mathematics

MDPI

Article

Some Multisecret-Sharing Schemes over Finite Fields

Selda Çalkavur [1,*] and Patrick Solé [2]

[1] Math Department, Köseköy Vocational School, Kocaeli University, 41135 Kocaeli, Turkey
[2] I2M, Aix Marseille University, Centrale Marseille, CNRS, 12M, 163 Avenue de Luminy, 13009 Marseille, France; sole@enst.fr
* Correspondence: selda.calkavur@kocaeli.edu.tr

Received: 29 March 2020; Accepted: 22 April 2020; Published: 25 April 2020

Abstract: A secret sharing scheme is a method of assigning shares for a secret to some participants such that only some distinguished subsets of these subsets can recover the secret while other subsets cannot. Such schemes can be used for sharing a private key, for digital signatures or sharing the key that can be used to decrypt the content of a file. There are many methods for secret sharing. One of them was developed by Blakley. In this work, we construct a multisecret-sharing scheme over finite fields. The reconstruction algorithm is based on Blakley's method. We determine the access structure and obtain a perfect and ideal scheme.

Keywords: secret sharing; multisecret-sharing scheme; finite field; vector space

1. Introduction

A cryptosystem is an implementation of cryptographic techniques providing information security services. Encryption is the process of scrambling a message and can provide a means of securing information. A secret sharing scheme is an encryption method. The secret s is divided into n pieces called shares. The pieces alone have no information about the secret, but the secret can be reached by combining some pieces.

Secret sharing was first introduced by Shamir [1] and Blakley [2] in 1979. Shamir's scheme is constructed based on the Lagrange interpolation polynomial, as a (t, n)-threshold secret sharing scheme. In a (t, n)-threshold secret sharing scheme, the secret is divided into n shares and distributed each share to one of n parties called shareholders. Only t or more shareholders combining their shares together can recover the secret while $t - 1$ or fewer shareholders cannot obtain any information about the secret. There are several schemes [3–7] based on Shamir's scheme.

Blakley's method is based on finite geometry. In this scheme, the geometry of hyperplanes over a finite field is used to solve the secret sharing problem [8]. To generate a (t, n)-threshold scheme, each of the n participants is given a 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 hyperlanes. Once participants need to reconstruct the secret by solving the system of equations [9].

Multisecret-sharing schemes are one of the most important families of secret sharing schemes, since the secret has been constructed as multi party not single party. Thus, it is more difficult to reach the secret than for a single secret sharing scheme. Some multisecret-sharing schemes are constructed in [6,7,10–13]. In these schemes [6,13,14], there is a set of which consists of r secrets. The elements of this set can be shared and reconstructed at the same time or none of the r secrets can be retrieved. However, every (r, m, n)-multisecret-sharing scheme gives r single secret (m, n)-threshold schemes [15]. Especially, we presented in [10] a multisecret sharing scheme based on error correcting codes. Moreover, in [16], we constructed a new multisecret-sharing scheme based on LCD codes. The reconstruction algorithm is given by using Blakley's method.

In cryptosystems, the secure storage of private keys is an important problem. Secret sharing satisfies the distribution the private keys to the participants safely and does not trust a creature and central system. One type of such systems is blockchain systems. The private keys check the important seeds such as money and identities in this system. Their loss can have serious consequences. Thus, the distributed storage blockchain (DSB) scheme is introduced in [17,18]. Krawczyk [19] consolidated the DSB scheme with Shamir's [1] secret sharing scheme and private key encryption and information dispersal algorithm (IDA) [20]. The DSB scheme decreases the storage to a part of the original blockchain's impose.

Proactive secret sharing (PSS) was proposed by Herzberg et al. [21]. This is a stronger scheme by means of security. PSS is effective in the sharing of the shares to the participants when the secret s is kept. The participants get the new pieces of the secret s. These pieces are independent of the old ones and then the old pieces are removed. PSS protects the secret s from possible attacks.

Maram et al. [22] presented CHURP (CHUrn-Robust Proactive Secret Sharing). CHURP satisfies a secure secret sharing in dynamic setting. The collection of nodes keeps the secret changes in this scheme. It is also constructed for blockchains and has a simpler structure.

