Construction and Analysis of Nonlinear Secret Sharing Schemes

Deepak Agrawal

Construction and Analysis of Nonlinear Secret Sharing Schemes

A

Thesis submitted

in Partial Fulfilment of the Requirements

for the Degree of

Doctor of Philosophy

by

Deepak Agrawal

Supervisor:

Dr. Smarajit Das

Dr. Srinivasan Krishnaswamy

Department of Electronics and Electrical Engineering
Indian Institute of Technology Guwahati
Guwahati - 781039, Assam, India

Sept, 2024

Declaration

I hereby declare that the thesis entitled "**Construction and Analysis of Nonlinear Secret Sharing Schemes**", submitted in the *Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, Assam, India*, for the award of the degree of **Doctor of Philosophy**, has been carried out by me under the supervision and guidance of Dr. Smarajit Das and Dr. Srinivasan Krishnaswamy. The results embodied in this thesis are original and have not been submitted to any other University or Institute for the award of any degree or diploma.

Dated:

Place: Guwahati

Deepak Agrawal

Research Scholar

Dept. of Electronics and Electrical Engineering

Indian Institute of Technology Guwahati

Guwahati - 781039, Assam, India.

Certificate

This is certify that the thesis entitled "**Construction and Analysis of Nonlinear Secret Sharing Schemes**", submitted by **Deepak Agrawal** (166102008), a research scholar in the Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, for the award of the degree of **Doctor of Philosophy**, is a record of an original research work carried out by his under our supervision and guidance. The thesis has fulfilled all requirements as per the regulations of the institute and in our opinion has reached the standard needed for submission. The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

Dated:

Dr. Smarajit Das

Dr. Srinivasan Krishnaswamy

Dept. of Electronics and Electrical Engg.

Indian Institute of Technology Guwahati

Guwahati - 781 039, Assam, India.

To

My Parents

Mrs. Bimla Devi Agrawal & Late Shri Ramawatar Agrawal

Acknowledgments

First and foremost, I wish to express my gratitude to my thesis supervisors Dr. Smarajit Das and Dr. Srinivasan Krishnaswamy, for their guidance throughout my Ph.D. tenure. I would like to thank my doctoral committee members: Dr. A. Rajesh, Prof. Anupam Saikia, and Dr. Tony Jacob for sparing time out of their busy schedule to evaluate my progress and enrich this work with their valuable suggestions and feedbacks. I would also like to thank Dr. Hanumant Singh Shekahawat and Dr. Kuntal Deka for helping me with my research work in innumerable ways. I thank to Mukut Da, Fulchand Kumawat, Sumit Singha for offering a helping hand whenever I needed. I would also like to thank everyone in communications Lab III, who made these years really enjoyable. During my stay here in IIT Guwahati, I made many friends with whom I shared several precious memories that will stay with me forever. The comradery shared among myself, Dr. Ujwal, Vikas, Pothan, Dr. Ashish and Gangesh is unbelievable and I thank them all for their friendship. The encouragement and guidance received from seniors Dr. Prateek, Dr. Pawan and Dr. Uddipana were immensely helpful in writing this thesis.

My sincere thanks to my seniors Dr. Sam Darshi and Dr. Brijesh Kumbhani for some of the extremely important discussions and feedbacks during the National Conference on Communication at IITG.

I express my deep appreciation to my wife Ruchi for her unconditional support and understanding for all these moments. This Ph.D. would not have been possible without her help and support. I extend my love to my Son Yogesh and Harsh.

Lastly, I extend my sincere thanks to all the staff members from EEE office and Academic office for helping me out in all sorts of ways during my stay at IITG.

Abstract

A secret sharing scheme is a method by which a set of shares are generated from secret data. These shares are then distributed among a set of participants. The secret can then be recovered from the shares of legitimate subsets of participants. The set of these subsets is called the access structure of the scheme. If the functions that recover the secret from the shares are all linear, then the scheme is called a linear secret sharing scheme. The inherent linearity of these secret recovery functions enable participants to cheat by wrongly declaring their shares during secret recovery. An example of such an attack is the 'Tompa-Woll' attack. In these attacks, the wrongly declared share leads to a wrongly recovered secret. However, the cheating participants can use the linearity of the recovery function to calculate the correct secret from the wrongly recovered one. Various verification techniques have been devised to detect this kind of cheating. An alternate method of resisting such attacks is by designing schemes with nonlinear secret recovery functions. These functions must be such that the cheating participants gain no information about the actual secret from the wrongly recovered one. This motivates the study of nonlinear secret sharing schemes.

The first contribution of this thesis is to formulate a framework for defining access structures of nonlinear code based secret sharing schemes. This framework is then used to define access structures of secret sharing schemes based on the Nordstrom-Robinson code and other codes derived from the Nordstrom-Robinson code. Further, access structures for schemes based on a few Hadamard codes have also been derived.

We then look at nonlinear boolean functions from a secret sharing point of view. In particular, boolean expressions derived from linear equations over the ring $\mathbb{Z}_4$ have been explored. Closed-form formulae for such expressions have been derived. We have then derived a few information-theoretic results that enable us to analyse these equations from a secret sharing point of view. A couple of secret sharing schemes are then designed and

analysed based on these results. Finally, a few areas of potential research related to this thesis have been suggested.

Contents

List of Tables

List of Acronyms

SSS	Secret Sharing Scheme
AS	Access structure
RM	Reed-Muller code

List of Symbols

$\mathcal{N}_{16}$	Nordstrom-Robinson code
G_{24}	Extended binary Golay code
F_2	Finite field of cardinality 2
Z	Ring of integers
Z_4	Ring of integers modulo 4
Z_{2^k}	Ring of integers modulo 2^k
$+$	Addition in F_2 or Z_4 depending on the context
$H(X)$	Shannon Entropy of the random variable X
$H(X/Y)$	Shannon Entropy of the random variable X conditioned on the random variable Y
$I(X;Y)$	Mutual information between random variable X and Y
$\mathcal{K}(m)$	Kerdock code of order m
$\mathcal{P}(m)$	Preparata code of order m
V	n-dimension vector space over F_2
W_C	Weight distribution of the code C
$\widehat{\mathcal{N}}_{16}$	Minkowski sum of the code $\mathcal{N}_{16}$ with itself

d_{min}	Minimum Hamming distance of code

1

Introduction

Contents

Secret sharing is a mechanism by which a secret is shared among a set of participants. A legitimate subsets of these participants can than regenerate the secret. A typical example why such a mechanism is required is given as below.

Consider an encryption scheme wherein decrypted data can be recovered only by a party who possess a secret key. Here the loss of secret key, results in loss of the data. A way of overcoming this problem is by giving the key to a number of participants, this however compromises the security of encryption scheme. An elegant way of working around this problem is through the use of a secret sharing scheme. Here, a mathematical function generates a set of shares from the secret. These shares are then distributed among a set of participants. The individual shares contain little or no information about the secret but the secret can be recovered from legitimate subsets of shares. If the number of such legitimate subsets is sufficiently high, even if a few of the shares are lost, the secret can be recovered. Besides key sharing, secret sharing is used in a wide array of applications ranging from multiparty communication to blockchain.

The following section gives a brief history of secret sharing and a concise literature review.

1.1 Secret Sharing Schemes: A Brief History

Secret sharing was introduced simultaneously by Shamir and Blakley in the year 1979. A secret sharing scheme is a method of generating a set of shares from a secret. These shares are then distributed among a set of participants. The shares of legitimate subsets of participants can then recover the secret.

In Shamir's scheme a secret is considered to be a coefficient of a k^{th} degree polynomial and the other coefficients are chosen randomly. The shares consist of evaluations of this polynomial at a set of points. To reconstruct the secret one needs any k such evaluations. In other words, the secret can be recovered from any set of k shares. This property is known as 'thresholdness' and such a scheme is called a (k, n)-threshold scheme. Besides threshlodness, Shamir's scheme has the following properties:

- Mutual information between the secret and any set of less than k shares is zero. This property is known as perfectness.
- The size of share and secret is same.

A scheme, like that of Shamir's, which satisfies both the above properties is known as an ideal secret sharing scheme.

In contrast, Blakley's secret sharing scheme considers the secret to be the intersection of n hyperplanes in a k dimensional space. Each share contains information from which a hyperplane can be reconstructed. In order to determine the secret, k such hyperplanes need to be reconstructed. In contrast to Shamir's secret sharing scheme Blakley's scheme is not perfect.

An implementation of Shamir's secret sharing scheme using Reed Solomon codes is given in [1]. Consider an (n, k)-Reed Solomon code. The shares are generated by encoding a message vector $\mathbf{m} \in \mathbb{F}_q^k$ using the Reed Solomon code. The first entry m_0 of the message vector is the secret while the remaining entries are chosen randomly. If G is a generator matrix of the Reed-Solomon code then the share vector $\mathbf{s} \in \mathbb{F}_\mathbf{q}^\mathbf{n}$ is calculated as $\mathbf{s} = \mathbf{mG}$. Clearly, the number of shares is equal to the number of columns of G. Consider a column vector $\mathbf{v} \in \mathbb{F}_\mathbf{q}^\mathbf{n}$ such that $G\mathbf{v} = (\mathbf{1}, \mathbf{0}, \ldots, \mathbf{0})^\mathbf{T}$. Now,

$$\mathbf{sv} = \mathbf{m}G\mathbf{v} = \mathbf{m} \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = m_0$$

Thus the secret can be recovered from subsets of shares such that the span of the corresponding columns contains the vector $(1, 0, \ldots, 0)^T$. This defines the access structure of the scheme.

An alternate method of using a code for secret sharing scheme is given in [2]. Here, a secret is considered to be an entry of a codeword. Without loss of generality this entry can be taken as the first one. The linear relations between the entries of the codewords are used to reconstruct the secret. The access structure in such schemes is determined by those codewords of the dual code whose first entry is non-zero. For example, consider a linear code C with a dual code C'. Let $v = (v_0, v_1, \ldots, v_{n-1})$ be an element of C', where $v_0 \neq 0$. Apart from v_0, let $v_{i_1}, v_{i_2}, \ldots, v_{i_k}$ be the nonzero entries in v. Now for any $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, $c_0 = -v_0^{-1}(c_{i_1}v_{i_1} + c_{i_2}v_{i_2} + \cdots + c_{i_k}v_{i_k})$. Thus, if c_0 corresponds to the secret, then it can be recovered as a function of $c_{i_1}.c_{i_2}, \ldots, c_{i_k}$. Thus, the access structure corresponds to the support of elements of the dual code with a nonzero first entry.

