Computer Technology and Application 7 (2016) 269-272
doi: 10.17265/1934-7332/2016.06.001

DAVID PUBLISHING

Some Secret Sharing Schemes Based on the Finite Fields

Selda Çalkavur

Department of Mathematics, Kocaeli University, Kocaeli 41135, 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. We explore some (*k*, *n*)—secret sharing schemes based on the finite fields.

Key words: Secret sharing, threshold secret sharing scheme, finite field.

1. Introduction

Secret sharing schemes were introduced by Shamir in 1979 [1]. 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.

The person who distributes the shares is called the dealer and a minimal $t-$subset of participants that can reconstruct the secret is called a coalition. Shamir scheme was based on polynomial interpolation but was later shown by McEliece and Sarwate to be an application of Massey scheme, a scheme based on codes [2], to Reed Solomon codes [3].

In this paper, we present a $(k, n)-$ threshold scheme based on the finite fields.

The material is organized as follows. Section 2 contains some algebraic background. Section 3 describes the scheme and analyses its security. Section 4 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 an 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 [4].

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 m divides n [4].

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 α, α^q,..., $\alpha^{q^{m-1}}$ of F_{q^m} [4].

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} [4].

Definition 1. Let F_{q^m} be an extension of F_q and let $\alpha \in F_{q^m}$. Then the elements α, α^q,..., $\alpha^{q^{m-1}}$ are called the conjugates of α with respect to F_q [4].

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 α, α^q,..., $\alpha^{q^{d-1}}$ each repeated m/d times.

Theorem 2. The conjugates of $\alpha \in F_q^*$ with

Corresponding author: Selda Çalkavur, Pd.D., assistant professor, research fields: coding theory, cryptography, algebra.

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 [4].

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 [4].

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 $T_{\Gamma_{F/K}}(\alpha)$ of α over K is defined by

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

If K is the prime subfield of F, then $T_{\Gamma_{F/K}}(\alpha)$ is called the absolute trace of α and simply denoted by $T_{\Gamma_F}(\alpha)$ [4].

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 α, $\alpha^q, \ldots, \alpha^{q^{d-1}}$ and by Definition 1, the roots of g in F are precisely the conjugates of α with respect to K. Hence

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

$$= (x-\alpha).(x-\alpha^q)\ldots(x-\alpha^{q^{m-1}}) \qquad (1)$$

and a comparison of coefficients shows that

$$T_{\Gamma_{F/K}}(\alpha) = -a_{m-1} \qquad (2)$$

$T_{\Gamma_{F/K}}$ is always an element of K [4].

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

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

Moreover, by comparing the constant terms in Eq. (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.

2.3 Secret Sharing Schemes

Definition 4 (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 cannot do so [5].

Definition 5 (Access structure). The access structure of a secret sharing scheme is the set of all minimal access sets [5].

3. The Scheme

In this section, we present a $(k, n)-$threshold scheme that combines of Shamir scheme with our scheme.

3.1 First Scheme

Let the F_q be the secret space and F_{q^m} which is extension field of F_q be sharing space. Assume a characteristic polynomial $g(x)$ of α, where $\alpha \in F_{q^m}$ and degree $g(x)$ is m such that $g(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$.

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

These m participants recover the secret while combining their shares. In the first scheme, we need the trace function of α:

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

We know that $T_{\Gamma_{F/K}}(\alpha)$ is also equal to $-a_{m-1}$. So α, $\alpha^q, \ldots, \alpha^{q^{m-1}}$ elements can reach the secret together.

3.2 Second Scheme

Now we construct another scheme using the norm function.

In this scheme the dealer chooses the element $(-1)^m.a_0 \in F_q$ as the secret and distributes the m elements of F_{q^m} which are α, α^q,…, $\alpha^{q^{m-1}}$. 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 α, α^q,…, $\alpha^{q^{m-1}}$ elements can reach the secret together. If $m-h$ say, with $1<h<m$, participants group together they can guess the secret with probability $\frac{1}{h+1} < \frac{1}{2}$.

Another possible attack would be to isolate elements of F_{q^m} which are reached the secret. In our secret sharing scheme, only the conjugates of α with respect to F_q can recover the secret. These elements are determined uniquely. So, there are no elements which can recover the secret, except the conjugate elements.

Proposition 1. With the above condition the finite extension field F_{q^m} determines a $(m, q^m)-$threshold scheme.

Proof. It is clear that the number of elements of F_{q^m} is q^m and the conjugates of α with respect to F_q are m. These m elements out of q^m can reach the secret together.

Corollary 1. There are m elements in the minimal access set in the $(m, q^m)-$threshold schemes.

Proof. In these threshold schemes m elements can recover the secret by combining their shares. This means the number of minimal access set is m.

Example 1. Let F_{2^3} be the secret sharing space. 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 conjugates of α are $\alpha, \alpha^2, \alpha^{2^{3-1}} = \alpha^4$.

It is clear that $\alpha^3 = \alpha^2 + 1$ and $\alpha^4 = \alpha^3 + \alpha = \alpha^2 + \alpha + 1$.

We recover the secret calculating the trace of α as follows.

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

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

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

As it is seen both of these schemes are a (3, 8)—threshold scheme.

3.3 Why Use Extension Fields?

What is the advantage of using extension field in these schemes? An irreducible polynomial in F_{q^m} has at least a root and the conjugates of this root can be found by its. In both of these schemes, the secret can be reached by the conjugates elements and we know that these elements are determined uniquely. So, the elements of F_{q^m} cannot reach the secret, except the conjugates elements. This means the access structure of these schemes is very strong and reliable.

4. Conclusion

In the present article we obtain some (*k*, *n*)—threshold schemes using the trace and norm functions. These schemes are based on the finite extension fields. Possible attacks have been considered.

Our scheme has the same distributed as Shamir's scheme does. We send an element of F_q and then participants use properties of trace and norm functions to recover the secret.

The secret can be recovered only by the special participants which are the conjugates of a root of characteristic polynomial. So the access structure of this scheme is very strong and reliable.

References

[1] Shamir, A. 1979. "How to Share a Secret." *Comm. of the ACM* 22: 612-3.

[2] Massey, J. L. 1993. "Minimal Codewords and Secret Sharing." In *Proc. of 6th Joint Swedish-Russian Workshop on Information Theory*, Mölle, Sweden.

[3] McEliece, R. J., and Sarwate, D. V. 1981. "On Sharing Secrets and Reed-Solomon Codes." *Common. Assoc. Comp. Mach.* 24: 583-4.

[4] Lidl, R., and Nieddereiter, H. 1997. *Finite Fields.* vol. 20. Cambridge: Cambridge University Press.

[5] Özadam, H., Özbudak, F., and Saygı, Z. 2007. "Secret Sharing Schemes and Linear Codes." In *Proceedings of Information Security Cryptology Conference with International Participation*, 101-6.