In the area of cryptocurrency, and blockchain design, secret sharing schemes (SSS) are used extensively, in particular in electronic voting [23], data storage [18], and wallet management [24]. The most used of these schemes is the Shamir scheme [1]. In this note, we explore a variant of an alternative scheme, the Blakley scheme. We show that the Blakley scheme is not adapted to finite fields. We give a multisecret scheme which exploits similar ideas.

The rest of the paper is organised as follows. In Section 2, we introduce Blakley's secret sharing scheme based on hyperplane geometry over the reals, and show it cannot work over finite fields. In Section 3, we construct a new multisecret-sharing scheme by using linear algebra over finite fields. We use Blakley's method and determine the access structure. Section 4 collects the concluding remarks.

2. Preliminaries

2.1. Blakley Threshold Secret Sharing Scheme

In a (t,n)-Blakley Scheme, the dealer selects a secret point $X = (x_1, x_2, \ldots, x_t)$ from $\mathbb{R}^t$. The secret key to be shared is the first coordinate of X. Other coordinates of X are random. For each participant $u \in P$, the dealer selects a random vector

$$A_u = (a_{u_1}, a_{u_2}, \ldots, a_{u_t}) \tag{1}$$

from $\mathbb{R}^t$ and assigns the scalar

$$y_u = A_u X^T = \sum_{i=1}^{t} a_{u_i} x_i$$

as the secret share to user u.

In other words, the dealer assigns a hyperplane equation that is passing through X to each participant u. When a t-member coalition $W = \{u_1, u_2, \ldots, u_t\}$ is present, they have t-hyperplanes passing through X. The linear system formed by the shares of $u_i \in W$ is

$$\begin{pmatrix} A_{u_1} \\ A_{u_2} \\ \vdots \\ A_{u_t} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{pmatrix} = \begin{pmatrix} y_{u_1} \\ y_{u_2} \\ \vdots \\ y_{u_t} \end{pmatrix}$$

$$M_W X^T = Y_W^T \tag{2}$$

where Y_W denotes the $1 \times t$ vector formed by the shares of participants included in W. Since all entries in M_W are generated randomly, M_W is nonsingular with probability one: the set of singular matrices forming a hypersurface in n^2 dimensions is of measure zero for the Lebesgue measure. Since M_W is nonsingular, the subset W can find the secret by solving the linear system in Equation (2). When a coalition $W^{'}$ of size $t^{'} < t$ is present, it only sees t' columns of A, yielding an underdetermined system to solve.

Qualified coalitions find the secret and unqualified coalitions gain no information about the secret.

Remark 1. *The Blakley scheme does not work well if we replace $\mathbb{R}$ with a finite field, because the probabilistic argument for the nonsingularity of M_w breaks down. Building a matrix of order n over the finite field $GF(q)$ by choosing its rows at random will not give a nonsingular matrix with probability one, even for large matrix order. The probability $P(n,q)$ of building a nonsingular n by n matrix over $GF(q)$ by random choice is*

$$P(n,q) = |GL(n,q)|q^{-n^2} = \prod_{j=1}^{n}(1-1/q^j),$$

by $|GL(n,q)| = \prod_{j=1}^{n}(q^n - q^{n-j})$ [25]. Since the infinite product $\prod_{j=1}^{\infty}(1-1/q^j)$ converges, we see that $P(n,q)$ tends to a finite value $\neq 1$ for $n \to \infty$.

For instance, for $q = 2$, we have the numerical approximation $P(n,2) \sim 0.29$, for $n \to \infty$.

2.2. Ramp Secret Sharing Scheme

Ramp secret sharing scheme is a cryptographic method to encode a secret s into multiple shares $s_1, \ldots, s_n$ that only from specified subsets of the shares one can recover s. In ramp schemes, a secret can be shared among a group of participants in such a way that only sets of at least k participants can reconstruct the secret and $k-1$ participants cannot [26].

A linear ramp secret sharing scheme is called **t-privacy** if from no set of size t one can guess any information about the secret, but from some set of size $t+1$ can recover some information about it.

3. Multisecret-Sharing Schemes over Finite Fields

3.1. Notation

In this section, we consider a finite extension $\mathbb{F} = \mathbb{F}_q^m$ of the finite field $K = \mathbb{F}_q$ as a vector space over K. Then, $\mathbb{F}$ has dimension m over K and if $\{\alpha_1, \ldots, \alpha_m\}$ is a basis of $\mathbb{F}$ over K, each element $\alpha \in \mathbb{F}$ can be uniquely represented in the form

$$\alpha = c_1\alpha_1 + ... + c_m\alpha_m$$

with $c_j \in K$ for $1 \leq j \leq m$.