The above paradigms are used in the construction of various secret sharing schemes [1, 3–5]:

In all the schemes mentioned above, the secret is recovered by evaluating a linear function of the shares. Such schemes are called linear secret sharing schemes. The inherent linearity of these schemes enables a participant to cheat by modifying his share.

For example, consider a secret s that is got by evaluating the following linear function on a set of shares $s_1, s_2, \ldots, s_k$ as

$$s = a_1 s_1 + a_2 s_2 + \cdots + a_k s_k.$$

If the first participant maliciously declares her share as $s_1 + \epsilon$, then the recovered secret will be $s' = s + a_1\epsilon$. Knowing the values of a_1 and ϵ, the cheating participant can recover the correct secret from s'. However, the other participants will be stuck with the wrong secret s'. An example of such an attack is the Tompa-Woll attack on Shamir's scheme described in [6].

In a secret sharing scheme the party distributing the share is called as dealer while the party recalculating the secret is called as the combiner. The data could be corrupted on the communication line between the dealer and the participants. This, along with participant cheating makes it necessary to verify the integrity of shares at both the participants' end and the combiner's end. This led to the development of verifiable secret sharing schemes [7].

A verifiable secret sharing scheme has an additional algorithm which allows the participants to verify the shares that they have got from the dealer. In a publicly verifiable secret sharing scheme, the shares can be verified by any entity using information that is publicly available. An example of such a scheme is the one given in [8]

A robust secret sharing scheme is a scheme in which the secret can be recovered in the presence of incorrect or faulty shares [9]. This is achieved by using techniques like adding authentication tags and error correction. Typically, in such schemes the share size will be more than that of the secret.

1.2 Motivation of Thesis

As mentioned in the previous section the linearity of secret sharing scheme facilitates cheating by participants. Therefore nonlinear secret recovery functions can potentially diminish the ability of a participant or a group of participants to cheat. This motivates the study of nonlinear codes for secret sharing.

This thesis looks at the following aspects of secret sharing schemes using nonlinear codes.

1. Defining access structure for such schemes:

We first give a general method for constructing access structures of nonlinear code based secret sharing schemes. We then used this method to construct the access structure of various nonlinear codes like the Nordstrom-Robinson code and it's derived codes and Hadamard codes,. Further we analyse these schemes from the point of view of perfectness and ability of participants to cheat.

2. Study of Boolean Functions for Secret Sharing: While boolean functions and their constructions have been thoroughly analysed from a cryptographic point of view [10–15], there is not much literature that analyses boolean functions from the point of view of secret sharing. $\mathbb{Z}_4$ linear codes like the Nordstrom-Robinson code can be used to construct nonlinear binary secret sharing schemes. However, the secret recovery functions in schemes defined in [16–18], which are based on well known $\mathbb{Z}_4$ linear codes, are linear in some of their arguments. This enables some of the participants to launch 'Tompa-Woll'-like attacks. The closeness of a secret sharing scheme to perfectness and its resilience to 'Tompa-Woll'-like attacks depends on its secret recovery functions. The secret recovery functions in such schemes are boolean functions that originate from linear equations over $\mathbb{Z}_4$. This work characterizes linear equations over $\mathbb{Z}_4$ that give rise to boolean expressions that are desirable for secret sharing. Further, conditions that ensure that such boolean functions are nonlinear in all their arguments are derived. Then, closed-form expressions for these boolean functions are found. For a function of several boolean random variables, an expression for the mutual information between the evaluation of the function and maximal strict subsets of its arguments is derived. For secret recovery functions, this value must be close to zero for the scheme to be nearly perfect. Further, when one of the arguments of such a function is changed, assuming that the argument's value is known, we derive an expression for the mutual information between the evaluation of the function with the original argument and its evaluation with the modified one. For secret recovery functions, this value should be close to zero for the scheme to be resistant to 'Tompa-Woll'-like attacks. These information theoretic results are then appled to the derived closed-form expressions for analyzing and designing secret sharing schemes based on $\mathbb{Z}_4$ linear codes. The first scheme has a single element access structure. This scheme is then extended to a scheme with a multi-element access structure. Both these schemes are evaluated for their closeness to 'perfectness' and their ability to resist 'Tompa-Woll'-like attacks.

1.3 Organisation of Thesis

Chapter 2 describes a framework for defining the access structure of secret sharing schemes based on nonlinear codes. Using this framework, the access structure of schemes based on the Nordstrom-Robinson code, a few of its derivatives, and a few Hadamard codes have been defined.

Chapter 3 analyses a special class of boolean functions from a secret sharing point of view. Closed-form expressions have been calculated for nonlinear boolean functions derived from linear functions over $\mathbb{Z}_4$. These expressions have been used to construct a couple of secret sharing schemes.

Chapter 4 discusses a few open questions related to nonlinear secret sharing. These are potential areas for future research. The thesis is summarized in Chapter 5.

2

Secret Sharing Schemes based on Nordstrom-Robinson and Hadamard Codes

Contents

In this chapter, we construct secret sharing schemes based on nonlinear codes. The following nonlinear codes are considered: Hadamard codes, Nordstorm-Robinson code ($\mathcal{N}_{16}$), and codes obtained by shortening and puncturing of $\mathcal{N}_{16}$. We analyse the resilience of these schemes to "Tompa-Woll"- like attacks.

2.1 Nordstrom-Robinson Code($\mathcal{N}_{16}$)

The Nordstrom-Robinson code $\mathcal{N}_{16}$ is a nonlinear $(16, 256, 6)$ code.

The code $\mathcal{N}_{16}$ may be viewed [19] as a subcode of the extended binary Golay code $\mathcal{G}_{24}$. The code $\mathcal{G}_{24}$ is a linear $[24, 12, 8]$ code. As the code has minimum Hamming distance 8, we change the order of the symbols of $\mathcal{G}_{24}$ so that $\mathcal{G}_{24}$ contains the codeword $1111111100...0 = 1^8 0^{16}$. Let G be a generator matrix of the code $\mathcal{G}_{24}$. As it is self-dual, any 7 columns of G are linearly independent. Thus the first 7 coordinates may be taken as information symbols, and the 8^{th} coordinate is the sum of the first 7 symbols. We divide the codewords according to their values on the first 7 coordinates: there are 2^7 possibilities, and for each of these there are $2^{12}/2^7 = 32$ codewords. Thus there are $8 \times 32 = 256$ codewords which begin either with seven $0's$ (with 8^{th} coordinate 0), six $0's$ and a 1 (with 8^{th} coordinate 1). The table below illustrates the construction of the code $\mathcal{N}_{16}$ from $\mathcal{G}_{24}$.

Table 2.1: Nordstrom-Robinson Code from G_{24}

length 7	*length* 1	*length* 16
0000000	0	32 codewords
1000000	1	32 codewords
0100000	1	32 codewords
0010000	1	32 codewords
0001000	1	32 codewords
0000100	1	32 codewords
0000010	1	32 codewords
0000001	1	32 codewords
....		32×120 codewords (the rest of the codewords of G_{24})

Note that the Nordstrom-Robinson code $\mathcal{N}_{16}$ is subcode of the Golay code G_{24}. As the Golay code is a binary linear code of dimension 12, it contains 32×120 more codewords in addition to the 256 codewords of the Nordstrom-Robinson code.

2.2 Access Structure of Nonlinear Secret Sharing Schemes

Let V be an n-dimensional vector space over $\mathbb{F}_2$. For an $x \in V$, the symbol $|x|$ represents the Hamming weight of x. For two vectors $x = (x_1, x_2, \cdots, x_n), y = (y_1, y_2, \cdots, y_n) \in V$, we define $x.y$ as $(x_1y_1, \cdots, x_ny_n)$ and $x \vee y$ is the vector $z = (z_1, z_2, \cdots, z_n)$ where $z_i = 1$ if $x_i = 1$ or $y_i = 1$. We say the vector x is covered by a vector y if $y_i = 1$ whenever $x_i = 1$.

If $C \subset V$ contains M vectors with minimum Hamming distance d, then C is called an (n, M, d) code. The n codeword symbols of a codeword $c \in C$ are indexed by the set $\langle n \rangle = \{1, 2, \cdots, n\}$ and we write $c = (c_1, c_2, \cdots, c_n)$. For an (n, M, d) code C, let A_i be the number of codewords of Hamming weight i in the code C. The weight enumerator of the code C is defined as the polynomial

$$\sum_{i=0}^{n} A_i x^{n-i} y^i.$$

The weight enumerator of the code $\mathcal{N}_{16}$ is $x^{16} + 112x^{10}y^6 + 30x^8y^8 + 112x^6y^{10} + y^{16}$.

For any two subsets A, B of the vector space V, Minkowski sum $A + B$ is defined as the set

$$A + B = \{a + b | a \in A, b \in B\}.$$

If $A = B = \mathcal{N}_{16}$, then Minkowski sum is denoted by

$$\widehat{\mathcal{N}}_{16} = \mathcal{N}_{16} + \mathcal{N}_{16}.$$

Using the description of the code $\mathcal{N}_{16}$ as shown in the 2.1 table, it is easy to verify that $\widehat{\mathcal{N}}_{16}$ is a $[16, 29 \times 32 = 928, 4]$ nonlinear code. Furthermore, the weight enumerator of $\widehat{\mathcal{N}}_{16}$ is $x^{16} + 448x^{10}y^6 + 30x^8y^8 + 448x^6y^{10} + y^{16}$.

For any subset $B \subset \langle n \rangle$, the punctured code $C|_B$ is the code obtained from C where the symbols of each codeword of C that are outside B are punctured. In the process, two codewords of C may become identical after puncturing. However, $|C|_B|$ will denote the number of distinct elements in $C|_B$.

An (n, M, d) binary code C can equivalently be described by a collection $\mathcal{M}$ of subsets of $\langle n \rangle$ such that a codeword $c = (c_1, c_2, \cdots, c_n) \in C$ is identified as the subset $A = \{i | c_i = 1, i = 1, 2, \cdots, n\}$.

