EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 11, No. 2, 2018, 468-475
ISSN 1307-5543 – www.ejpam.com
Published by New York Business Global

A New Approach to Construct Secret Sharing Schemes Based on Field Extensions

Fatih Molla[1], Selda Çalkavur[2,*]

[1] *Engineering of Information Systems, Faculty of Technology, Kocaeli University, Kocaeli, Turkey*
[2] *Mathematics, Faculty of Arts and Sciences, Kocaeli University, Kocaeli, Turkey*

Abstract. Secret sharing has been a subject of study since 1979. It is important that a secret key, passwords, information of the map of a secret place or an important formula must be kept secret. The main problem is to divide the secret into pieces instead of storing the whole for a secret sharing. 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.
In this paper, we propose a new approach to construct secret sharing schemes based on field extensions.

2010 Mathematics Subject Classifications: 12F05, 94A62.

Key Words and Phrases: Field extension, secret sharing, secret sharing scheme.

1. Introduction

A secret sharing scheme is a method of hiding a secret among several shadows such that the secret can be retrieved only by some subsets of these shadows. Secret sharing is useful in many cryptographic applications [2], [17], [18], [5].

There are numerous studies about secret sharing schemes. Several authors have considered the construction of secret sharing schemes using linear error correcting codes. [4], [8], [10], [11], [13], [15].

Shamir [17] and Blakley [2] were introduced secret sharing schemes. Massey [10] used linear codes for secret sharing and explained the relationship between the access structure and the minimal codewords of the dual code of the underlying code [15], [6].

Another secret sharing scheme is the multisecret-sharing scheme. This scheme was proposed in [5], [7], [9], [16], [19], [3]. In the multisecret-sharing schemes [9], [16], [1] there is a set of p secrets can be shared at once and each participant needs to keep one share

*Corresponding author.

Email addresses: selda.calkavur@kocaeli.edu.tr (S. Çalkavur)
fatih.molla@hotmail.com (F. Molla)

is called secret share. In these schemes all p secrets cannot reconstruct. To recover the secret the participants need to keep one share is called secret share. In these schemes all p secrets cannot reconstruct. To recover the secret the participants need to submit a pseudo-share computed from their secret share instead of the secret share itself.

In this work, we present a new approach to construct secret sharing schemes. We use the system of Shamir's scheme. So our scheme is a (k, n)-threshold scheme.

The rest of this paper organized as follows. The next section gives the basic preliminaries used in paper. Section III presents secret sharing scheme based on field extensions. Section IV collects concluding remarks.

2. Background and Preliminaries

In this section we give the basic preliminaries. In this context we remind Shamir's secret sharing scheme.

2.1. Shamir's Secret Sharing Scheme

In a secret sharing scheme, a secret s is divided into n shares and distributed to n shareholders by a trusted dealer. The shared secret s can only be recovered when k $(k < n)$ or more than k shares are available. Such a scheme is called a (k, n)-secret sharing.

In 1979, Shamir introduced a secret sharing scheme. Shamir's secret sharing scheme is an effective way to distribute secret to a group of shareholders. Shamir's scheme is a (k, n) threshold secret sharing scheme and this scheme was based on polynomial interpolation.

In the Shamir's secret sharing [17], there are n shareholders $P = \{P_0, P_1, \ldots, P_{n-1}\}$ and a trusted dealer D. We use the shareholders' IDs $(z_0, z_1, \ldots, z_{n-1})$ to denote each participant. Secret is generated and distributed to shareholders by the dealer D secret can be reconstructed based on Lagrange interpolation polynomial by taking any k shares $(\alpha_{i_0}, \ldots, \alpha_{i_{n-1}})$ of participants and their IDs, $(z_{i_0}, \ldots, z_{i_{n-1}})$ where $\{i_0, \ldots, i_{k-1}\} \subseteq \{0, 1, \ldots, n-1\}$ [17], [18], [5].

