EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 11, No. 2, 2018, 410-416
ISSN 1307-5543 – www.ejpam.com
Published by New York Business Global

Secret sharing schemes based on extension fields

Selda Çalkavur

Department of Mathematics, Kocaeli University, Kocaeli, Turkey

Abstract. A $(t, n)-$secret sharing scheme is a method of distribution of information among n participants such that $t > 1$ can reconstruct the secret but $t - 1$ cannot. There is numerous research about secret sharing schemes. However there is little research on secret sharing schemes based on extension fields. In this paper, we study secret sharing schemes based on extension fields over finite fields. We use two methods to recover the secret. We define the access structure and the accessibility degree for these secret sharing schemes. We also describe our theorems, definitions and a corollary.

2010 Mathematics Subject Classifications: 12F05, 94A62

Key Words and Phrases: Extension fields, secret sharing, secret sharing schemes

1. Introduction

Secret sharing has been a subject of study for over 30 years. A secret sharing scheme is a way of distributing a secret among a finite set of people such that only some distinguished subsets of these subsets can recover the secret. The collection of these special subsets is called the access structure of the scheme.

Secret sharing schemes were constructed by Shamir [11] and Blakley [1] in 1979. Shamir scheme was based on polynomial interpolation but was later shown by Mc Eliece and Sarwate to be an application of Massey scheme [8], a scheme based on codes, to Reed Solomon codes [9]. Massey [8] used linear codes for secret sharing and explored the relationship between the access structure and the minimal codewords of the dual code of the underlying code in 1993.

Several authors has been studied on secret sharing schemes [3], [4], [7], [8].

Secret sharing schemes were applied to various fields such as cloud computing, controlling, nuclear weapons in military, recovering information from multiple servers, and controlling access in banking system [5].

Another secret sharing system is the (t, n)-threshold system [10]. A (t, n)-threshold scheme is a method of distribution of information among n participants such that $t > 1$ participants can reconstruct the secret but $t - 1$ cannot.

Email address: selda.calkavur@kocaeli.edu.tr (S. Çalkavur)

In this work, we present a (t, n)-threshold scheme based on extension fields over finite fields.

The material is organized as follows. Section II contains some algebraic background. Section III describes the schemes and analyses their security. We also determine the access structure of these secret sharing schemes and prove its properties. Section IV collects concluding remarks.

2. Algebraic preliminaries

2.1. Roots of irreducible polynomials

In this section, we remind some information about the set of roots of an irreducible polynomial over a finite field.

Lemma 1. *Let $f \in F_q[x]$ be an irreducible polynomial over a finite field F_q and α be a root of f in extension field of F_q. Then for a polynomial $h \in F_q[x]$ we have $h(\alpha)=0$ if and only if f divides h [6].*

Lemma 2. *Let $f \in F_q[x]$ be an irreducible polynomial over F_q of degree m. Then $f(x)$ divides $x^{q^n} - x$ if and only if f divides h [6].*

Theorem 1. *If f is an irreducible polynomial in $F_q[x]$ of degree m, then f has a root α in F_{q^m}. Furthermore, all the roots of f are simple and are given by the m distinct elements $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ of F_{q^m} [6].*

Corollary 1. *Let f be an irreducible polynomial in $F_q[x]$ of degree m. Then the splitting field of f over F_q is given by F_{q^m} [6].*

Definition 1. Let F_{q^m} be an extension of F_q and let $\alpha \in F_{q^m}$. Then the elements $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ are called the conjugates of α with respect to F_q [6].

The conjugates of $\alpha \in F_{q^m}$ with respect to F_q are distinct if and only if minimal polynomial of α over F_q has degree m. Otherwise, the degree d of this polynomial is a proper divisor of m and then the conjugates of α with respect to F_q are the distinct elements $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{d-1}}$ each repeated m/d times.

Theorem 2. *The conjugates of $\alpha \in F_{q^*}$ with respect to any subfield of F_q have the same order in the group F_{q^*}, where F_{q^*} is a cyclic group of nonzero elements of which consists of nonzero elements of F_q [6].*

Corollary 2. *If α is a primitive element of F_q, then so are all its conjugates with respect to any subfield of F_q [6].*

2.2. Traces and norms

In this part, we consider the viewpoint of regarding a finite extension $F = F_{q^m}$ of the finite field $K = F_q$ as a vector space over K.