Let us fix a codeword symbol $c_s, s \in \langle n \rangle$ as the secret and we want to find a subset A of $\langle n \rangle \setminus \{s\}$ such that the codeword symbol c_s can be determined uniquely from the knowledge of the codeword symbols indexed by the set A. In other words, we have to verify whether the following condition holds:

$$|C|_{\{s\} \bigcup A}| = |C|_A|. \tag{2.1}$$

The collection $\mathcal{A}_s$ of all such subsets $A \subset \langle n \rangle \setminus \{s\}$ will be called the access structure for the code C corresponding to the fixed symbol c_s considered as the secret. Note that the access structure $\mathcal{A}_s$ for the code C is dependent on the symbol c_s chosen as secret.

We also define another access structure $\mathcal{B}$ for the code C as follows: we say the set $B \subset \langle n \rangle$ is an element of $\mathcal{B}$ if

$$|C|_{B \setminus \{b\}}| = |C|_B | \forall b \in B.$$

In other words, B is in the access structure $\mathcal{B}$ if we consider any symbol from the set B as secret and it will be determined uniquely by knowing only the remaining symbols from the set B. Note that

$$\begin{aligned} &|C|_{B \setminus \{b\}}| = |C|_B | \forall b \in B \\ &\text{if and only if } d_{\min}(\mathcal{C}|_B) \geq 2. \end{aligned} \tag{2.2}$$

These two access structures are related as follows:

$$\text{If } B \in \mathcal{B}, \text{ then } B \setminus \{s\} \in \mathcal{A}_s \forall s \in B. \tag{2.3}$$

2.2.1 Shortened and Punctured Codes from Nordstrom-Robinson Code ($\mathcal{N}_{16}$)

We consider several codes constructed from the code $\mathcal{N}_{16}$ using two operations called shortening and puncturing.

Puncturing is the process of removing a symbol from each codeword of a code. In this work, shortening of a code refers to choosing those codeowrds of a code that have zeros in specified positions. Puncturing $\mathcal{N}_{16}$ by at most five symbols results in a code that has as many codewords as it is in the original code. This is because the minimum Hamming distance of $\mathcal{N}_{16}$ is six. The codes obtained by puncturing any one symbol of $\mathcal{N}_{16}$ are all equivalent to each other. We denote this code by $\mathcal{N}_{15}$. It is a $(15, 256, 5)$ nonlinear code.

Similarly, if we remove two symbols from each codeword of the code $\mathcal{N}_{16}$, we have a (14, 256, 4) nonlinear code denoted by $\mathcal{N}_{14}$.

Likewise, we get a (13, 256, 3) code ($\mathcal{N}_{13}$) and a (12, 256, 2) code $\mathcal{N}_{12}$ by puncturing the last 3 and 4 symbols of $\mathcal{N}_{16}$ respectively.

On the other hand, if we apply a shortening operation on the code $\mathcal{N}_{16}$, we get codes with fewer number of codewords while keeping the minimum Hamming distance fixed.

We consider those codewords of $\mathcal{N}_{16}$ with i-th coordinate zero and then remove the i-th symbol from them. The resulting shortened code is a $(15, 128, 6)$ code denoted by $\mathcal{N}'_{15}$.

Similarly, we can construct a (14,64,6) code ($\mathcal{N}'_{14}$), a (13,32,6) code ($\mathcal{N}'_{13}$) and a (12,16,6) code($\mathcal{N}'_{12}$) by shortening the last $2, 3$ and 4 symbols of $\mathcal{N}_{16}$ respectively.

2.3 Weight Distribution of the Punctured and Shortened Subcodes of $\mathcal{N}_{16}$

Weight distribution of the dual of a linear code C conveys a lot of information about the access structure of a secret sharing scheme based on the code C. In the nonlinear case too, the weight polynomial of a code plays an important role. In the following, we list the weight polynomials of the codes considered here.

In the following table 2.2, we state the weight polynomials of the code $\mathcal{N}_{16}$ and it's punctured subcodes, namely, $\mathcal{N}_{15}$, $\mathcal{N}_{14}$, $\mathcal{N}_{13}$ and $\mathcal{N}_{12}$.

The code $\mathcal{N}_{16}$ consists of one codeword of Hamming weight zero and also of Hamming weight 16, 112 codewords of Hamming weight 6 and 10, 30 codewords of weight 8. As the code $\mathcal{N}_{15}$ is obtained by puncturing one symbol from the code $\mathcal{N}_{16}$, we can calculate the weight distribution of the code $\mathcal{N}_{15}$ as follows. There are 42 codewords of weight 5 and 70 codewords of weight 6 in the code $\mathcal{N}_{15}$ resulting from the 112 codewords of weight 6 in the code $\mathcal{N}_{16}$. This is because $112 \times 6/16 = 42$ is the number of codewords of Hamming weight 5 and the remaining $112 - 42$ codewords are of Hamming weight 6. Similarly, there are $30 \times 8/16 = 15$ codewords of Hamming weight 7 and $30 - 15$ codewords of Hamming weight 8 in the code $\mathcal{N}_{15}$. Finally, there are $112 \times 10/16 = 70$ codewords of Hamming weight 9, $112 - 70 = 42$ codewords of Hamming weight 10 and one codeword of Hamming weight 15 in the code $\mathcal{N}_{15}$.

We can find the weight distribution of the codes $\mathcal{N}_{15}$, $\mathcal{N}_{14}$, $\mathcal{N}_{13}$ and $\mathcal{N}_{12}$ similarly.

Codes	Weight Polynomials
$\mathcal{N}_{16}(16, 256, 6)$	$x^{16} + 112x^{10}y^6 + 30x^8y^8 + 112x^6y^{10} + y^{16}$
$\mathcal{N}_{15}(15, 256, 5)$	$x^{15} + 42x^{10}y^5 + 70x^9y^6 + 15x^8y^7 + 15x^7y^8 + 70x^6y^9 + 42x^5y^{10} + y^{15}$
$\mathcal{N}_{14}(14, 256, 4)$	$x^{14}+14x^{10}y^4+56x^9y^5+49x^8y^6+16x^8y^7+49x^6y^8+56x^5y^9+14x^4y^{10}+y^{14}$
$\mathcal{N}_{13}(13, 256, 3)$	$x^{13} + 4x^{10}y^3 + 30x^9y^4 + 57x^8y^5 + 36x^7y^6 + 36x^6y^7 + 57x^5y^8 + 30x^4y^9 + 4x^3y^{10} + y^{13}$
$\mathcal{N}_{12}(12, 256, 2)$	$x^{12} + x^{10}y^2 + 12x^9y^3 + 43x^8y^4 + 52x^7y^5 + 38x^6y^6 + 52x^5y^7 + 43x^4y^8 + 12x^3y^9 + x^2y^{10} + y^{12}$

Table 2.2: Weight polynomials of $\mathcal{N}_{15}, \mathcal{N}_{14}, \mathcal{N}_{13}$ and $\mathcal{N}_{12}$

In the following table 2.3 we state the weight polynomials of the code $\mathcal{N}_{16}$ and it's shortened subcodes $\mathcal{N}'_{15}$, $\mathcal{N}'_{14}$, $\mathcal{N}'_{13}$ and $\mathcal{N}'_{12}$.

The code $\mathcal{N}_{16}$ consists of one codeword of Hamming weight zero and also of Hamming weight 16. 112 codewords of Hamming weight 6 and 10, 30 codewords of weight 8. As the code $\mathcal{N}'_{15}$ is obtained by shortening last one symbol from the code $\mathcal{N}_{16}$. We remove all the codewords of $\mathcal{N}_{16}$ whose last symbol is one and we collect all the codewords whose last symbol is zero. We can calculate the weight distribution of the code $\mathcal{N}'_{15}$ as follows. There are $112 \times 6/16 = 42$ codewords of weight 6 whose last symbol is one and $112 - 42 = 70$ codewords of weight 6 whose last symbol is zero in the code $\mathcal{N}_{16}$. There are $30 \times 8/16 = 15$ codewords of weight 8 whose last symbol is one and $30 - 15 = 15$ codewords of weight 8 whose last symbol is zero in the code $\mathcal{N}_{16}$. There are $112 \times 10/16 = 70$ codewords of weight 10 whose last symbol is one and $112 - 70 = 42$ codewords of weight 10 whose last symbol is zero. Hence by removing all such codewords whose last symbol is one in the code $\mathcal{N}_{16}$ we obtain one codeword of weight 0, 70 codewords of weight 6, 15 codewords of weight 8 and 42 codewords of weight 10.

We can find the weight distribution of the codes $\mathcal{N}'_{14}$, $\mathcal{N}'_{13}$ and $\mathcal{N}'_{12}$ using the above method.

Codes	Weight Polynomials
$\mathcal{N}_{16}(16, 256, 6)$	$x^{16} + 112x^{10}y^6 + 30x^8y^8 + 112x^6y^{10} + y^{16}$
$\mathcal{N}'_{15}(15, 128, 6)$	$x^{15} + 70x^9y^6 + 15x^7y^8 + 42x^5y^{10}$
$\mathcal{N}'_{14}(14, 64, 6)$	$x^{14} + 42x^8y^6 + 7x^6y^8 + 14x^4y^{10}$
$\mathcal{N}'_{13}(13, 32, 6)$	$x^{13} + 24x^7y^6 + 3x^5y^8 + 4x^3y^{10}$
$\mathcal{N}'_{12}(12, 16, 6)$	$x^{12} + 13x^6y^6 + x^4y^8 + x^2y^{10}$

Table 2.3: Weight polynomials of $\mathcal{N}'_{15}, \mathcal{N}'_{14}, \mathcal{N}'_{13}$ and $\mathcal{N}'_{12}$

We state the weight polynomials of $\widehat{\mathcal{N}_{16}}, \widehat{\mathcal{N}_{15}}, \widehat{\mathcal{N}_{14}}, \widehat{\mathcal{N}_{13}}, \widehat{\mathcal{N}_{12}}$ in the following Table 2.4 and weight polynomials of $\widehat{\mathcal{N}_{16}}, \widehat{\mathcal{N}'_{15}}, \widehat{\mathcal{N}'_{14}}, \widehat{\mathcal{N}'_{13}}\widehat{\mathcal{N}'_{12}}$ in the Table 2.5.