Shamir's secret sharing scheme provides a method of hiding this secret such that any k or more participants would be able to reconstruct the original secret but any less than k participants would not be able to reconstruct the original secret. Assume all the computations are in $GF(p^m)$ $(n < p^m)$ (p is prime), in which m is the number of bits of the secret. Shamir's secret sharing scheme consists of two algorithms [17], [5]:

2.1.1. Share generation algorithm

Construct a polynomial $\alpha(z) = s_0 + s_1 z + s_2 z^2 + \ldots + s_{k-1} z^{k-1}$, where $s_i (i \in \{0, 1, \ldots, k-1\})$ and z belongs to $GF(p^m)$. $s_i (i \in \{0, 1, \ldots, k-1\})$ is randomly generated in $GF(p^m)$ and s_{k-1} is the secret. Each shareholder with ID z_i receives a share $a(z_i)$ and we assume the IDs z_i are publicly known and unique for each different shareholder. We denote $\alpha(z_i)$ as α_i and z_{i_j} for simplicity in this part.

2.1.2. Secret reconstruction algorithm

For a polynomial of degree $k-1$, with knowledge of at least k data points, we can reconstruct the exact polynomial using Lagrange interpolation in $GF(p^m)$ and thus reconstruct the secret s_{k-1}.

Now we remind some definitions and a proposition associated with subject.

Definition 1. *(Minimal access set) A subset of participants is called a minimal access set, if the participants in the subsets can recover the secret by combining their shares but any subset at the participants can not do so [14].*

Definition 2. *(Access structure) The access structure of a secret sharing scheme is the set of all minimal access sets [14].*

3. A Secret Sharing Scheme Based on Field Extensions

In this part we obtain a secret sharing scheme using the some results of [12]. Now we construct the Shamir's secret sharing scheme by using a field extension. Consider the input and output values of secret sharing scheme as the integers. However, we work on polynomials to do algebraic operations.

Let 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.

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

We transform the selected integers to the polynomials of $(GF(q))[x]$ by Algorithm 1.

Algorithm 1.
input: $a \in M_q$
output: $b \in GF(q)$
Step 1. a is transformed into vectors of length m with respect to base p.
Step 2. these vectors are written as a polynomial.

Example 1. *Consider* $5 \in M_8 \Rightarrow 5 = (101)_2 = \theta^2 + 1 \in GF(8)$, *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* $GF(9)$.

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

Algorithm 2.
input: $b \in GF(q)$
output: $a \in M_q$
Step 1. b 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. *Consider* $\theta^2+1 \in GF(8) \Rightarrow \theta^2+1 = (101)_2 = 5 \in M_8$, *where* θ *is a primitive element of* $GF(8)$.

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

3.1. Proposed Scheme

We consider a polynomial of degree $k-1$ as follows.

$$p(x) = \sum_{i=0}^{k-1} a_i x^i \in M_q[x], \tag{2}$$

where the coefficients a_i $(1 \leq i \leq k-1)$ are randomly selected. Let the secret be a_0 which is a constant term of a polynomial.

This polynomial is written as a polynomial of $(GF(q))[x]$.

$$t(x) = \sum_{i=0}^{k-1} b_i x^i \in (GF(q))[x]. \tag{3}$$

3.2. Secret Distribution

Let the IDs of participants be $u_1, u_2, \cdots, u_n \in M_q - \{0\}$. It is obtained the polynomials of $v_1, v_2, \cdots, v_n \in (GF(q))$ by applying Algorithm 1. It is calculated the images of a secret pieces in GF(q) as follows.

$$r_i = t(v_i) \in GF(q), \tag{4}$$

where r_i is an image of participant v_i $(0 \leq i \leq k-1)$.

By using Algorithm 2, the obtained polynomials are transformed to the integers of $y_1, y_2, \cdots, y_n \in M_q$ and distributed to the participants.

3.3. Secret Retrieval Procedure

Now we explain how the secret is recovered. Consider a set of $W = \{d_1, d_2, \cdots, d_k\}$ $(d_1, d_2, \cdots, d_k \in M_q)$. The elements of W are recovered the secret by combining their shares.

In the ordered pair (d_i, y_i) $(1 \leq i \leq k)$, d_i is denoted by the identity of participant and y_i is denoted by the secret piece of participant d_i.

These ordered pairs are transformed to the polynomial pairs (v_i, r_i) $(v_i, r_i \in GF(q))$ by using Algorithm 1.