3.2. Scheme Description

In this subsection, we examine a multisecret-sharing scheme over finite fields. To explain the reconstruction method, we use Blakley's algorithm.

- Let the vector space $\mathbb{F}_q^m$ be both the secret space and the participants set.
- Let any vector of $\mathbb{F}_q^m$ be the secret.

The m secrets are the m coordinates of a vector $X \in \mathbb{F}_q^m$. Let P denote an m-subset of participants. For each participant $u \in P$, the dealer selects a random vector

$$A_u = (a_{u_1}, a_{u_2}, \ldots, a_{u_t}) \tag{3}$$

from $\mathbb{F}_q^m$ and assigns the scalar

$$y_u = A_u X^T = \sum_{i=1}^{t} a_{u_i} x_i$$

as the secret share to user u. The linear system formed by the shares of $u_i \in W$ is

$$\begin{pmatrix} A_{u_1} \\ A_{u_2} \\ \vdots \\ A_{u_t} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_t \end{pmatrix} = \begin{pmatrix} y_{u_1} \\ y_{u_2} \\ \vdots \\ y_{u_t} \end{pmatrix}$$

$$M_W X^T = Y_W^T \tag{4}$$

Thus, we obtain a linear equation system in X and the secret can be retrieved by solving this system, provided M_W is non singular, or, equivalently, the family $(A_u)_{u \in W}$ is free.

Theorem 1. *This multisecret-sharing scheme has the following properties:*

(1) The access structure consists of sets of m elements.
(2) No subset of size less than m can be used in recovering the secret.

Proof. The following facts are immediate by basic linear algebra. (1) Any basis of $\mathbb{F}_q^m$ can recover the secret by combining their shares, as the matrix of the system in nonsingular in that case.

(2) The above system is undetermined in that case, because the matrix of the system is not square. □

Corollary 1. *This multisecret-sharing scheme is a (m, m)-threshold secret sharing scheme.*

Proof. The secret is recovered thanks to the basis elements of $\mathbb{F}_q^m$ in this scheme. Thus, each minimal access set consists of m elements. The size of secret is m, since it is any vector of $\mathbb{F}_q^m$. That is, in this scheme, all m secrets of X can be determined together. Therefore, the new scheme is a (m, m)-threshold scheme. □

Corollary 2. *The multisecret-sharing scheme satisfying the above theorem is also a ramp secret sharing scheme with $m - 1$ privacy.*

Proof. The number of participants retrieving the secret is m. This means the size of minimal access subsets is m. Thus, this scheme is also a ramp secret sharing scheme with $m - 1$ privacy by definition of a ramp secret sharing scheme. □

3.3. Statistics on Coalitions

Theorem 2. *Let $\mathbb{F}_q^m$ be the finite extension over the finite field $\mathbb{F}_q$. In a multisecret-sharing scheme over $\mathbb{F}_q$, the number of minimal coalitions is*

$$\frac{|GL(m, q)|}{m!} = \prod_{j=1}^{m} (q^m - q^{m-j}).$$

Proof. Recall that, in our scheme, the secret space is the finite extension $\mathbb{F}_q^m$ and the minimal access sets consist of the bases. These m participants can recover the secret together. Thus, the number of minimal coalitions is the number of rows of a nonsingular matrix of order m over $\mathbb{F}_q$ up to ordering. This number is calculated by the above formula. □

3.4. Security Analysis

Assume that $t < m$ participants collude together and agree to pool their share to try and guess the secret. For the attack to be better than random choice, we must assume that their corresponding vectors A_u are linearly independent. Assuming they correspond to a system of t linearly independent vectors, they can be completed into a basis in $X(t, m, q)$ ways. In general, this quantity is a complicated combinatorial coefficient. Let us assume the most favorable case to the attackers, that is $t = m - 1$. In that situation, the basis extension vector is any vector that is not in the linear span of the $m - 1$ vectors attached to the colluders. Thus, $X(t, m, q) = q^m - q^{m-1}$. This vector being chosen, there are q choices for its share.