Codes	Weight polynomials
$\widehat{\mathcal{N}_{16}}(16, 256, 6)$	$x^{16} + 448x^{10}y^6 + 30x^8y^8 + 448x^6y^{10} + y^{16}$
$\widehat{\mathcal{N}_{15}}(15, 256, 5)$	$x^{15} + 168x^{10}y^5 + 280x^9y^6 + 15x^8y^7 + 15x^7y^8 + 280x^6y^9 + 168x^5y^{10} + y^{15}$
$\widehat{\mathcal{N}_{14}}(14, 256, 4)$	$x^{14}+56x^{10}y^4+224x^9y^5+196x^8y^6+16x^8y^7+49x^6y^8+224x^5y^9+56x^4y^{10}+y^{14}$
$\widehat{\mathcal{N}_{13}}(13, 256, 3)$	$x^{13}+16x^{10}y^3+120x^9y^4+228x^8y^5+36x^7y^6+36x^6y^7+57x^5y^8+120x^4y^9+16x^3y^{10}+y^{13}$
$\widehat{\mathcal{N}_{12}}(12, 256, 2)$	$x^{12}+4x^{10}y^2+48x^9y^3+132x^8y^4+208x^7y^5+152x^6y^6+52x^5y^7+43x^4y^8+48x^3y^9+4x^2y^{10}+y^{12}$

Table 2.4: Weight polynomials of $\widehat{\mathcal{N}_{16}}, \widehat{\mathcal{N}_{15}}, \widehat{\mathcal{N}_{14}}, \widehat{\mathcal{N}_{13}}$ and $\widehat{\mathcal{N}_{12}}$

Codes	Weight Polynomials
$\widehat{\mathcal{N}_{16}}(16, 256, 6)$	$x^{16} + 448x^{10}y^6 + 30x^8y^8 + 448x^6y^{10} + y^{16}$
$\widehat{\mathcal{N}'_{15}}(15, 128, 6)$	$x^{15} + 280x^9y^6 + 15x^7y^8 + 168x^5y^{10}$
$\widehat{\mathcal{N}'_{14}}(14, 64, 6)$	$x^{14} + 168x^8y^6 + 7x^6y^8 + 56x^4y^{10}$
$\widehat{\mathcal{N}'_{13}}(13, 32, 6)$	$x^{13} + 96x^7y^6 + 3x^5y^8 + 16x^3y^{10}$
$\widehat{\mathcal{N}'_{12}}(12, 16, 6)$	$x^{12} + 52x^6y^6 + x^4y^8 + 4x^2y^{10}$

Table 2.5: Weight polynomials of $\widehat{\mathcal{N}'_{16}}, \widehat{\mathcal{N}'_{15}}, \widehat{\mathcal{N}'_{14}}, \widehat{\mathcal{N}'_{13}}$ and $\widehat{\mathcal{N}'_{12}}$

2.4 Secret Sharing Scheme based on Nordstrom-Robinson Code ($\mathcal{N}_{16}$)

In this section, we determine the access structure $\mathcal{B}$ for the code $\mathcal{N}_{16}$ according to the definition given by (2.2). For any subset $A \subset \langle 16 \rangle$, we calculate the number of codewords in $\mathcal{N}_{16}|_A$ and then we use the equation (2.1) to determine if the subset A lies in the access structure or not. In the following lemma, we consider subsets of cardinality at most 7.

Lemma 1. *Let $A \subset \langle 16 \rangle$ be a set of cardinality at most 7. Then, $|\mathcal{C}|_A| = 2^{|A|}$.*

Proof. The code $\mathcal{C}$ has the dual distance $d' = 6$, By a theorem of Delsarte [19], any set of $r \leq d' - 1$ columns of $\mathcal{C} = \mathcal{N}_{16}$ contains each r-tuple exactly 2^{8-r} times. Therefore, if the cardinality of A is $r \leq 5$, then the number of distinct codewords in $\mathcal{C}|_A$ is 2^r, i.e., $|\mathcal{C}|_A| = 2^r$. It can also be checked by exhaustive search that the number of codewords in $\mathcal{C}|_A$ is $2^{|A|}$ even if the cardinality of A is 6 or 7. (However, in these cases, all r-tuples may not occur identical number of times in the code C.) □

It follows that the subsets of cardinality at most 7 are not in the access structure $\mathcal{B}$. On the other hand, each subset of cardinality at least 12 is in the access structure $\mathcal{B}$ as the minimum Hamming distance of $\mathcal{N}_{16}$ is 6.

The table below lists the number of distinct codewords in $\mathcal{N}_{16}|_A$ for all $A \subset \langle 16 \rangle$ containing $8, 9, 10$ or 11 elements.

Table 2.6: Access Structure $\mathcal{A}_{16}$

Number of Codewords \ $\lvert A\rvert$	8	9	10	11
128	**30**	0	0	0
192	10080	0	0	0
224	0	4480	**448**	0
256	2760	6960	**840** + 6720	**1680**+ 2688

For example, if A is an 8-element set, then $|\mathcal{C}|_A| \in \{128, 192, 256\}$. In particular, there are 30 sets of cardinality 8 for which the number of distinct codewords in the corresponding punctured code is 128, similarly $10,080$ sets with 192 distinct codewords and 2760 sets with 256 codewords.

The numbers in boldface in the Table 2.6 indicate the number of sets of given cardinality lying in the access structure. For example, there are exactly 30 sets of cardinality 8 in the access structure. Note that we also have $1288(840 + 448)$ sets of cardinality 10 and 1680 sets of cardinality 11 in the

access structure. We follow this convention while describing access structures of several codes given later. It can be easily verified that 840 sets of cardinality 10 and 1680 sets of cardinality 11 are obtained from 30 sets of cardinality 8 by adding two elements and three elements respectively. Thus among all the sets that are in the access structure, the minimal elements with respect to set inclusion are the 30 sets of cardinality 8 and 448 sets of cardinality 10. Note that there are 30 codewords of Hamming weight 8 and 448 codewords of Hamming weight 10 in the code $\widehat{\mathcal{N}}_{16}$. These codewords correspond to the minimal elements in the access structure.

In the following, we establish that these are the only elements in the access structure $\mathcal{B}$. We first state few lemmas.

Lemma 2. *Let $x, y \in \widehat{\mathcal{N}}_{16}$ and $|x| \neq 6$. Then, $|x.y| \neq 1$.*

Proof. It is sufficient if it holds for x for which $|x| = 8$ or 10.

(i) Let $|x| = 8$. Suppose there exist an element $y \in \widehat{\mathcal{N}}_{16}$ such that $|x.y| = 1$, then, $|y| \leq 9$ as $|x \vee y| = |x| + |y| - |x.y| \leq 16$.

If $|y| = 8$, then $|x - \overline{y}| = 2$. We get a contradiction as $\overline{y} \in \widehat{\mathcal{N}}_{16}$ and the minimum Hamming distance is 4 for this code. Note $\overline{y} = y + 1$ is the complement of y.

If $|y| = 6$, then $|x - \overline{y}| = 4$. We again get a contradiction as the distance between any weight-8 and weight 10- codeword of $\widehat{\mathcal{N}}_{16}$ is 6.

(ii) Let $|x| = 10$. Suppose there exist an element $y \in \widehat{\mathcal{N}}_{16}$ such that $|x.y| = 1$, then, $|y| \leq 7$ as $|x \vee y| = |x| + |y| - |x.y| \leq 16$.

If $|y| = 6$, then $|x - \overline{y}| = 2$. This contradicts the fact that the minimum Hamming distance is 4 for this code.

□

We first define a notion of covering a binary vector x by another binary vector y.

Definition 1. *A vector $x \in \mathbb{F}_2^n$ is said to be covered by a vector $y \in \mathbb{F}_2^n$ if y_i is one whenever x_i is one.*

The following results can be verified using Matlab explicitly as the code $\widehat{\mathcal{N}}_{16}$ is not too large.

- Let $x \in \widehat{\mathcal{N}}_{16}$ be any codeword of Hamming weight 8. Let $\widehat{x}$ be any vector of weight at least 10 such that x is covered by $\widehat{x}$. Then, $|\widehat{x}.y| \neq 1 \forall y \in \widehat{\mathcal{N}}_{16}$.

- Define the sets $\mathcal{H}_1$ and $\mathcal{H}$ as follows:

$$\mathcal{H}_1 = \{\widehat{x} | \widehat{x} \text{ covers } x \in \widehat{\mathcal{N}}_{16}, |x| = 8, |\widehat{x}| \geq 10\},$$
$$\mathcal{H} = \{x \in \widehat{\mathcal{N}}_{16} || x| \neq 0, 6\} \cup \mathcal{H}_1. \tag{2.4}$$

Let $x \in \mathbb{F}_2^{16}$ be a vector which is not in $\mathcal{H}$. Then, $|\widehat{x}.y| = 1$ for some $y \in \widehat{\mathcal{N}}_{16}$.

- For any 9-element A with $|\mathcal{C}|_A| = 256$, there exists at least one 8-element subset $B \subset A$ such that $|\mathcal{C}|_B|$ is either 128 or 192.

Theorem 1. *The access structure $\mathcal{B}$ of $\mathcal{N}_{16}$ is given by the collection of sets $\mathcal{H}$ as described by* (2.4).

Proof. Let $A \subset \langle 16 \rangle$ be a set such that $d_{\min}(\mathcal{C}|_A) \geq 2$. Then, the minimum Hamming weight of the code $\widehat{N}_{16}|_A$ is at least 2. This is the case if $|x_A.y| \neq 1 \forall y \in \widehat{\mathcal{N}}_{16}$, where x_A is the binary vector corresponding to the set A. It follows from the Lemma 2 and the above observations that the vector x_A must be in the set $\mathcal{H}$. We have $\mathcal{B} = \mathcal{H}$.

□

The determination of the access structure of the first kind as given by equation (2.1) can be derived from the above result.

