"Science Stays True Here"
Journal of Mathematics and Statistical Science, Volume 2016, 741-750 | Science Signpost Publishing

Secret Sharing Schemes and Syndrome Decoding

Selda Çalkavur

Math Dept, Kocaeli University, Kocaeli, Turkey.

Abstract

Error correcting codes are used to correct errors when messages are transmitted through a noisy communication channel. Syndrome decoding is a method of correcting errors. Secret sharing is an important topic in cryptography. In this paper, we explore some relations between secret sharing schemes based on the binary linear code which is a single error correcting and syndrome decoding. Then we obtain some results using this relation.

1. Introduction

Transmission and storage of information should be performed effectively and safely. Information should be handled, stored and submitted by fast and wide-ranging network connections. Errors should be corrected that occur during this process. This is the starting point of coding theory. E-mail, internet, intranet, radio, satellite, photographs from deep space, remote control of unmanned drones, store scanners (bar codes), international standard book number (ISBN) are some applications of coding theory.

Shannon showed errors can be corrected that occur during transmission or storage in a channel in 1948. The noise is the most important part in this process. A general communication system is explained as follows.

A message is transmitted to encoder from the message source. The codeword is transmitted from encoder to the noisy communication channel (The channel maybe a telephone line, a radio link with high frequency or a satellite communication link. The noise maybe a human error, lightning, thermal noise, imperfections in equipment, etc.). The received vector is transmitted to decoder. The decoded message is transmitted to user.

Secret sharing has been a subject of study for over 30 years. It is important that a secret key,

Corresponding author: Selda Çalkavur, Math Dept, Kocaeli University, Kocaeli, Turkey. Email: selda.calkavur@kocaeli.edu.tr.

passwords, informations of the plan of a secret place or an important formula of a product or i.e. must be kept secret. One of the ways of solving this problem is to give secret sharing schemes. In fact, for a secret sharing the main problem is to divide the secret into pieces instead of storing the whole. 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 are called the access structure of the scheme.

Secret sharing schemes were introduced by Blakley [1] and Shamir [11] in 1979. Then many constructions were developed. One of them is based on linear codes. The relation between secret sharing schemes and linear codes was presented in [7]. Several authors have considered the construction of secret sharing schemes using error correcting codes [3], [5], [6], [12].

In this work, we examine the relation between secret sharing schemes based on the binary linear code which is a single error correcting and syndrome decoding.

This paper is organized as follows. Section 2 reminds the necessary definitions. Section 3 explains the relation between secret sharing schemes based on the binary linear code which is a single error correcting and syndrome decoding. Section 4 collects concluding remarks.

2. Definitions

We shall begin with the necessary definitons to explain the relation between secret sharing schemes based on the binary linear code which is a single error correcting and syndrome decoding.

2.1. Codes and Syndrome Decoding

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 $C^{\perp}$. $C^{\perp}$ 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 $x = x_1 x_2 ... x_k$ as follows.

If $(x_1 x_2 ... x_k)G$, then $C = \{uG \mid u \in (F_q)^k\}$. $u \to uG$ maps the vector space q^k onto a $k-$ dimensional subspace of $(F_q)^n$.

2.2. Coset Decoding

Suppose that C is an $[n,k]$- code over F_q and a is any vector in $(F_q)^n$. Then the set $a + C$ defined by $a + C = \{a + x \mid x \in C\}$ is called a coset of C [4]. Suppose that a codeword x is sent, y is received. Then $e = y - x$ (x, y $\in (F_q)^n$), $e = e_1 e_2 ... e_n$, where e is an error vector.

Theorem 1. (Lagrange) Suppose C is an $[n,k]$- code over F_q. Then,

i) every vector of $(F_q)^n$ is in some coset of C,

ii) every coset contains exactly q^k vectors,

iii) two cosets either are disjoint or coincide,

iv) C contains exactly q^{n-k} cosets [4].

2.3. Coset Leader

The vector having minimum weight in a coset is called the coset leader. If there is more than one vector with the minimum weight, we choose one at random and call it the coset leader. Suppose H is a parity-check matrix of an $[n,k]$- code C. Then for any vector $y \in (F_q)^n$, the row vector $S(y) = yH^T$ is called the syndrome of y [4]. Moreover,

$$S(y) = 0 \Leftrightarrow y \in C.$$

Lemma 1. The vectors u and v are in the same coset of C if and only if they have the same syndrome [4].

Proof. u and v are in the same coset $\Leftrightarrow$ $u + C = v + C$

$$\Leftrightarrow u - v \in C$$

$$\Leftrightarrow (u - v)H^T = 0$$

$$\Leftrightarrow uH^T = vH^T$$

$$\Leftrightarrow S(u) = S(v)$$

[4].