Thus, the probability of success of the attack is $\frac{1}{(q-1)(q^m - q^{m-1})}$. To make this quantity small, we should operate the system with a large m. Having a large q would increase the computational burden of the field arithmetic.

3.5. Information Theoretic Efficiency

The ratio of the size of the secret to the size of the participants gives the information rate [27] of the secret sharing scheme. In this scheme, the secret is a vector of dimension m and its size is m. The sharings are the sets of basis elements and their size is m. Thus, the information rate is

$$\rho = \frac{m}{m} = 1.$$

This scheme is **ideal**, since $\rho = 1$.

3.6. Comparison with other Schemes

In this section, we compare our scheme with other secret sharing schemes in the literature by means of, in order, the number of participants, the size of a secret, and the number of coalitions for an arithmetic over $\mathbb{F}_q$. We denote by A, B, and C these three quantities in the Table 1. In the fourth column, the symbol t denotes the error-correcting capacity of code. As a basis of comparison, in Columns 2–4, we consider an $[n, k, d \geq 2t + 1]$-code over $GF(q)$. For codes of similar alphabets and dimensions, the new scheme allows exponentially more participants and more coalitions, compared to the other schemes, for a secret size of the same order of magnitude.

Massey's scheme has a single secret sharing system, not a multisecret-sharing. To recover the secret, the linear algebra in Ding's scheme is used. The reconstruction algorithm is based on the decoding in Çalkavur et al. scheme [10]. In our new system, to recover the secret, we use Blakley's method. However, the secret will be retrieved safely since the system has m independent equations and m unknowns. This means there exists a unique solution in the system.

Table 1. Comparison with other Schemes.

System	**[28]**	**[15]**	**[10]**	**This Paper**
A	$n-1$	n	n	q^m
B	q	q^k	q^k	q
C	$\binom{n}{k}$	$\binom{n}{k}$	$\geq \binom{n}{d-t}$	$\frac{\prod_{i=0}^{m-1}(q^m - q^i)}{m!}$
ρ	1	$\frac{k}{k-1}$	1	1

4. Conclusions

In [29], Çalkavur et al. introduced a new multisecret-sharing scheme based on vector spaces over the $\mathbb{F}$ vector space $\mathbb{F}^n$ for some field $\mathbb{F}$. In this work, we generalise the results in [29] and construct a multisecret-sharing scheme over finite fields. We use Blakley's algorithm to explain the recovering method of a secret. We determine the access structure, examine the statistics on coalitions and show the ideality and perfectness of our scheme. Attack analysis indicates that the important security parameter is the dimension m of the vector space we consider.

Compared to other schemes based on finite fields, our scheme displays for the same order of magnitude of parameters more users and more coalitions. It is also a multisecret scheme.