Theorem 2. *Let s-th co-ordinate of the codewords in the code $\mathcal{N}_{16}$ be considered as the secret. Then, the access structure $\mathcal{A}_s$ of the secret sharing scheme based on $\mathcal{N}_{16}$ is determined as follows: a set $A \subset \langle 16 \rangle \setminus \{s\}$ is in $\mathcal{A}_s$ if and only if $A \cup \{s\}$ is in $\mathcal{B}$ or if $|\mathcal{N}_{16}|_A| = 256$.*

Proof. By Equation (2.3), if $A \cup \{s\}$ is in $\mathcal{B}$, then $A \in \mathcal{A}_s$. If $|\mathcal{N}_{16}|_A| = 256$, then $|\mathcal{N}_{16}|_{A\cup\{s\}|} = 256 = |\mathcal{N}_{16}|_A|$, hence $A \in \mathcal{A}_s$. Now we prove the converse. Suppose there exists an $A \in \mathcal{A}_s$ such that $A \cup \{s\} \notin \mathcal{B}$. Then, $|\mathcal{N}_{16}|_A| = |\mathcal{N}_{16}|_{A\cup\{s\}|}$. This does not hold if $|A| < 7$. For $|A| \geq 7$, it follows that $|\mathcal{N}_{16}|_A| = 256$ using table 2.6. □

2.4.1 Formally Dual Code

Let C and C' be two nonlinear codes with weight polynomials $W_C(x, y)$ and $W_{C'}(x, y)$ respectively. The codes C and C' are said to be formally dual of each other if the corresponding weight polynomials satisfy Macwilliams identity, ie.,

$$W_{C'}(x, y) = \frac{1}{|C|} W_C(x + y, x - y).$$

The codes $\mathcal{N}_{15}$ and $\mathcal{N}'_{15}$ are formally dual of each other.

2.5 Access Structure of the Secret Sharing Schemes based on $\mathcal{N}_{15}$ and $\mathcal{N}'_{15}$

We first determine the access structure $\mathcal{A}_{15}$ of the secret sharing scheme based on the codes $\mathcal{N}_{15}$.

The table below lists the number of distinct codewords in $\mathcal{N}_{15}|_A$ for all subsets $A \subset \langle 15 \rangle$ of cardinality $7, 8, 9, 10$ and 11.

The access structure $\mathcal{A}_{15}$ consists of the following sets:

(i) 15 **sets of cardinality 8**: these sets correspond to the codewords of Hamming weight 8 in the code $\widehat{\mathcal{N}'_{15}}$.

Table 2.7: Access Structure $\mathcal{A}_{15}$

Number of Codewords \ $\lvert A\rvert$	7	8	9	10	11
64	0	0	0	0	0
128	6435	**15**	0	0	0
192	0	5040	0	0	0
224	0	0	1960	**168**	0
256	0	1380	3045	**315** + 2520	**525** + 840

(ii) 483 **sets of cardinality 10**: It comprises of sets corresponding to 168 codewords of Hamming weight 10 in the code $\widehat{\mathcal{N}'_{15}}$ and the remaining sets obtained by adding two elements to the 15 sets of cardinality 8 in the access structre $\mathcal{A}_{15}$. Note that $315 = 15 \times \binom{7}{2}$.

(iii) **525 sets of cardinality 11**. These sets are obtained by adding three elements to the 15 sets of cardinality 8 in the access structure $\mathcal{A}_{15}$, Note that $525 = 15 \times \binom{7}{3}$.

(iv) **Sets of size 12 or more**.

Thus, the minimal elements in the access structure $\mathcal{A}_{15}$ comprise of 15 sets of cardinality 8 and 168 sets of cardinality 10. These sets correspond to the codewords of Hamming weight 8 and 10 respectively in the code $\widehat{\mathcal{N}'_{15}}$.

If we compare the access structure of the code $\mathcal{N}_{16}$ and $\mathcal{N}_{15}$, it follows that $\mathcal{A}_{15}$ can be obtained from $\mathcal{A}_{16}$ by shortening operation.

We now determine the access structure $\mathcal{A}'_{15}$ of the secret sharing scheme based on the code $\mathcal{N}'_{15}$. In the Table 2.8 below, we describe this access structure.

The access structure $\mathcal{A}'_{15}$ consists of following sets:

(i) **15 sets of cardinality 7 and 15 sets of cardinality 8**: These sets correspond to the codewords of Hamming weight 7 and 8 in the code $\widehat{\mathcal{N}_{15}}$.

(ii) **There are** $280 + 525 = 805$ **sets of cardinality 9**: 280 sets correspond to the codewords of Hamming weight 9 in the $\widehat{\mathcal{N}_{15}}$ and the remaining 525 sets are formed by adjoining one (two)

Table 2.8: Access Structure $\mathcal{A}'_{15}$

Number of Codewords \ $\lvert A\rvert$	6	7	8	9	10
64	5005	**15**	0	0	0
96	0	5040	0	0	0
112	0	0	2520	**280**	**168**
128	0	1380	**15** + 3900	**525** + 4200	**1155** + 1680

element(s) to the sets of cardinality 7 (8) described above. Note that

$$525 = 15 \times \binom{8}{2} + 15 \times \binom{7}{1}.$$

(iii) **There are** $168 + 1155$ **sets of cardinality 10 in access structure**: 168 sets correspond to the codewords of Hamming weight 10 in the $\widehat{\mathcal{N}_{15}}$ and the remaining sets are supersets of the 7-element and 8-element sets described above. Note that

$$1155 = 15 \times \binom{8}{3} + 15 \times \binom{7}{2}.$$

(iv) **Sets of size 11 and more**.

Thus, the minimal elements in the access structure $\mathcal{A}'_{15}$ comprise of 15 sets of cardinality 7, 15 sets of cardinality 8, 280 sets of size 9 and 168 sets of size 10.

These sets correspond to the codewords of Hamming weight $7, 8, 9$ and 10 in the code $\widehat{\mathcal{N}_{15}}$.

If we compare the access structure of the code $\mathcal{N}_{16}$ and $\mathcal{N}'_{15}$, it follows that $\mathcal{A}'_{15}$ can be obtained from $\mathcal{A}_{16}$ by puncturing operation.

2.6 Access Structure of the Secret Sharing Scheme based on $\mathcal{N}_{14}$

Table 2.9: Access Structure $\mathcal{A}_{14}$

$\|A\|$ / Number of Codewords	6	7	8	9	10	11
64	3003	0	0	0	0	0
128	0	3443	**7**	0	0	0
192	0	0	2352	0	0	0
224	0	0	0	784	**56**	0
256	0	0	644	1218	**105** + 840	**140** + 224

There are 7 sets of cardinality 8 in the access strucutre: These sets correspond to the 7 codewords of weight 8 .in the code $\widehat{N'_{14}}$.

There are $56 + 105$ **sets of cardinality 10 in the access structure**: Of these sets, 56 sets correspond to the codewords of weight 10 in the code $\widehat{N'_{14}}$ and the remaining 105 sets supersedes of 7-element sets described above. Note that

$$105 = 7 \times \binom{6}{2}.$$

There are 140 sets of cardinality 11 in the access structure: these sets are obtained by adding elements to the sets of size 7 listed above. We have

$$140 = 7 \times \binom{6}{3}.$$

2.7 Access Structure of Secret Sharing Scheme based on the $\mathcal{N}_{13}(13, 256, 3)$

Table 2.10: Access Structure $\mathcal{A}_{13}$

Number of Codewords \ $\lvert A\rvert$	6	7	8	9	10	11
64	1716	0	0	0	0	0
128	0	1716	**3**	0	0	0
192	0	0	1008	0	0	0
224	0	0	0	280	**16**	0
256	0	0	276	435	**30** + 240	**30** + 48

From the above table, we can see that there are 3 sets of cardinality 8, $(16+30 = 46)$ sets of cardinality 10 and 30 sets of cardinality 11 in the access structure $\mathcal{A}_{13}$. It can be easily verified that these 3 sets of Hamming weight 8 and 16 sets of weight 10 correspond to the codewords of weight 8 and weight 10 respectively in the code $\widehat{\mathcal{N}'_{13}}$.

Note that these three sets of cardinality 8 and 16 sets of cardinality 10 constitute the minimal elements of the access structure. Note that

$$30 = 3 \times \binom{5}{2} = 3 \times \binom{5}{3}.$$

2.7.1 Access Structure of Secret Sharing Scheme based on the $\mathcal{N}_{12}(12, 256, 2)$

Table 2.11: Access Structure $\mathcal{A}_{12}$

Number of Codewords \ $\lvert A\rvert$	6	7	8	9	10	11
64	924	0	0	0	0	0
128	0	792	**1**	0	0	0
192	0	0	390	0	0	0
224	0	0	0	88	**4**	0
256	0	0	104	132	**6**+56	**4**+8

From the above table, it follows that there is exactly one set of the cardinality 8 and 4 sets of cardinality 10 in the access structure. These sets correspond to the weight 8 and weight 10 codewords in the code $\mathcal{N}'_{12}$. Also, we have the following elements in the access structure: 6 more sets cardinality 10 and 4 sets of cardinality 11 that are supersets of the set of size 8 in the access structure.

$$6 = 1 \times \binom{4}{2}, 4 = 1 \times \binom{4}{3}.$$

2.8 Secret Sharing Schemes based on Hadamard codes

2.8.1 Hadamard codes

A Hadamard matrix H_n of order n is an $n \times n$ matrix of $+1$'s and -1's such that $HH^T = nI$. For any prime p, such that $p+1$ is multiple of 4, Paley's construction [19] can be used to generate Hadamard matrix of order $n = p + 1$.

Paley's construction:

Let

$$H_n = \begin{bmatrix} 1 & \mathbf{1} \\ \mathbf{1}^T & Q - I \end{bmatrix},$$

where Q is the Jacobsthal matrix $Q = (q_{ij})$. This is a $p \times p$ matrix whose rows and columns are labeled $0, 1, \cdots, p-1$ and $q_{ij} = \chi(j-i)$, where χ is the Legendre symbol defined on the integers by

(i) $\chi(i) = 0$ if i is a multiple of p.

(ii) $\chi(i) = 1$ if i is a quadratic residue mod p.

(iii) $\chi(i) = -1$ if i is a quadratic non-residue mod p.

If $+1$'s are replaced by 0's and -1's are replaced by 1's, then H_n is changed into the binary

Hadamard matrix A_n. The matrix A_{12} is shown below.

$$A_{12} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

The matrix A_n gives three Hadamard codes, i.e.,

(i) An $(n-1, n, \frac{1}{2}n)$ code $\mathcal{A}_{n-1}$ consisting of the rows of A_n, with the first column deleted.