□

Corollary 1. There is one-to-one correspondence between cosets and syndromes [4].

2.4. Syndrome Decoding

For the syndrome decoding we need only two columns. They are syndromes and coset leaders. This table is called syndrome-decoding look-up table. We know that two vector x and y are in the same coset of C if and only if they have the same syndrome. We also know that there is one-to-one correspondence between cosets and syndromes. The procedure (for decoding) is

i) if received vector is y, compute $S(y) = yH^T$,

ii) locate $S(y)$ in the first column of the look-up table and determine the coset leader e which has the same syndrome with y,

iii) decode y as $y - e$

[4].

2.5. Secret Sharing

The basic secret sharing scheme is Massey's scheme. Massey constructed a scheme based on an $[n,k]$- code using the generator matrix of this code. Let $s \in F_q$ be the secret. Let G be the generator matrix for a code C of length n. In a secret sharing scheme a dealer has a secret. The secret is created as follows.

Let u be any vector such that $ug_0 = s$, where g_0 is the first column vector of G. The vector u is the information vector. The dealer gives a share of the secret to each participant. There is a set P of subsets of the participants with the property that any subset of participants that is in P can determine the

secret. This set is called minimal access set [2]. The access structure of a secret sharing scheme is the set of all minimal access sets [9]. The secret s is shared to participants. The participants can recover the secret by combining their shares.

Another secret sharing scheme is a (t,n)- threshold scheme. This scheme is a method of distribution of information among n participants such that $t>1$ participants can reconstruct the secret but $t-1$ cannot. Shamir's scheme is a (t,n)- threshold scheme and was based on polynomial interpolation.

3. Secret Sharing Schemes and Syndrome Decoding

In this section, we examine the relation between secret sharing schemes based on the binary linear code which is a single error correcting and syndrome decoding. We know that syndrome decoding is an error correcting method on linear codes. Consider an $[n,k]$- code C over F_2 which is corrected a single error. Suppose that construct a secret sharing scheme based on C. Let $(F_2)^n$ be the secret space. There are participants and a dealer in this space. The dealer chooses randomly a codeword of $(F_2)^k$ as a secret s (so, it can be chosen 2^k secrets) and distributes s to participants. The participants can recover the secret by combining their shares as follows.

The secret s is transmitted to a noisy channel. Since s is a codeword, will be as r by noisy. First we get the syndrome decoding look-up table calculating syndromes of coset leaders via $S(r)=rH^T$. When a vector r is received, we calculate $S(r)$ and locate $S(r)$ in the first column of the look-up table and determine the coset leader e which has the same syndrome with r. Decode r as $r-e$. Hence the secret s is recovered.

Therefore we can write the following theorems.

Theorem 2. Let C be an $[n,k]$- code over F_2 which is a single error correcting. Suppose that the secret s is transmitted and s will be as r. To determine the secret in the secret sharing scheme based on C it should be $S(r)\neq 0$.

Proof. Suppose that $S(r)=0$. Then $r\in C$. So, the secret s is not distributed to participants. That

is $s = r$. Thus, to determine the secret it should be $S(r) \neq 0$.

□

Theorem 3. Let C be an $[n,k]$- code over F_2 which is a single error correcting. In the access structure of the secret sharing scheme based on C there are at least n minimal access sets.

Proof. The secret is recovered thanks to the coset leaders. It should be chosen the coset leaders which are to be minimal. These coset leaders are also minimal access sets in this scheme. The weight of the coset leader should be at least 1. It is known that every coset leader is length of n. Thus, there are n coset leaders which having the weight of 1. So, there are at least n minimal access sets.

□

Theorem 4. The secret sharing scheme satisfied the hypothesis of the above theorems is also the $(w_t(h), n)$-threshold scheme, where $w_t(h)$ denotes the weight of minimal access sets.

Proof. In this scheme, the minimal access sets consist of the coset leaders which are to be minimal and there are n participants in every set, as many as coordinates of C. The set of participants recovering the secret is also the set of support of these minimal access sets. The number of these participants in each of minimal access set is equal to the weight of the coset leader. So, this scheme is a $(w_t(h), n)$-threshold scheme.

□

Example 1.

Let C be the binary $[5,2]$- code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

The parity-check matrix H of C is

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Since the minimum distance is 3, the code C corrects a single error. Now we construct a secret

sharing scheme based on C and examine some properties of this scheme.

