LINEAR MULTISECRET-SHARING SCHEMES

Selda Çalkavur

Math Dept, Kocaeli University, Kocaeli, Turkey
selda.calkavur@kocaeli.edu.tr

Abstract: Cyclic codes form an important class of linear codes. These codes have a rich algebraic structure. Secret sharing is a major topic of cryptography. In this paper, we present a multisecret-sharing scheme based on cyclic codes. This scheme is linear in the sense of that form of each secret. Its security improves on that of multisecret-sharing schemes.

Keywords: Secret sharing, linear multisecret sharing scheme, cyclic code.

Introduction

Secret sharing schemes were examined by Blakley (Blakley, 1979) and Shamir (Shamir, 1997) in 1979. Shamir's scheme is a (t, n)-threshold secret sharing scheme and this scheme was based on polynomial interpolation. 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.

In a secret sharing scheme there are some participants and a dealer. The dealer has a secret and distributes it the other participants. In a minimal t-subset of participants recover the secret while combining their shares. These subsets are called the minimal access sets.

Another secret sharing scheme is the multisecret-sharing scheme. This scheme was proposed in (Horn, 1995), (He, 1994), (Li, 2016), (Pang, 2005), (Yang, 2004), (Çalkavur et al, 2017). In the multisecret-sharing schemes (Li, 2016), (Pang, 2005), (Bai, 1993) there is a set of p secrets can be shared at once and each participant needs to keep one share is called secret share. In these schemes all p secrets are recovered at once or 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 propose a new multisecret-sharing scheme based on cyclic codes. We give a secret reconstruction algorithm based on generator polynomial of the code. We analyse the security and performance of the scheme by means of cyclic code theory. We calculate the number of minimal coalitions in this scheme. We introduce the access structure of this scheme and define its accessibility degree and explain its linearity.

We conclude by a comparison between our scheme and the three main other code-based schemes in the literature: Massey's scheme (Massey, 1993), Ding et al (Ding, 1997) and (Çalkavur et al, 2017) multisecret scheme.

The rest of this paper is organized as follows. The next section gives the basic preliminaries used in the paper. Section III presents the proposed scheme, analyses its security and defines the accessibility degree of the scheme. Section IV contains the said comparison and against cheating. Section V collects concluding remarks.

Background and Preliminaries

In this section we give the basic preliminaries and some necessary mathematical information used in this work.

A. Linear Codes

Let q be a prime power and denote the finite field of order q by F_q. An $[n, k]$-code C over F_q is a subspace in $(F_q)^n$, where n is length of the code C and k is dimension of C. The dual code of C is defined to be the set of those vectors $(F_q)^n$ which are orthogonal to every codeword of C. It is denoted by $C^\perp$. The code $C^\perp$ is an $[n, n-k]$-code. A generator matrix G for a linear code C is a $k \times n$ matrix for which the rows are a basis of C. A parity-check matrix for a linear code C is a generator matrix for its dual code $C^\perp$. It is denoted by H.

Let C be an $[n, k]$-code over F_q with generator matrix G. C contains q^k codewords and can be used to communicate any one of q^k distinct messages. We encode the message vector $x = x_1 x_2 \cdots x_k$ as the codeword xG.

If G is a generator matrix for C, then $C = \{ uG \mid u \in (F_q)^k \}$. The map $u \to uG$ maps the vector space q^k onto a

k-dimensional subspace of $\left(F_q\right)^n$.

B. Cyclic codes

A code C is cyclic if

1. C is a linear code,
2. any cyclic shift of a codeword is also a codeword, whenever $a_0a_1\cdots a_{n-1}$ in C, then so is $a_{n-1}a_0a_1\cdots a_{n-2}$ (Hill, 1986).

Theorem 1. Let C be a non-zero cyclic code. Then,

1. there exists a unique polynomial $g(x)$ of smallest degree in C,
2. $C = < g(x) >$,
3. $g(x)$ is a factor of $x^n - 1$ (Hill, 1986).

Definition 1. In a non-zero cyclic code C the monic polynomial of least degree, given by Theorem 1, is called the generator polynomial of C (Hill, 1986).

Lemma 1. Let $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ be the generator polynomial of a cyclic code. Then g_0 is non-zero (Hill, 1986).

Theorem 2. Suppose C is a cyclic code with generator polynomial $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ of degree $n-k$. Then $dim(C) = k$ and a generator matrix for C is

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}.$$

This means $aG = (a_0 + a_1x + \cdots + a_{k-1}x^{k-1})g(x)$, where $a = (a_0, a_1, \cdots, a_{k-1}) \in \left(F_q\right)^k$ (Hill, 1986).

C. 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 2. 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 (Kim, 2016). Determining the minimal access structure is a hard problem (Ding, 2000).

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

Definition 3. The accessibility index on P is the map $\delta_p(\Gamma): A_p \rightarrow \mathbb{R}$ 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 (Carreras, 2006).