(ii) An $(n-1, 2n, \frac{1}{2}n-1)$ code $\mathcal{B}_{n-1}$ consisting of $\mathcal{A}_{n-1}$, together with the complements of all its codewords.

(iii) An $(n, 2n, \frac{1}{2}n)$ code $\mathcal{C}_n$ consisting of the rows of A_n and their complements [19].

We consider the above three kind of Hadamard codes for $n = 12$.

Let

$$\mathcal{D}_{11} = \{x + y | x, y \in A_{11}, x \neq y\},$$

$$\mathcal{E}_{11} = \{x, \mathbf{1} + x | x \in \mathcal{D}_{11}\},$$

$$\mathcal{F}_{12} = \{(\mathcal{P}(x), x) | x \in \mathcal{E}_{11}\},$$

where $\mathbf{1}$ denotes the all-1 vector and $\mathcal{P}(x)$ is 1 if the number of 1's in x is odd, else 0. Note that the code $\mathcal{D}_{11}$ contains 66 codewords of Hamming weight 6 only. Furthermore, $\mathcal{E}_{11}$ contains 66 codewords of Hamming weight 6 and 66 codewords of Hamming weight 5. Finally, the code $\mathcal{F}_{12}$ contains 132 codewords of Hamming weight 6 only.

Let $\mathcal{J}_1, \mathcal{J}_2$ and $\mathcal{J}_3$ be the access structures of the secret sharing schemes based on the codes $\mathcal{A}_{11}, \mathcal{B}_{11}$ and $\mathcal{C}_{12}$ respectively. The tables shown below list the number of distinct codewords in $\mathcal{A}_{11}|_A, \mathcal{B}_{11}|_A$ and $\mathcal{C}_{12}|_A$ for all subsets $A \subset \langle 11 \rangle$ consisting of $2, 3, 4, 5$ and 6 elements.

Table 2.12: Access Structure $\mathcal{J}_1$

Number of Codewords \ $\lvert A\rvert$	2	3	4	5	6
4	55	0	0	0	0
8	0	165	0	0	0
11	0	0	330	**66**	0
12	0	0	0	396	**66**+396
Total	55	165	330	462	462

The following observations play an important role in determining the access structure of these codes. This has been verified by exhaustive search.

(i)

$$\mathcal{E}_{11} \subset \mathcal{J}_1. \tag{2.5}$$

(ii) Let A be a subset of $\mathbb{F}_2^n$ and $\mathcal{B}_1(A)$ be the union of the sets of points in the Hamming sphere of radius 1 with center at the points in A. Then,

$$\mathcal{B}_1(\mathcal{D}_{11}) = \cup_{i=4}^{7} \mathbb{P}_i(\langle 11 \rangle). \tag{2.6}$$

Table 2.13: Access Structure $\mathcal{J}_2$

Number of Codewords \ $\lvert A\rvert$	2	3	4	5	6
4	55	0	0	0	0
8	0	165	0	0	0
16	0	0	330	0	0
22	0	0	0	462	**66**
24	0	0	0	0	396
Total	55	165	330	462	462

Table 2.14: Access Structure $\mathcal{J}_3$

Number of Codewords \ $\lvert A\rvert$	2	3	4	5	6
4	66	0	0	0	0
8	0	220	0	0	0
16	0	0	495	0	0
22	0	0	0	792	**132**
24	0	0	0	0	792
Total	55	165	330	792	924

In the following, we determine the access structure for the three codes described above.

Theorem 3. *Let $\mathcal{J}_1, \mathcal{J}_2$ and $\mathcal{J}_3$ be the access structures of the secret sharing schemes based on the codes $\mathcal{A}_{11}, \mathcal{B}_{11}$ and $\mathcal{C}_{12}$ respectively. Then,*

$$\begin{aligned}\mathcal{J}_1 &= \{A \subset \langle 11\rangle \mid |A| \geq 7\} \cup \mathcal{E}_{11},\\ \mathcal{J}_2 &= \{A \subset \langle 11\rangle \mid |A| \geq 8\} \cup \mathcal{D}_{11},\\ \mathcal{J}_3 &= \{A \subset \langle 12\rangle \mid |A| \geq 8\} \cup \mathcal{F}_{12}.\end{aligned}$$

Proof. The access structure $\mathcal{J}_1$ is determined as follows. Define $X = \{1, 2, \cdots, 11\}$. For two subsets A and B of X, define $d(A, B)$ to be the size of the set $(A \setminus B) \cup (B \setminus A)$.

As $\mathcal{A}_{11}$ is a nonlinear $(11, 12, 6)$ code, any subset of X containing at least 7 elements lies in $\mathcal{J}_1$.

By Lemma (2.5), $\mathcal{E}_{11} \subset \mathcal{J}$. We now show that any set that does not fall in any of the above types, must not be in the access structure J_1.

We start with a set A of cardinality 6 that is not in $\mathcal{E}_{11}$. From Lemma (2.6), it follows that there exists a set $B \in \mathcal{E}_{11}$ such that $d(A, B) = 1$. Furthermore, B must have an odd number of elements. This forces the cardinality of B to be 5. As $B + X$ has cardinality 6, we have $B + X \in \mathcal{D}_{11}$ and $|(B + X) \cap A| = 1$. This implies that $A \notin \mathcal{J}_1$

Let $A \notin \mathcal{E}_{11}, |A| = 5$. Consider any 4-element subset D of A. By Lemma 4, there exists a set $B \in \mathcal{E}_{11}, |B| = 5$ such that $D \subset B$. It is clear that $d(A, B) = 2$. Therefore, $|A \cap (B + X)| = 1$. Note that $B + X \in \mathcal{A}_{11} + \mathcal{A}_{11}$. Thus, $A \notin \mathcal{J}_1$

We now show that $|\mathcal{A}_{11}|_A| < 12$ for all $A \in \mathcal{E}_{11}, |A| = 5$. We have $(A + X) \in \mathcal{E}_{11}$. In fact, $(A + X) \in \mathcal{D}_{11}$. Then, $A + X = C_1 + C_2$ for some $C_1, C_2 \in \mathcal{A}_{11}$. Hence, $C_1 \cap A = C_2 \cap A$. This shows that $|\mathcal{A}_{11}|_A| < 12$. Given $A \in \mathcal{E}_{11}, |A| = 5$, there is exactly one pair of codewords $C_1, C_2 \in \mathcal{A}_{11}$ such that $A + X = C_1 + C_2$. Therefore, $|\mathcal{A}_{11}|_A| = 11$ for all $A \in \mathcal{E}_{11}, |A| = 5$.

Furthermore, as $|\mathcal{A}_{11}|_A| = 11$ and $d_{min}(\mathcal{A}_{11}|_A) \geq 2$, we have $|\mathcal{A}_{11}|_B| = 11$ for all $B \subset A, |B| = 4$. Any 4-element subset of $\langle 11 \rangle$ can be obtained by removing one element from the 5-element sets of $\mathcal{E}_{11}$. Therefore, $|\mathcal{A}_{11}|_B| = 11$ for any 4-element subset B of $\langle 11 \rangle$. This shows that no 4-element subset of $\langle 11 \rangle$ is in the access structure.

As $|\mathcal{A}_{11}|_B| = 11$ for all $B \subset A, |B| = 4$, we have $|\mathcal{A}_{11}|_C| \geq 6$ for all $C \subset \langle 11 \rangle, |B| = 3$. Therefore, no 3-element subset of $\langle 11 \rangle$ is in the access structure. Furthermore, no one-element or two-element set is in $\mathcal{J}_1$ as the dual distance of $\mathcal{A}_{11}$ is three. In the similar way, one can determine the access structures $\mathcal{J}_2$ and $\mathcal{J}_3$ corresponding to $\mathcal{B}_{11}$ and $\mathcal{C}_{12}$ respectively. □

2.9 Tompa-Woll attack

We now analyze the performance of $\mathcal{N}_{16}$ against "Tompa-Woll attack". In this secret sharing scheme, let the symbol $c_s, s \in \langle 16 \rangle$ of a codeword $c \in \mathcal{N}_{16}$ be the secret and the remaining 15 symbols are given as shares to the 15 participants. The access structure $\mathcal{A}_s$ consists of sets of size 7 or more as described in Theorem 2.

Let $A \in \mathcal{A}_s$ be a set of size 7, i.e., $\hat{A} := A \cup \{s\} \in \mathcal{B}$. As the symbols indexed by $\hat{A}$ satisfies a linear equation, i.e., $c_s + \sum_{i \in A} c_i = 0$, "Tompa-Woll attack" will be successful in this case.

We now consider a set $A \in \mathcal{A}_s$ with 8 elements, i.e., $|C|_A| = 256$. Suppose the set $\hat{A} := A \cup \{s\}$ has a subset $B \in \mathcal{B}$ of size 8, then $s \in B$, otherwise c_s can not be determined the participants indexed by A. In this case, c_s is effectively determined by the participants indexed by $B \setminus \{s\}$. In fact, $c_s = \sum_{i \in B \setminus \{s\}} c_i$. It is similar to the previous case.

Let us consider a set $A \in \mathcal{A}_s, |A| = 8$ such that $A \cup \{s\}$ has no 8-element subset B in $\mathcal{B}$. Let $A = \{a_0, a_1, \cdots, a_7\}$ and $x_i = c(a_i)$ for $i = 0, 1, \cdots, 7$. Then, c_s is not a linear function of x_i's. For one such A, we will have the following expression of c_s in terms of x_i's:

$$\begin{aligned} c_s =& x_2 + x_4 + (x_1 + x_3 + x_6 + x_1x_3 + x_3x_6 + x_6x_1) \\ &+ x_0(x_1 + x_3 + x_5 + x_7) + x_5(x_3 + x_6 + x_7) \\ &+ x_7(x_1 + x_6) \end{aligned}$$

Note the participant x_2 or the participant x_4 can cheat others but no other participant can cheat the others. As long as the two participants x_2 and x_4 are reliable, the Tompa-Woll attack can be resisted in this case.

