheme.

Proof. It is clear that the participants are the basis elements of F^n and their number is n. These n participants can be reached the secret by combining their shares.

Example 1. Consider the vectors

$$v_1 = (1, 2, 1), v_2 = (2, 9, 0), v_3 = (3, 3, 4).$$

The set $V = \{v_1, v_2, \dots, v_3\}$ is a basis for F^3.

- To show that the set V spans F^3, we must show that an arbitrary vector

$$b = (b_1, b_2, \dots, b_3)$$

can be expressed as a linear combination

$$b = c_1 v_1 + c_2 v_2 + c_3 v_3$$

of the vectors in V. Expressing this equation in terms of component gives

$$(b_1, b_2, \dots, b_3) = c_1(1, 2, 1) + c_2(2, 9, 0) + c_3(3, 3, 4),$$

where $c_1, c_2, \dots, c_3 \in F$ or

$$(b_1, b_2, \dots, b_3) = (c_1 + 2c_2 + 3c_3, 2c_1 + 9c_2 + 3c_3, c_1 + 4c_3)$$

on equating corresponding components

$$c_1 + 2c_2 + 3c_3 = b_1, \ , 2c_1 + 9c_2 + 3c_3 = b_2, c_1 + 4c_3 = b_3 \quad (4)$$

- Thus, to show that V spans F^3, we must demonstrate that the system (4) has a solution for all choices of $b = (b_1, b_2, \dots, b_3)$.

- To prove that V is linearly independent, we must show that the only solution of

$$c_1 v_1 + c_2 v_2 + c_3 v_3 = 0 \quad (5)$$

is $c_1 = c_2 = c_3 = 0$. As above, if (5) is expressed in terms of components, the verification of independence reduces to showing that the homogeneous system

$$c_1 + 2c_2 + 3c_3 = 0, 2c_1 + 9c_2 + 3c_3 = 0, c_1 + 4c_3 = 0 \quad (6)$$

has only the trivial solution. Observe that systems (4) and (6) have the same coefficient matrix. Thus, we can prove that in systems (4) and (6) the matrix of coefficients

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 9 & 3 \\ 1 & 0 & 4 \end{pmatrix}.$$

has a nonzero determinant, that is $|A| = -1$. So V is a basis for F^3.

Now we try to construct a multisecret-sharing scheme based on F^3. Let the secret vector be $S = (s_1, s_2, \dots, s_3) = (-3, 1, -1) \in F^3$. We calculate the shares as follows.

$$y_1{}^T = v_1 S^T = (1, 2, 1).(-3, 1, -1)^T = -2$$
$$y_2{}^T = v_2 S^T = (2, 9, 0).(-3, 1, -1)^T = 3$$
$$y_3{}^T = v_3 S^T = (3, 3, 4).(-3, 1, -1)^T = -10$$

The participants (the basis elements) can reach the secret by combining their shares as follows.

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 9 & 0 \\ 3 & 3 & 4 \end{pmatrix}.\begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} = \begin{pmatrix} -2 \\ 3 \\ -10 \end{pmatrix}.$$

It is seen that the secret $S = (s_1, s_2, \dots, s_3) = (-3, 1, -1)$ by solving the above linear system.

This multisecret-sharing scheme is also a $(3, 3)$-threshold scheme.

B. *Information Throughput*

Since the security of a system depends on the amount of information that must be kept secret, the size of the shares given to the participants is an important point in the design of secret sharing schemes. Besides, if the shares are too large, the memory requirements for the participants will be too strong, and the algorithms used to compute the shares will become inefficient. So one of the basic parameters in secret sharing is the **information rate** ρ of the scheme, which is defined in [14] to be the ratio between the length (in symbols) of the secret and the maximum length of the shares given to the participants.

A secret sharing scheme is said to be **ideal** if its information rate is equal to one, which is the

maximum possible value. So our scheme is ideal since the secret S is one of the element of F, like the share Y_i of the generic user i.

C. *Security Analysis*

In a secret sharing scheme, there exists the possibility that some participants lie about the value of their shares in order to obtain some illicit benefit. Therefore, the security against cheating is a key point in the implementation of secret sharing schemes. If $F = F_q$ a finite field of order q, one possible attack would be for s participants to collude together, and to guess the shares of the remaining $n - s$ users. It is readily seen that the probability of success of such an attack is $\frac{1}{q^{n-s}}$. Thus a safe system would require q to be large.