Then the polynomial $t(x)$ is recovered by Lagrange Interpolation and the polynomial $p(x)$ is obtained by Algorithm 2. So the secret is recovered by using the following equality.

$$s = p(0) \tag{5}$$

Note that it is used the Extended Euclid Algorithm to find the multiplicative inverse of a polynomial with respect to (mod $f(x)$), where $f(x)$ is the irreducible polynomial of $(GF(p))[x]$.

Example 5. *Assume that $GF(2^3)$ 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 $GF(2^3)$ with these parameters.*

Consider an irreducible polynomial of $f(x) = x^3 + x + 1 \in (GF(2))[x]$. Let θ be a root of $f(x)$. So the elements of $GF(2^3)$ are the following.

$$GF(8) = \{0, 1, \theta, \theta + 1, \theta^2, \theta^2 + 1, \theta^2 + \theta, \theta^2 + \theta + 1\}.$$

$$\begin{aligned}
\theta^1 &= \theta \\
\theta^2 &= \theta^2 \\
\theta^3 &= \theta^2 + 1 \\
\theta^4 &= \theta^2 + \theta + 1 \\
\theta^5 &= \theta + 1 \\
\theta^6 &= \theta^2 + \theta \\
\theta^7 &= 1
\end{aligned}$$

The relationship between M_q and $GF(q)$ is as follows.

$$\begin{aligned}
0 &\longleftrightarrow 0 \\
1 &\longleftrightarrow 1 \\
2 &\longleftrightarrow \theta \\
3 &\longleftrightarrow \theta + 1 \\
4 &\longleftrightarrow \theta^2 \\
5 &\longleftrightarrow \theta^2 + 1 \\
6 &\longleftrightarrow \theta^2 + \theta \\
7 &\longleftrightarrow \theta^2 + \theta + 1
\end{aligned}$$

We choose a polynomial in $M_8[x]$ to construct the secret pieces.

$$p(x) = x^2 + 5x + 4 \in M_8[x].$$

We write the elements of $GF(8)$ corresponding to the coefficients of $p(x)$.

$$t(x) = x^2 + (\theta^2 + 1)x + \theta^2 \in (GF(8))[x].$$

Let the IDs of participants be $u_1 = 1, \quad u_2 = 2, \quad u_3 = 3, \quad u_4 = 4, \quad u_5 = 5$.
These elements correspond to $v_1 = 1,\ v_2 = \theta,\ v_3 = \theta + 1,\ v_4 = \theta^2,\ v_5 = \theta^2 + 1$ in $(GF(8))[x]$.
We obtain the secret pieces as follows.

$$\begin{array}{llll} r_1 & = t(v_1) & = t(1) & = 0 & \Rightarrow y_1 = \boldsymbol{0} \\ r_2 & = t(v_2) & = t(\theta) & = \theta^2+\theta+1 & \Rightarrow y_2 = \boldsymbol{7} \\ r_3 & = t(v_3) & = t(\theta+1) & = \theta+1 & \Rightarrow y_3 = \boldsymbol{3} \\ r_4 & = t(v_4) & = t(\theta^2) & = 0 & \Rightarrow y_4 = \boldsymbol{0} \\ r_5 & = t(v_5) & = t(\theta^2+1) & = \theta^2 & \Rightarrow y_5 = \boldsymbol{4} \end{array}$$

The secret will be recovered when 3 *participants by combining their shares. We try to find the secret with participants* 2, 4 *and* 5.

$$t(x) = \sum_{j \in W} y_j l_j(x),$$

$$l_j(x) = \prod_{m \in W-\{j\}} \frac{x - x_m}{x_j - x_m},$$

where $W = \{2, 4, 5\}$.