Definition 2. For $\alpha \in F = F_{q^m}$ and $K = F_q$, the trace $T_{r_{F/K}}(\alpha)$ of α over K is defined by

$$T_{r_{F/K}}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + ... + \alpha^{q^{m-1}}.$$

If K is the prime subfield of F, then $T_{r_{F/K}}(\alpha)$ is called the absolute trace of α and simply denoted by $T_{r_F}(\alpha)$ [6].

Definition of the trace may be obtained as follows.

Let $f \in K[x]$ be the minimal polynomial of α over K and its degree d is a divisor of m. Then $g(x) = f(x)^{m/d} \in K[x]$ is called the characteristic polynomial of α over K. By Theorem 1, the roots of f in F are given by $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{d-1}}$ and by Definition 1, the roots of g in F are precisely the conjugates of α with respect to K. Hence

$$\begin{aligned} g(x) &= x^m + a_{m-1}x^{m-1} + ... + a_0 \\ &= (x-\alpha).(x-\alpha^q)...(x-\alpha^{q^{m-1}}) \end{aligned} \tag{1}$$

and a comparison of coefficients shows that

$$T_{r_{F/K}}(\alpha) = -a_{m-1}. \tag{2}$$

$T_{r_{F/K}}(\alpha)$ is always an element of K [6].

Definition 3. For $\alpha \in F = F_{q^m}$ and $K = F_q$, the norm $N_{F/K}(\alpha)$ of α over K is defined by

$$N_{F/K}(\alpha) = \alpha.\alpha^q.\alpha^{q^2}.....\alpha^{q^{m-1}} = \alpha^{q^m-1}/(q-1).$$

Moreover, by comparing the constant terms in (1), it can be written the following equation:

$$N_{F/K}(\alpha) = (-1)^m.a_0.$$

$N_{F/K}(\alpha)$ is also an element of K [6].

The number of distinct bases of F over K is too large, but there are two special types of bases . The first base is a polynomial basis $\{1, \alpha, \alpha^2, ..., \alpha^{m-1}\}$, made up of the powers of a defining element α of F over K, where α is taken to be a primitive element of F. Another type of basis is a normal basis.

Definition 4. Let $K = F_q$ and $F = F_{q^m}$. Then a basis of F over K of the form $\{\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}\}$, consisting of a suitable element $\alpha \in F$ and its conjugates with respect to K, is called a normal basis of F over K [6].

2.3. Secret sharing schemes

In this section we should think about a case of some malicious behaviors lying among participants which are called cheaters. They modify their shares in order to cheat.

If a group of participants can recover the secret by combining their shares, then any group of participants containing this group can also recover the secret.

Definition 5. An access group is a subset of a set of participants that can recover the secret from its shares. A collection Γ of access groups of participants is called an access

structure of the scheme. An element $A \in \Gamma$ is called a minimal access element. Hence a set is a minimal access group if it can recover the secret but no proper subset can recover the secret. Let $\bar{\Gamma}$ be the set of all minimal access elements.

We call $\bar{\Gamma}$ the minimal access structure [5].

Determining the minimal access structure is a hard problem [3].

Now let us consider the accessibility of an access structure of secret sharing scheme based on binary linear code. Let $P = \{P_1, P_2, ..., P_m\}$ be a set of m participants and let A_p be the set of all access elements on P.

Definition 6. The accessibility index on P is the map $\delta_p(\Gamma)$: $A_p \to \mathbb{R}$ given by

$$\delta_p(\Gamma) = \frac{|\Gamma|}{2^m}$$

for $\Gamma \in A_p$, where $m = |P|$. The number $\delta_p(\Gamma)$ will be called the accessibility degree of structure Γ [2].

3. The Schemes

In this section, we present the new $(t, n)-$ threshold schemes that combine of Shamir scheme with our schemes.

3.1. First scheme

Let F_q be the secret space and F_{q^m} be the sharing space. We consider a finite extension of F_{q^m} of the finite field F_q as a vector space over F_q, where m is the dimensional of F_{q^m} over F_q. Assume a characteristic polynomial $g(x)$ of α, where $\alpha \in F_{q^m}$ and the degree of $g(x)$ is m such that

$$g(x) = x^m + a_{m-1}x^{m-1} + ... + a_0.$$

- Let all of elements of F_{q^m}, except 0, be the participants.
- The dealer pics the element $-a_{m-1} \in F_q$ as the secret and distributes to m elements of F_{q^m} which are $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$.