Multisecret-Sharing Schemes and Cyclic Codes

A. Scheme Description

In this section, we examine a new multisecret-sharing scheme based on cyclic codes.

Consider an $[n,k]$-cyclic code C over F_q. We construct now a multisecret-sharing scheme based on C.

Let $(F_q)^k$ be the secret space and $(F_q)^n$ be the share space. In the multisecret-sharing scheme the dealer uses a share function $f:(F_q)^k \rightarrow (F_q)^n$ to compute the shares among the n participants. The sharing function is chosen as $f(s) = sG$, where $s = (s_0, s_1, \cdots, s_{k-1}) \in (F_q)^k$ is the secret and G is a $k \times n$ matrix over $(F_q)^n$ with rank k. Assume for convenience $s \neq 0$. Thus $c = sG$ is a nonzero codeword of the code C.

In this scheme, the n participants recover the secret by combining their shares as follows.

1. get the generator polynomials and matrices of cyclic code,
2. choose the polynomial for each generator polynomial such that
   $sG = (s_0 + s_1x + \cdots + s_{k-1}x^{k-1})g(x),$ (1)
   where $deg(g(x)) = n - k.$
3. get s by solving the linear system (1) of rank k.

Proposition 1. The motivation for condition 2 above is the following inequality: $2 \leq k < n$.

Proof. With the above notation it is clear that $k \neq 0$.
Assume that $k = 1$. In this case the secret consists one entry and then the scheme cannot be multisecret.
If $k = n$, then $deg(g(x)) = n - k = 0$. This means the generator polynomial is 1. Since $k = n$, the secret has size of n.

Corollary 1. If $deg(g(x)) = n - k \geq 2$, then the multisecret-sharing scheme can be constructed based on $[n,k]$-cyclic code.

Proof. By Proposition 1, while $n - k \geq 2$ it can be mentioned about multisecret-sharing. Otherwise it will be single secret-sharing.

An immediate corollary is the following.

Corollary 2. The multisecret-sharing scheme satisfied the hypothesis of the above theorems is also a (k,n)-threshold secret sharing scheme, where k is dimension and n is length of cyclic code C.

Proof. In this scheme, there are n participants and the secret has size of k. So, the result follows.

Now we have to remind an important theorem about linearity of the multisecret-sharing scheme in (Ding, 1997).

Theorem 3. A multisecret-sharing scheme defined over the above secret and share spaces is linear if and only if its share function is of the form

$$f(s) = sG,$$

where $s = (s_0, s_1, \cdots, s_{k-1}) \in (F_q)^k$ and G is a $k \times n$ matrix over $(F_q)^n$ with rank k.

Corollary 3. The multisecret-sharing scheme based on the cyclic code with generator matrix G is a linear (k,n)-threshold scheme.

Proof. It is easily seen from Theorem 3.

B. Statistics on Coalitions

Theorem 4. Let C be a q-ary $[n,k]$-cyclic code with generator matrix G. In a multisecret-sharing scheme based on C while $n-k \geq 2$, the number of minimal coalitions is $\binom{n}{k}$.

Proof. Recall that our scheme is a (k,n)-threshold secret sharing scheme. This means k out of n participants can recover the secret. These k participants consist of minimal access sets. So the number of minimal coalitions is $\binom{n}{k}$.

C. Accessibility Degree

The accessibility degree for multisecret-sharing scheme based on cyclic codes can be defined as follows.

Definition 4. Let $P = \{P_1, P_2, \cdots, P_m\}$ be a set of m participants and let A_p be the set of all access elements on P. The accessibility index on P is the map $\delta_p(\Gamma)\colon A_p \to \mathbb{R}$ given by

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

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

Example 1. Lets find all the ternary cyclic codes of length 4 and write down a generator matrix for each of them.

Over $GF(3)$, the factorization of x^4-1 into irreducible polynomials is

$$x^4-1 = (x-1)(x^3+x^2+x+1) = (x-1)(x+1)(x^2+1).$$

So there are $2^3=8$ divisors of x^4-1 in $F_3[x]$ each of which generates a cyclic code. By Theorem 1, these are the only ternary cyclic codes of length 4. The codes are specified below by their generator matrices

Generator Poynomial	Generator Matrix
11	(I_4)
$x-1$	$\begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}$
$x+1$	$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$
x^2+1	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$
$(x-1)(x+1) = x^2-1$	$\begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$
$(x-1)(x^2+1) = x^3-x^2+x-1$	$\begin{pmatrix} -1 & 1 & -1 & 1 \end{pmatrix}$
$(x+1)(x^2+1) = x^3+x^2+x+1$	$\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$
x^4-1	$\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}$

Now we construct a linear multisecret-sharing scheme based on this cyclic code. First we consider the generator polynomial $g(x) = x+1$. Since $deg(g(x)) = 1$ that is $n-k=1$, $k=3$. Let the secret vector be $s = (s_0, s_1, s_2)$, where $s_i \in F_3$, $i = 0,1,2$. We can encode s as follows.