IV. CONCLUSION

In the present article, we have introduced a new multisecret-sharing scheme based on vector spaces over the F vector space F^n for some field F. The reconstruction algorithm is based on Blakley's method. We determine the access structure, and calculate the information rate of this scheme. We have analyzed its information flow. The new system is ideal in a precise sense in terms of information throughput. It is reasonably secure if a sufficiently large field is used.

The choice of a field depends on the practical application and machine implementation. Using a finite field $F = F_q$ might require a large size q in view of probabilistic attacks. Using an infinite field like the reals removes this security problem at the price of a possible computational burden and precision issues. So we have performed to expose our system for a general computation field F.

REFERENCES

[1] H. Anton, C. Rorres, *Elementary Linear Algebra, Applications Version*, USA, 1994.

[2] C. Asmuth and J. Bloom, *A modular approach to key safeguarding*, IEEE Trans. Information Theory, vol. 29, no. 2, pp. 208-210, 1993.

[3] G. R. Blakley, *Safeguarding Cryptographic Keys*, in Proc. 1979 National Computer Conf., New York, pp. 313-317, Jun. 1979.

[4] G. R. Blakley and G. A. Kabatianski, *Linear algebra approach to secret sharing schemes*, in Proc. of Error Control, Cryptology and Speech Compression, Lecture Notes in Computer Science, vol. 829, pp. 33-40, 1994.

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

[6] C. C. Shen and W. Y. Fu, *A geometry-based secret image sharing approach*, Journal of Information Science and Engineering, vol. 24, no. 5, pp. 1567-1577, 2008.

[7] S. Çalkavur, P. Solé, *Multisecret-sharing schemes and bounded distance decoding of linear codes*, International Journal of Computer Mathematics, vol. 94, no. 1, pp. 107-114, 2017.

[8] C. Ding, T. Laihonen and A. Renvall, *Linear multisecret-sharing schemes and error correcting codes*, J. Comput. Sci. vol. 3, no. 9, pp. 1023-1036, 1997.

[9] J. He and E. Dawson, *Multistage secret sharing based on one-way function*, Electronic Letters, vol. 30, no. 19, pp. 1591-1592, 1994.

[10] X. Hei, X. Du, and B. Song, *Two Matrices for Blakley's Secret Sharing Scheme*, IEEE ICC 2012-Communication and Information Systems Security Symposium, pp. 810-814, 2012.

[11] L. Horn, Comment: *Multistage secret sharing based on one-way function*, Electronic Letters, vol. 31, no. 4, p. 262, 1995.

[12] E. D. Karnin, J. W. Greene and M. E Hellman, *On secret sharing systems*, IEEE Trans. Inf. Theory IT, vol. 29, no. 1, pp. 35-41, 1983.

[13] H. -X. Li, C. -.T. Cheng, and L. J. Pang, *A New (t, n)-Threshold Multisecret Sharing Scheme, CIS 2005, vol. 3802, pp. 421-426, 2005.*

[14] C. Padro, *Robust vector space secret sharing schemes*, Information Processing Letters 68, pp. 107-111, 1998.

[15] L. J. Pang and Y. -M. Wong, *A New (t, n)- multisecret-sharing scheme based on Shamir's secret sharing*, Applied Math, vol. 167, pp. 840-848, 2005.

[16] A. Shamir, *How to share a secret*, Comm. Of the ACM 22, pp. 612-613, 1979.

[17] H. K. Tso, *Sharing secret images using Blakley's concept*, Optical Engineering, vol. 47, no. 7, pp. 21-23, 2008.

[18] M. Ulutaş, V. V. Nabiyev and G. Ulutaş, *Improvements in Geometry-Based Secret Image Sharing Approach with Steganography*, Mathematical Problems in Engineering, vol. 53, pp. 101-110, 2009.

[19] C. -C. Yang, T. Y. Chang, M. -S. Hwang, *A New (t, n)-multisecret sharing scheme*, Applied Mathematics and Computation, vol. 151, pp. 483-490, 2004.