First we write the codewords of C:

$$C = \{00000, 10101, 01011, 11110\}.$$

and the cosets of C are

$$00000 + C = \{00000, 10101, 01011, 11110\}$$

$$10000 + C = \{10000, 00101, 11011, 01110\}$$

$$01000 + C = \{01000, 11101, 00011, 10110\}$$

$$00100 + C = \{00100, 10001, 01111, 11010\}$$

$$00010 + C = \{00010, 10111, 01001, 11100\}$$

$$00001 + C = \{00001, 10100, 01010, 11111\}$$

$$11000 + C = \{11000, 01101, 10011, 00110\}$$

$$10010 + C = \{10010, 00111, 11001, 01100\}.$$

It is seen that C has $q^{n-k} = 2^{5-2} = 8$ coset leaders. Some of them are minimal access sets. The elements of minimal access set have to be minimal. So, there are $n = 5$ minimal access sets:

$$\{10000\}, \{01000\}, \{00100\}, \{00010\}, \{00001\}.$$

The coset leaders of C and syndromes of their as follows.

Syndromes	Coset Leader
(000)	00000
(101)	10000
(011)	01000
(100)	00100
(010)	00010
(001)	00001
(110)	11000
(111)	10010

Let any element of C be the secret s. It will be shared to participants. Then the secret s is transmitted to channel. To determine the secret it should be calculated the syndrome of the received vector.

Let the secret s be 01011 and is transmitted to channel and the received vector r be 01010. We calculate the syndrome of r:

$$S(r) = rH^T = (01010).\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (001)$$

(001) belongs to (00001) coset leader. So, where the error vector is $e = (00001)$. Therefore

$$s = r - e$$

$$s = (01010) - (00001)$$

$$s = (01011)$$

is obtained. Thus, the secret is recovered.

3.1. Why Use Syndrome Decoding?

What is the advantage of using syndrome decoding in this scheme? The nonzero coset leaders which are to be minimal are minimal access sets here. The components in every coset leader can recover the secret by combining their shares. Also the order of the components is too important. Because, if the position of any component is changed, then the secret can not recover. This means the access structure of this scheme is very strong and reliable.

4. Conclusion

In the present article, we have explored the relation between secret sharing schemes based on the binary linear code which is a single error correcting and syndrome decoding. In this context, we have obtained the following results.

- In this scheme to determine the secret it should be $S(r) \neq 0$, where r is the received vector,
- there are at least n minimal access sets,
- this scheme is a $(w_t(h), n)$-threshold scheme, where $w_t(h)$ denotes the weight of minimal access sets.

References

[1]. Blakley, G. R. ”Safeguarding Cryptographic Keys”, in Proc. 1979 National Computer Conf., New York, pp. 313-317, Jun. 1979.

[2]. Brickell, E. F., "Some Ideal Secret Sharing Schemes", Advances in Cryptology-EUROCRYPT 89, Lecture Notes in Computer Science, vol. 434, pp.468-475, 1990.

[3]. Ding, C., Kohel, D. and Ling, S. "Secret Sharing with a Class of Ternary Codes", Theor. Comp. Sci., vol. 246, pp. 285-298, 2000.

[4]. Hill, R. " A First Course in Coding Theory", Oxford: Oxford University, 1986.

[5]. Karnin, E. D., Greene, J. W. and Hellman, M. E. "On Secret Sharing Systems", IEEE Trans. Inf. Theory, vol. IT-29, no:1, pp. 35-41, Jan. 1983.

[6]. Massey, J. L. "Minimal Codewords and Secret Sharing", in Proc. 6th Joint Swedish-Russian Workshop on Information Theory, Mölle, Sweden, pp. 276-279, Aug. 1993.

[7]. Mc. Eliece, R. and Sarwate, D., "On Sharing Secrets and Reed-Solomon Codes", Communications of the ACM, vol. 24, pp. 583-584. 1981.

[8]. Okada, K. and Kurosawa, K. "MDS Secret Sharing Scheme Secure Against Cheaters", IEEE Trans. Inf. Theory, vol. 46, no. 3, pp. 1078-1081.

[9]. Özadam, H., Özbudak, F., Saygı, Z., "Secret Sharing Schemes and Linear Codes", Information Security Cryptology Conference with International Participation, Proceedings, pp.101-106, December 2007.

[10]. Piepryzk, J. and Zhang, X. M. "Ideal Threshold Schemes from MDS Codes" , in Information Security and Cryptology-Proc. of ICISC 2002 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2003, vol. 2587, pp. 269-279.

[11]. Shamir, A. ”How to Share a Secret", Commun. Assoc. Comp. Mach., vol. 22, pp. 612-613, 1979.

[12]. -"Some Applications of Coding Theory", Cryptography, Codes and Ciphers: Cryptography and Coding IV, pp. 33-47, 1995.

Published: Volume 2016, Issue 12 / December 25, 2016