We now analyse the performance of Hadamard code against "Tompa-Woll" attack. We choose one subset $A \subset \langle 11 \rangle$ from the access structure of the code $\mathcal{E}_{11}$. Let $A = \{2, 4, 5, 6, 10\}$. The corresponding polynomial equation is

$$\begin{aligned} x_2 =& x_4x_5x_6 + x_4x_5x_{10} + x_4x_5 + x_4x_6x_{10} + x_4x_6 + x_4x_{10} \\ &+ x_5x_6x_{10} + x_5x_6 + x_5x_{10} + x_6x_{10}. \end{aligned}$$

From the above equation, it follows that no participant can fool other by modifying its share.

3

Nonlinear Secret Sharing Schemes based on Z_4 Linear Codes

Contents

As seen in the previous chapter, nonlinear codes can be used to build secret sharing schemes. $\mathbb{Z}_4$ linear codes are a class of nonlinear codes that are derived from linear codes over the ring $\mathbb{Z}_4$. In this chapter, we analyse Boolean secret recovery functions appearing in secret sharing schemes based on $\mathbb{Z}_4$ linear codes. We derive closed form formulae for such functions and derive conditions for their nonlinearity. Finally, we propose a couple of schemes and analyse their resistance to 'Tompa-Woll'-like attacks.

3.1 Nonlinear Codes from $\mathbb{Z}_4$ Linear Codes and a few Assumptions

A linear code over $\mathbb{Z}_4$ can be converted to a code over $\mathbb{F}_2$ by replacing each symbol with its corresponding Gray code representation. Thus, each symbol in $\mathbb{Z}_4$ gives rise to two binary symbols. The resulting binary codes are often nonlinear due to the nonlinearity of the Gray map ($0 \longrightarrow 00, 1 \longrightarrow 01, 2 \longrightarrow 11, 3 \longrightarrow 10$). An example of such a code is the Nordstrom-Robinson code.

In this work, it is assumed that the secret is uniformly distributed. For a secret s, the shares are generated by randomly sampling a codeword from the uniform distribution on the set of codewords whose first entry is s. Thus, if the code is balanced in the first symbol i.e., the number of codewords corresponding to each value of the first symbol is the same, then the shares can come from any codeword with equal probability.

If the shares are taken as random variables, then their respective distributions and mutual correlations depend on the code. For example, if the secret sharing scheme is based on the Reed-Solomon code, then any two shares are mutually independent.

In the following section, we look at boolean expressions that arise from linear equations over $\mathbb{Z}_4$ and at some simple results in information theory that help us analyze boolean secret sharing schemes that are derived from linear codes over $\mathbb{Z}_4$.

3.2 Some Basic Results

When symbols in $\mathbb{Z}_4$ are represented by their corresponding Gray codes, every linear function from $\mathbb{Z}_4^n$ to $\mathbb{Z}_4$, gives rise to two boolean functions corresponding to each bit of the output. This section looks at the properties of such boolean functions.

Theorem 4. *Consider the linear function $s = a_1c_1 + \cdots + a_nc_n$ where $s, c_1, \ldots, c_n \in \mathbb{Z}_4$ and $a_1, a_2, \ldots, a_n$ are units in $\mathbb{Z}_4$. For, $1 \leq i \leq n$, let (c_{i1}, c_{i2}) be the Gray code representation of c_i. Let (s_1, s_2) be the Gray code representation of s. If $s_2 = f(c_{11}, c_{12}, \ldots, c_{n1}, c_{n2})$, then, f is a nonlinear function in each of its arguments.*

Proof. Proving that the function f is nonlinear in arguments c_{ij} is equivalent to proving the following.

- The function f depends on c_{ij}. This is proved by showing that there exists a set of values for the other arguments such that a change in c_{ij} causes a change in s_2.
- The nonlinear dependence on c_{ij} is proved by showing that there exists a set of values for the other arguments such that a change in c_{ij} does not cause a change in s_2.

Consider the equation $s = a_1c_1 + \cdots + a_nc_n$. Consider $c^1, c^2 \in \mathbb{Z}_4$ such that they differ only in the second Gray code symbol. The values of all other variables remaining the same, when the value of c_n is changed from c^1 to c^2 the change in the value of s is $a_n(c^1 - c^2)$. Further, $c^1 - c^2$ is either 1 or 3 (-1 mod 4). As a_n is a unit in $\mathbb{Z}_4$, it can either be 1 or 3. Hence, $a_n(c^1 - c^2)$ is either 1 or 3.

If $a_n(c^1-c^2) = 1$, then consider a choice of $c_1, \ldots, c_{n-1}$, where $a_1c_1+a_2c_2+\cdots+a_{n-1}c_{n-1}+a_nc^2 = 1$. Therefore, $a_1c_1 + a_2c_2 + \cdots + a_{n-1}c_{n-1} + a_nc^1 = 2$.

Similarly, if $a_n(c^1 - c^2) = 3$ then consider a choice of $c_1, \ldots, c_{n-1}$, where $a_1c_1 + a_2c_2 + \cdots + a_{n-1}c_{n-1} + a_nc^2 = 0$. Therefore, $a_1c_1 + a_2c_2 + \cdots + a_{n-1}c_{n-1} + a_nc^1 = 3$.

In both these cases, the change in value of c_{n2} does not change the value of s_2. Hence, if the evaluation of the function f depends on the value of c_{n2}, then f is nonlinear in c_{n2}. We now proceed to prove the dependence of the function f on c_{n2}.

If $a_n(c^1 - c^2) = 1$ then choose $c_1, \ldots, c_{n-1}$ such that $a_1c_1 + a_2c_2 + \cdots + a_{n-1}c_{n-1} + a_nc^2 = 2$. Therefore, $a_1c_1 + a_2c_2 + \cdots + a_{n-1}c_{n-1} + a_nc^1 = 3$.

If $a_n(c^1 - c^2) = 3$ then choose $c_1, \ldots, c_{n-1}$ such that $a_1c_1 + a_2c_2 + \cdots + a_{n-1}c_{n-1} + a_nc^2 = 1$. Therefore, $a_1c_1 + a_2c_2 + \cdots + a_{n-1}c_{n-1} + a_nc^1 = 0$.

In both these cases a change in c_{n2} changes the value of s_2. Thus, the evaluation of the function f depends on the value of c_{n2}. Thus, the function f is nonlinear in c_{n2}. We can similarly prove that f is nonlinear in each of its arguments. □

In the following set of results, we derive closed-form expressions for boolean functions arising from linear functions over $\mathbb{Z}_4$.

Lemma 3. *Consider $c_1, c_2 \in \mathbb{Z}_4$. Let $c \in \mathbb{Z}_4$ be the sum of c_1 and c_2 i.e., $c = c_1 + c_2$. Let (x, y), (x_1, y_1) and (x_2, y_2) be the Gray code representations of c, c_1, and c_2 respectively. Then,*

$$x = (y_1 + x_1).(y_2 + x_2) + x_1 + x_2,$$
$$y = (y_1 + x_1).(y_2 + x_2) + y_1 + y_2,$$

where '+' and '.' indicate addition and multiplication over $\mathbb{F}_2$ respectively.

Proof. The binary representations of c, c_1, and c_2 are $(x, x + y)$, $(x_1, x_1 + y_1)$ and $(x_2, x_2 + y_2)$ respectively. Therefore,

$$x + y = x_1 + y_1 + x_2 + y_2. \tag{3.1}$$

The carry generated by the addition of x_1+y_1 and x_2+y_2 is given by $c = (x_1+y_1).(x_2+y_2)$. Therefore,

$$x = (x_1 + y_1).(x_2 + y_2) + x_1 + x_2. \tag{3.2}$$

The following expression for y is got by adding Equations (3.1) and (3.2).

$$y = (x_1 + y_1).(x_2 + y_2) + y_1 + y_2.$$

□

Corollary 1. *Consider $c_1, c_2 \in \mathbb{Z}_4$. Let $c \in \mathbb{Z}_4$ be given by the following linear combination of c_1 and c_2,*

$$c = c_1 + 2c_2. \tag{3.3}$$

Let (x, y), (x_1, y_1) and (x_2, y_2) be the images under the Gray map of c, c_1, and c_2 respectively. Then,

$$x = x_2 + y_2 + x_1,$$
$$y = x_2 + y_2 + y_1.$$

Proof. Equation (3.3) can be written as follows.

$$c = c_1 + c_2 + c_2.$$

Let $z = c_1 + c_2$. Let (x_z, y_z) be the Gray code representation of z. Hence, by Lemma (3),

$$x_z = (x_1 + y_1).(x_2 + y_2) + x_1 + x_2,$$
$$y_z = (x_1 + y_1).(x_2 + y_2) + y_1 + y_2.$$

Therefore, $x_z + y_z = x_1 + x_2 + y_1 + y_2 = (x_1 + y_1) + (x_2 + y_2)$. Applying Lemma (3) to expression $c = z + c_2$ we get the following.

$$\begin{aligned}
x &= (x_z + y_z).(x_2 + y_2) + x_z + x_2 \\
&= [(x_1 + y_1) + (x_2 + y_2)].(x_2 + y_2) + (x_1 + y_1).(x_2 + y_2) + x_1 + x_2 + x_2 \\
&= x_2 + y_2 + x_1, \\
y &= (x_z + y_z).(x_2 + y_2) + y_z + y_2 \\
&= [(x_1 + y_1) + (x_2 + y_2)].(x_2 + y_2) + (x_1 + y_1).(x_2 + y_2) + y_1 + y_2 + y_2 \\
&= x_2 + y_2 + y_1.
\end{aligned}$$

□

The following two corollaries can be proved on similar lines.

Corollary 2. *Consider $c_1, c_2 \in \mathbb{Z}_4$. Let $c \in \mathbb{Z}_4$ be given by the following linear combination of c_1 and c_2,*

$$c = c_1 + 3c_2.$$

Let (x, y), (x_1, y_1) and (x_2, y_2) be the Gray code representations of c, c_1, and c_2 respectively. Then,

$$x = (y_1 + x_1).(y_2 + x_2) + x_1 + y_2,$$
$$y = (y_1 + x_1).(y_2 + x_2) + y_1 + x_2.$$

Corollary 3. *Consider $c_1, c_2 \in \mathbb{Z}_4$. Let $c \in \mathbb{Z}_4$ be given by the following linear combination of c_1 and c_2,*

$$c = 3c_1 + 3c_2.$$

Let (x, y), (x_1, y_1) and (x_2, y_2) be the Gray code representations of c, c_1, and c_2 respectively. Then

$$x = (y_1 + x_1).(y_2 + x_2) + y_1 + y_2,$$
$$y = (y_1 + x_1).(y_2 + x_2) + x_1 + x_2.$$

The above results lead to the following theorem regarding boolean expressions derived from linear equations over $\mathbb{Z}_4$ where the coefficients are all units.