Author Contributions: Investigation, P.S.; and supervision, S.Ç. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
2. Blakley, G.R. Safeguarding Cryptographic Keys. In Proceedings of the 1979 International Workshop on Managing Requirements Knowledge (MARK), New York, NY, USA, 4–7 June 1979; Volume 48, pp. 313–317.
3. Fuyou, M.; Yan, X.; Xingfu, W.; Badawy, M. Randomized component and its application to (t, m, n)-group oriented secret sharing. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 889–899. [CrossRef]
4. Horn, L.; Lin, C. Strong (n, t, n) verifiable secret sharing scheme. *Inf. Sci.* **2010**, *180*, 3059–3064. [CrossRef]
5. Horn, L.; Hsu, C.; Zhang, M.; He, T.; Zhang, M. Realizing secret sharing with general access structure. *Inf. Sci.* **2016**, *367*, 209–220. [CrossRef]
6. Pang, L.J.; Wong, Y.-M. A New (t, n)-multisecret sharing scheme based on Shamir's secret sharing. *Appl. Math* **2005**, *167*, 840–848.
7. Yang, C.-C.; Chang, T.-Y.; Hwang, M.-S. A New (t, n)-multisecret-sharing scheme. *Appl. Math. Comput.* **2004**, *151*, 483–490.
8. Al Ebri, N.; Yeun, C.Y. Study on Secret Sharing Schemes (SSS) and Their Applications. In Proceedings of the 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, UAE, 11–14 December 2011; pp. 40–45.
9. Bozkurt, I.N.; Kaya, K.; Selçuk, A.A.; Güloğlu, A.M. Threshold Cryptography Based on Blakley Secret Sharing. In Proceedings of the of Information Security and Cryptology 2008, Ankara, Turkey, 25-27 December 2008.
10. Çalkavur, S.; Solé P. Multisecret-sharing schemes and bounded distance decoding of linear codes. *Int. J. Comput. Math.* **2017**, *94*, 107–114. [CrossRef]
11. He, J.; Dawson, E. Multistage secret sharing based on one-way function. *Electron. Lett.* **1994**, *30*, 1591–1592. [CrossRef]
12. Karnin, E.D.; Greene, J.W.; Hellman, M.E. On secret sharing systems. *IEEE Trans. Inf. Theory* **1983**, *29*, 35–41. [CrossRef]
13. Li, H.-X.; Cheng, C.-T.; Pang, L.-J. A New (t, n)-Threshold Multisecret Sharing Scheme. In *International Conference on Computational and Information Science*; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3802, pp. 421–426.
14. Bai, L. A Reliable (k, n)-Image Secret Sharing Scheme. In Proceedings of the 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, IN, USA, 29 September–1 October 2006; pp. 1–6.
15. Ding, C.; Laihonen, T.; Renvall, A. Linear multisecret-sharing schemes and error correcting codes. *J. Comput. Sci.* **1997**, *3*, 1023–1036.
16. Alahmadi, A.; Altassan, A.; AlKenani, A.; Çalkavur, S.; Shoaib, H.; Solé P. A Multisecret-Sharing Scheme Based on LCD Codes. *Mathematics* **2020**, *8*, 272. [CrossRef]
17. Croman, K.; Decker, C.; Eyal, I.; Gencer, A.E.; Juels, A.; Kosba, A.; Miller, A.; Saxena, P.; Shi, E.; Sirer, E.G.; et al. On scaling decentralized blockchains. In em International Conference on Financial Cryptography and Data Security; Springer: Berlin/Heidelberg, Germany, 2016; pp. 106–125.
18. Raman, R.K.; Varshney, L.R. Distributed Storage Meets Secret Sharing on the Blockchain. ITA 2018. Available online: http://ita.ucsd.edu/workshop/18/files/paper/paper_1714.pdf (accessed on 13 March 2019).
19. Krawczyk, H. Secret sharing made short. In *Cryptology — CRYPTO '93*; ser. Lecture Notes in Computer Science; Stinson, D.R., Ed.; Springer: Berlin, Germany, 1994; Volume 773, pp. 136–146.
20. Rabin, M.O. Efficient dispersal of information for security, load balancing, and fault tolerance. *J. ACM* **1989**, *36*, 335–348. [CrossRef]
21. Herzberg, A.; Jarecki, S.; Krawczyk, H.; Yung, M. Proactive secret sharing or: How to cope with perpetual leakage. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 1995.

22. Maram, S.K.D.; Zhang, F.; Wang, L.; Low, A.; Zhang, Y.; Juels, A.; Song, D. CHURP: Dynamic-Committee Proactive Secret Sharing. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 2369–2386.
23. Bartolucci, S.; Bernat, P.; Joseph, D. SHARVOT: Secret SHARe-based VOTing on the blockchain. Available online: https://arxiv.org/pdf/1803.04861.pdf (accessed on 13 March 2019).
24. He, S.; Wu, Q.; Lu, X.; Liang, Z.; Li, D.; Feng, H.; Zheng, H.; Li, Y. A Social-Network-Based Cryptocurrency Wallet-Management Scheme. *IEEE Access* **2018**, *6*, 7654–7663. [CrossRef]
25. Taylor, D.E. *The Geometry of the Classical Groups*; Sigma Series in Pure Mathematics; Heldermann Verlag: Berlin, Germany, 1992; Volume 9.
26. Jackson, W.A.; Martin, K.M. A Combinatorial Interpretation of Ramp Schemes. *Aust. J. Comb.* **1996**, *14*, 51–60.
27. Padro, C. Robust vector space secret sharing schemes. *Inf. Process. Lett.* **1998**, *68*, 107–111. [CrossRef]
28. Massey, J.L. Minimal codewords and secret sharing. In Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory, Mölle, Sweden, 22–27 August 1993; pp. 276–279.
29. Çalkavur, S.; Solé P. Vector space multisecret-sharing scheme based on Blakley's method. *Chin. J. Electron.* **2020**, submitted.