Then we obtain the following equation. So we recover the secret in this way.

$$t(x) = x^2 + (\theta^2+1)x + (\theta^2) \in (GF(8))[x].$$

$$p(x) = x^2 + 5x + 4 \in M_q[x].$$

$$s = p(0) = 4.$$

4. Analysis and Discussion

4.1. Security Analysis

We discuss the security of the proposed (k, n)-secret sharing scheme is as follows. Introducing more general polynomial

$$p(x) = \sum_{i=0}^{k-1} a_i x^i \in M_q[x]$$

as the polynomial secret in Shamir's scheme we obtain, a scheme that is not simple to break the secret. To compute the secret we have to do computation in a field extension. We use a new approach in the elements of the field extension. That is by finding a primitive element of the field and then express each its elements as a power of a primitive element. The secret can be reached every element of field extension F_q $(q = p^m)$ can be uniquely expressed as a polynomial in θ over F_p of degree less then m. So, the access structure of this scheme is very strong and reliable.

4.2. Performance Analysis

The access structure of this scheme consists of the k elements since the degree of a polynomial $p(x)$ is $k-1$. The possible attack can be explained as follows.

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

5. Conclusion

In this present article we obtain a (k, n)-threshold scheme using the elements of field extension. Our scheme has the same distributed as Shamir's scheme does. We choose the secret as an element of M_q and then some participants use the Lagrange Interpolation to recover the secret.

Moreover, we introduce the access structure of this scheme and consider the possible attack.

The secret can be recovered only by the some elements of field extension which are uniquely determined. This means the access structure of this scheme is very strong and reliable.

References

[1] L Bai, "A reliable (k,n)-image secret sharing scheme", Proc. of the 2nd International Symposium on Dependable, Autonomic and Secure Computing DASC'06, pp.1-6, 1993.

[2] G R Blakley, "Safeguarding cryptographic keys", in Proceedings of the 1979 AFIPS National Computer Conference, vol. 48, pp. 313-317, Jun. 1979.

[3] S Çalkavur, and P Solé, "Multisecret sharing schemes and bounded distance decoding of linear codes", International Journal of Computer Mathematics, vol. 94, issue. 1, pp. 107-114, 2017.

[4] C Ding, D Kohel, and S Ling, "Secret sharing with a class of ternary codes", Theor. Comp. Sci., vol. 246, pp. 285-298, 2000.

[5] L Harn, and C Lin, "Detection and identification of cheaters in (t,n) secret sharing schem", Des. Codes Cryptography, vol. 52, no. 1, pp. 15-24, Jul. 2009.

[6] L Harn, Comment on "Multistage secret sharing based on one-way function", Electronics Letters, vol. 31(3), pp.262, 1995.

[7] J He, and E Dawson, "Multistage secret sharing based on one-way function", Electronic Letters, vol. 30 (19), pp.1591-1592, 1994.

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

[9] H -X Li, C -T Cheng, and L -J Pong, "A new (t,n) multi-secret sharing scheme", CIS 2005, vol. 3802, pp. 421-426, 2005.

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

[11] J L Massey, "Some applications of coding theory", Cryptography, Codes and Ciphers: Cryptography and Coding IV, pp. 33-47, 1995.

[12] F Molla, "A study on the secret image sharing schemes", Master Thesis, Kocaeli University, Kocaeli, 2018.

[13] K Okada, and K Kurosawa, "MDS secret-sharing scheme secure against cheaters", IEEE Trans. Inf. Theory, vol. 46, no. 3, pp. 1078-1081, May 2000.

[14] H Özadam, F Özbudak, and Z Saygı, "Secret sharing schemes and linear codes.", Information Security Cryptology Conference with International Participation, Proceedings, pp. 101-106, 2007.

[15] J Pieprzyk, and X M Zhang, "Ideal threshold schemes from MDS codes" in Information Security and Cryptology Proc. of ICISC 2002 (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, vol. 2587, pp. 269-279, 2003.

[16] L -J Pong, and Y -M Wang, "A new (t,n) multi-secret sharing scheme based on Shamir's secret sharing", Applied Math, vol. 167, pp. 840-848, 2005.

[17] A Shamir, "How to share a secret", Commun. ACM, vol. 22, no. 11, pp.612-613, Nov. 1979.

[18] A Tompa, and H Woll, "How to share a secret with cheaters", in Proceedings on Advances in cryptology - CRYPTO '86. London, UK, UK: Springer-Verlag, pp. 261-265, 1987.

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

[20] J Yuan, and C Ding, "Secret sharing schemes from three classes of linear codes", IEEE Trans. on Inf. Theory 52(1): 206-212, Jan. 2006.