We know that these elements are also the normal basis elements of F_{q^m} and uniquely determined and each element of F_{q^m} can be written as the linear combination of basis elements. These m participants recover the secret while pooling their shares. In the first scheme, we need the trace function of α to recover the secret.

$$T_{r_{F/K}}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + ... + \alpha^{q^{m-1}}.$$

We also know that $T_{r_{F/K}}(\alpha)$ is also equal to $-a_{m-1}$, where $-a_{m-1}$ is the coefficient of x^{m-1} for the characteristic polynomial $g(x)$. So $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ elements can reach the secret together.

3.2. Second scheme

Now we construct another scheme using the norm function. In this scheme the dealer pics the element $(-1)^m.a_0 \in F_q$ as the secret and distributes to the m elements of F_{q^m} which are $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$. These m participants recover the secret while combining their shares as follows.

$$N_{F/K}(\alpha) = \alpha.\alpha^q.\alpha^{q^2}.....\alpha^{q^{m-1}}.$$

We know that $N_{F/K}(\alpha)$ is also equal to $(-1)^m a_0$. So $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$ elements can reach the secret together.

If $m-h$ say, with $1 \leq h < m$, participants group together they can guess the secret with probability $\frac{1}{h+1} \leq \frac{1}{2}$.

Another possible attack would be to isolate elements of F_{q^m} which are reached the secret. In our secret sharing schemes, only the conjugates of α with respect to F_q can recover the secret. These elements are also the normal basis elements which are uniquely determined.

Theorem 3. *In these secret sharing schemes based on extension fields we have the following.*
i) The access structure consists of the m elements.
ii) No element of number less than m can be used in recovering the secret.

Proof. i) The secret is recovered thanks to the normal basis elements and their number is m.
ii) These m elements are uniquely determined. So there is no element which has this property. The proof is clear.

Corollary 3. *With the above condition the extension field F_{q^m} determines $(m, q^m - 1)-$threshold scheme.*

Proof. It is clear that the number of non-zero elements of F_{q^m} is $q^m - 1$ and the number of normal basis elements is m. These m elements out of $q^m - 1$ can reach the secret together.

Definition 7. *The access structure of these secret sharing schemes is given by*

$$\Gamma = \{(\alpha^k, \beta) | k = 1, q, q^2, ..., q^{m-1}, \beta \in F_{q^m}\}.$$

Theorem 4. *The number of parties in these secret sharing schemes is $q^m - 1$ and the access structure has the following properties:*
i) Only m elements can be used to recover the secret but $(m-1)$ cannot.
ii) When the parties come together, up to $[\frac{m}{2}]$ cheaters can be found in each group. ("$[x]$" denotes the greatest integer less than or equal to x.)

Proof. i) It is seen that by Definition 7.
ii) By definition of our scheme is $2 \leq m$ iff $1 \leq \frac{m}{2}$.

The accessibility degree of the access structure for these secret sharing schemes based on extension fields over finite fields can be defined as follows.

Definition 8. *The accessibility index on P is the map $\delta_p(\Gamma)$:$A_p \to \mathbb{R}$ given by*

$$\delta_p(\Gamma) = \frac{|\Gamma|}{q^m - 1},$$

for $\Gamma \in A_p$, where $m = |P|$ is the number of participants in the access structure. The number $\delta_p(\Gamma)$ will be called the accessibility degree of structure Γ.

Example 1. *Let F_{2^3} be the secret sharing space. This space is also $m-$dimensional vector space over F_2. Consider the polynomial $f(x) = x^3+x^2+1 \in F_2[x]$. The coefficients of polynomial are $a_0 = 1, a_1 = 1, a_2 = 1$. So the secret is $-a_2 = -1 = 1$ and $m = 3, q = 2$. The normal basis elements of F_{q^m} are $\alpha, \alpha^2, \alpha^{2^{3-1}} = \alpha^4$. It is clear that*

$\alpha^0 = 1$,
$\alpha^1 = \alpha$,
$\alpha^2 = \alpha^2$,
$\alpha^3 = \alpha^2 + 1$,
$\alpha^4 = \alpha^3 + \alpha = \alpha^2 + \alpha + 1$,
$\alpha^5 = \alpha^3 + \alpha^2 + \alpha = \alpha + 1$,
$\alpha^6 = \alpha^2 + \alpha$,
$\alpha^7 = \alpha^3 + \alpha^2 = 1$.