$$(s_0 + s_1 x + s_2 x^2)g(x).$$

Let $s_0 = 1, s_1 = 0, s_2 = 1$. Therefore we write

$$(1+x^2)(1+x).$$

We know that this product is equal to sG, where G is the generator matrix. So

$$(1+x^2)(1+x) = (s_0, s_1, s_2)\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

We obtain $s_0 = 1, s_1 = 0, s_2 = 1$ by solving the linear system: $s = (101)$. The generator polynomial $(1 + x)$ gives a $(3,4)$-threshold scheme for multisecret-sharing. The accessibility degree for this scheme is

$$\frac{3}{3^4} = 0{,}037\,.$$

Second we consider the generator polynomial $g(x) = x^2 + 1$. Since $deg(g(x)) = 2, k = 2$. Let the secret vector be $s = (s_0, s_1)$ and consider $(s_0 + s_1 x)g(x)$.

Let $s_0 = 1, s_1 = 0$.

$$1.(1 + x^2) = (s_0, s_1)\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\end{pmatrix}.$$

By solving the linear system we find $s_0 = 1, s_1 = 0$: $s = (10)$.

The generator polynomial $(1 + x^2)$ gives a $(2,4)$-threshold scheme for multisecret-sharing. The generator polynomial $(1 + x)$ gives a $(2,4)$-threshold scheme for multisecret-sharing. The accessibility degree for this scheme is

$$\frac{2}{3^4} = 0{,}024.$$

Note that the multisecret-sharing scheme cannot construct by using the generator polynomials $x^3 - x^2 + x - 1, x^3 + x^2 + x + 1, x^4 - 1$.

Comparison with Other Schemes

We summarize the comparison with other code-based secret sharing schemes in the following table, where we denote by A, B, C the number of participants, the size of a secret, the number of coalitions for an $[n,k]$-code over F_q.

System	Massey	Ding et al.	Çalkavur-Solè	This paper
A	$n-1$	n	n	n
B	q	q^k	q^k	$q^k - 1$
C	$\binom{n}{k}$	$\binom{n}{k}$	$\geq \binom{n}{d-t}$	$\binom{n}{k}$

t is the error-correcting capacity of code.

A. Against Cheating

In single-secret sharing schemes some participants may present a falsified share for cheating. This problem is the same as for single-secret sharing in multisecret-sharing. By the connection between linear multisecret-sharing schemes and linear codes established by Theorem 3.

Our scheme has been constructed based on cyclic codes. Cyclic codes have a rich algebraic structure. They are splitted the classes by the generator polynomials. This means the codewords are generated by their generator polynomial. We need the genarator polynomial to recover the secret. The polynomial which is multipled by the generator polynomial consists the pieces of secret. Thus, recovering the secret depend on the choice of generator polynomial. So the secret cannot be recovered by any polynomial.

The linear multisecret-sharing scheme based on cyclic codes is attractive in against cheating. This scheme is more resilient to algebraic attacks due to the reconstruction algorithm.

Concluding Remarks

In the present article, we have constructed a new linear multisecret-sharing scheme based on cyclic codes. The reconstruction algorithm is based on generator polynomial of code. Moreover, in this study we introduce the access structure of this scheme and define its accessibility degree.

We refer to approach considered in the paper as the coding approach since

1) in single-secret sharing the secret is a component of the codeword corresponding to the information vector and the shares form all components of the codeword corresponding to the information vector,
2) in multisecret-sharing the multisecret is exactly the information vector and shares form the exact codeword corresponding to the information vector.

The advantage of the coding approach is that a cyclic code has the exclusive generator polynomials and matrices. So each share vector is a codeword of the codes generated by this generator matrix. It is important that choice of generator polynomial has some special properties, this scheme stands well, in particular in terms of security.

References

Bai, L. (1993). *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.

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

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

Çalkavur, S. & Solè, P (2017). *Multisecret sharing schemes and bounded distance decoding of linear codes*, International Journal of Computer Mathematics, vol. 94, issue. 1, pp.107-114.

Ding, C., Laihonen, T. & Renvall, A. (1997). *Linear Multisecret-Sharing Schemes and Error Correcting Codes*, Journal of Computer Science, vol. 3, no. 9, pp. 1023-1036.

Ding, C., Kohel, D. & Ling, S. (2000). *Secret Sharing with a Class of Ternary Codes*, Theor. Comp. Sci., vol. 246, pp. 285-298.

Horn, L. (1995). Comment: Multistage secret sharing based on one-way function, Electronics Letters, vol.31 (4), pp. 262.

He, J. & Dawson, E. (1994). *Multistage secret sharing based on one-way function*, Electronics Letters, vol.30 (19), pp. 1591-1592.

Hill, R. (1986). *A First Course in Coding Theory*, Oxford: Oxford University.

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

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

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

Pang, L. -J. & Wang, Y. -M. (2005). *A New (t, n) multi-secret sharing scheme based on Shamir's secret sharing*, Applied Math, vol. 167, pp. 840-848.

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

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