All the sharings are

$K_1 = (\alpha^0, 1)$,
$K_2 = (\alpha^1, \alpha)$,
$K_3 = (\alpha^2, \alpha^2)$,
$K_4 = (\alpha^3, \alpha^2 + 1)$,
$K_5 = (\alpha^4, \alpha^2 + \alpha + 1)$,
$K_6 = (\alpha^6, \alpha^2 + \alpha)$,
$K_7 = (\alpha^7, 1)$.

K_2, K_3 and K_5 participants recover the secret while combining their shares by using the trace function of α as follows.

$$T_{r_{F/K}}(\alpha) = \alpha + \alpha^2 + \alpha^4 = \alpha + \alpha^2 + (\alpha^2 + \alpha + 1) = 1.$$

Now we assume that the secret is $(-1)^3.a_0 = (-1).1 = -1 = 1$ and the same participants recover the secret calculating the norm of α as follows.

$$N_{F/K}(\alpha) = \alpha.\alpha^2.\alpha^2 = \alpha^3.\alpha^4 = (\alpha^2 + 1).(\alpha^2 + \alpha + 1) = 1.$$

As it is seen that both of these schemes are the $(3, 7)-$threshold schemes. The accessibility degree of the access structure is $\frac{3}{2^3-1} = \frac{3}{7} = 0,42$.

4. Conclusion

In the present article we constructed some $(t, n)-$threshold schemes using the trace and norm functions. These schemes are mainly based on finite extensions over finite fields.

We introduced the access structure of these schemes. We defined the accessibility degree of the access structure. We obtained the new results. Possible attacks have been considered.

Our scheme has the same distributed as Shamir's scheme does. We send an element of F_q and the normal basis elements of F_{q^m} use the trace and norm functions to recover the secret.

The secret can be recovered only by the special participants which are uniquely determined. This means the access structure of these schemes is very strong and reliable.

References

[1] *Blakley, G.R., "Safeguarding cryptographic keys", American Federation of Information Processing Societies, National Computer Conference, pp. 313-317, (1979).*

[2] *Carreras, F., Magana, A., Munuera, C., The accessibility of an access structure, RAIRO-Theoretical Informatics and Applications, 40.04, pp. 559-567. (2006).*

[3] *Ding, C., Kohel, D. R., Ling, S., Secret-sharing with a class of ternary codes, Theoretical Computer Science, 246(1), pp.285-298, (2000).*

[4] *Dougherty, S. T., Mesnager, S., Solé, P., Secret sharing schemes based on self-dual codes, Information Theory Workshop (2008), ITW'08, IEEE (2008).*

[5] *Kim. J.L., Lee, N., Secret sharing schemes based on additive codes over $GF(4)$, Applicable Algebra in Engineering, Communication and Computing, pp. 1-19, (2016).*

[6] *R. Lidl, H. Niederreiter, Finite Fields, vol. 20, Cambridge.*

[7] *Li, Zhihui, Xue, Ting Xue, Lai, Hong, Secret sharing schemes from binary linear codes, Information Sciences 180(22), pp. 4412-4419, (2010).*

[8] *Massey, J. L., Minimal codewords and secret sharing,"in Proc. 6th Joint Swedish-Russian Workshop on Information Theory, Mölle, Sweden, pp. 276-279, (1993).*

[9] *McEliece R, J. and Sarwate D. V., On sharing secrets and Reed-Solomon codes, Common. Assoc. Comp. Mach., vol. 24, pp. 583-584, (1981).*

[10] *Piepryzk, J. and Zhang, X. M., Ideal threshold schemes from MDS codes, Proceedings of Information Security and Cryptology ICISC 2002, Lecture Notes in Computer Science, vol. 2587, Springer-Verlag, Berlin, pp. 269-279, (2003).*

[11] *Shamir, A., How to share a secret, Comm. of the ACM 22 pp. 612-613, (1979).*