Theorem 5. *Consider $c_1, c_2, \ldots, c_n \in \mathbb{Z}_4$. Let $c \in \mathbb{Z}_4$ be given by the following linear combination of $c_1, c_2, \ldots, c_n$,*

$$c = a_1c_1 + a_2c_2 + \cdots + a_nc_n,$$

where $a_1, a_2, \ldots, a_n$ are units in $\mathbb{Z}_4$. Let $(x, y), (x_1, y_1), \ldots, (x_n, y_n)$ be the respective Gray map images of $c, c_1, c_2, \ldots, c_n$. Then,

$$x = \sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(k_{i1}x_i + k_{i2}y_i),$$

$$y = \sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(l_{i1}x_i + l_{i2}y_i),$$

where

$$(k_{i1}, k_{i2}) = \begin{cases}(1,0) & \text{if } a_i = 1\\ (0,1) & \text{if } a_i = 3\end{cases}$$

and

$$(l_{i1}, l_{i2}) = \begin{cases}(0,1) & \text{if } a_i = 1\\ (1,0) & \text{if } a_i = 3.\end{cases}$$

Proof. This theorem is proved using induction. As a consequence of Lemma (3) and Corollaries (2) and (3), the result is true when only two terms are added. Let the result be true when p terms are added i.e., the result is assumed to be true for $n \le p$. When $n = p + 1$,

$$c = a_1c_1 + a_2c_2 + \cdots + a_pc_p + a_{p+1}c_{p+1}.$$

Let $z = a_1c_1 + a_2c_2 + \cdots + a_pc_p$ and (x_z, y_z) be the Gray code representation of z. As the result is true when p or fewer terms are added,

$$x_z = \sum_{1\le i<j\le p}(x_i + y_i).(x_j + y_j) + \sum_{i=1}^{p}(k_{i1}x_i + k_{i2}y_i), \tag{3.4}$$

$$y_z = \sum_{1\le i<j\le p}(x_i + y_i).(x_j + y_j) + \sum_{i=1}^{p}(l_{i1}x_i + l_{i2}y_i). \tag{3.5}$$

Therefore,

$$x_z + y_z = \sum_{i=1}^{p}(k_{i1} + l_{i1})x_i + \sum_{i=1}^{p}(k_{i2} + l_{i2})y_i.$$

Observe that $k_{i1} + l_{i1} = k_{i2} + l_{i2} = 1$. Therefore,

$$x_z + y_z = \sum_{i=1}^{p}(x_i + y_i). \tag{3.6}$$

Further, by the assumption of induction, the result is true when two terms are added. Therefore, it

can be applied to the equation $c = z + a_{p+1}c_{p+1}$. Hence,

$$x = (x_z + y_z).(x_{p+1} + y_{p+1}) + x_z + k_{(p+1)1}x_{p+1} + k_{(p+1)2}y_{p+1},$$
$$y = (x_z + y_z).(x_{p+1} + y_{p+1}) + y_z + l_{(p+1)1}x_{p+1} + l_{(p+1)2}y_{p+1}.$$

Substituting the expressions for x_z,y_z and $x_z + y_z$ from Equations (3.4), (3.5) and (3.6) in the above equations, we get the following,

$$\begin{aligned} x &= (\sum_{i=1}^{p}(x_i + y_i)).(x_{p+1} + y_{p+1}) + k_{(p+1)1}x_{p+1} + k_{(p+1)2}y_{p+1} + \sum_{1\le i<j\le p}(x_i + y_i).(x_j + y_j) \\ &\quad + \sum_{i=1}^{p}(k_{i1}x_i + k_{i2}y_i) \\ &= \sum_{1\le i<j\le p+1}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{p+1}(k_{i1}x_i + k_{i2}y_i), \\ y &= (\sum_{i=1}^{p}(x_i + y_i)).(x_{p+1} + y_{p+1}) + l_{(p+1)1}x_{p+1} + l_{(p+1)2}y_{p+1} + \sum_{1\le i<j\le p}(x_i + y_i).(x_j + y_j) \\ &\quad + \sum_{i=1}^{p}(l_{i1}x_i + l_{i2}y_i) \\ &= \sum_{1\le i<j\le p+1}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{p+1}(l_{i1}x_i + l_{i2}y_i). \end{aligned}$$

Thus, the result is true for $n = p + 1$. Hence, the theorem is proved by induction. □

In the following theorem, the above result is extended to the case where some of the summands are non-units.

Theorem 6. *Consider $c_1, c_2, \ldots, c_n, c_{n+1}, \ldots, c_{n+l} \in \mathbb{Z}_4$. Let $c \in \mathbb{Z}_4$ be given by a linear combination of $c_1, c_2, \ldots, c_{n+l}$,*

$$c = a_1c_1 + a_2c_2 + \cdots + a_nc_n + 2c_{n+1} + \cdots + 2c_{n+l},$$

where $a_1, a_2, \ldots, a_n$ are units in $\mathbb{Z}_4$. Let $(x, y), (x_1, y_1), \ldots, (x_{n+l}, y_{n+l})$ be the respective Gray map images of $c, c_1, c_2, \ldots, c_{n+l}$. Then,

$$\begin{aligned} x &= \textstyle\sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(k_{i1}x_i + k_{i2}y_i) + \sum_{i=1}^{l}(x_{n+i} + y_{n+i}), \\ y &= \textstyle\sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(l_{i1}x_i + l_{i2}y_i) + \sum_{i=1}^{l}(x_{n+i} + y_{n+i}), \end{aligned}$$

where

$$(k_{i1}, k_{i2}) = \begin{cases} (1,0) & \text{if } a_i = 1 \\ (0,1) & \text{if } a_i = 3 \end{cases}$$

and

$$(l_{i1}, l_{i2}) = \begin{cases} (0,1) & \text{if } a_i = 1 \\ (1,0) & \text{if } a_i = 3 \end{cases}$$

for $i = 1, 2, \ldots, n$.

Proof. This theorem is proved by induction on l. Let $w = a_1c_1 + a_2c_2 + \cdots + a_nc_n$ and (x_w, y_w) be the Gray map image of w. Therefore, by Theorem (5)

$$x_w = \sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(k_{i1}x_i + k_{i2}y_i),$$
$$y_w = \sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(l_{i1}x_i + l_{i2}y_i).$$

When $l = 1$, $c = w + 2c_{n+1}$. Therefore, by applying Corollary (1), we get the following,

$$\begin{aligned} x &= x_w + x_{n+1} + y_{n+1} \\ &= \sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(k_{i1}x_i + k_{i2}y_i) + x_{n+1} + y_{n+1}, \\ y &= y_w + x_{n+1} + y_{n+1} \\ &= \sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(l_{i1}x_i + l_{i2}y_i) + x_{n+1} + y_{n+1}. \end{aligned}$$

Hence, the theorem holds when $l = 1$. Suppose the theorem holds for $l \le p$. When $l = p + 1$, $c = a_1c_1+a_2c_2+\cdots+a_nc_n+2c_{n+1}+\cdots+2c_{n+p}+2c_{n+p+1}$. Let $z = a_1c_1+a_2c_2+\cdots+a_nc_n+2c_{n+1}+\cdots+2c_{n+p}$ and (x_z, y_z) be the Gray code representation of z. Therefore,

$$\begin{aligned} x_z &= \textstyle\sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(k_{i1}x_i + k_{i2}y_i) + \sum_{i=1}^{p}(x_{n+i} + y_{n+i}), \\ y_z &= \textstyle\sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(l_{i1}x_i + l_{i2}y_i) + \sum_{i=1}^{p}(x_{n+i} + y_{n+i}). \end{aligned}$$

Applying Corollary (1) to the equation $c = z + c_{n+p+1}$ we get the following.

$$\begin{aligned} x &= x_z + x_{n+p+1} + y_{n+p+1} \\ &= \sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(k_{i1}x_i + k_{i2}y_i) + \sum_{i=1}^{p}(x_{n+i} + y_{n+i}) + x_{n+p+1} + y_{n+p+1} \\ &= \sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(k_{i1}x_i + k_{i2}y_i) + \sum_{i=1}^{p+1}(x_{n+i} + y_{n+i}), \\ y &= y_z + x_{n+p+1} + y_{n+p+1} \\ &= \sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(l_{i1}x_i + l_{i2}y_i) + \sum_{i=1}^{p}(x_{n+i} + y_{n+i}) + x_{n+p+1} + y_{n+p+1} \\ &= \sum_{1\le i<j\le n}(x_i + y_i)(x_j + y_j) + \sum_{i=1}^{n}(l_{i1}x_i + l_{i2}y_i) + \sum_{i=1}^{p+1}(x_{n+i} + y_{n+i}). \end{aligned}$$

Hence, the result is true when $l = p + 1$. Thus, the result is proved by induction.

□

Given below are a few basic information theoretic results that help us analyse the secret sharing schemes discussed in the subsequent section.

Lemma 4. *Consider a set of $n+1$ boolean random variables $X_0, X_1, \ldots, X_n$. Let $\mathbf{X} = (X_1, \ldots, X_n)$. Let S be a random variable satisfying the equation $S = X_0 f(\mathbf{X}) + g(\mathbf{X})$ where f and g are functions that map $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The mutual information between S and the random vector $\mathbf{X}$ is given by*

$$I(S;\mathbf{X}) = H(S) - \sum_{\substack{x\in\mathbb{F}_2^n \\ f(x)=1}} p(x)H(X_0/\mathbf{X}=x), \tag{3.7}$$

where, $\mathbb{F}_2^n$ is the collection of binary n-tuples assumed by the random vector X and $p(x)$ is the probability that the value of X is x.

Proof. By the definition of mutual information,

$$I(S;\mathbf{X}) = H(S) - H(S/\mathbf{X}).$$

The second term in the right hand side of the above expression can be expanded as follows,

$$\begin{aligned} H(S/\mathbf{X}) &= \sum_{x\in\mathbb{F}_2^n} p(x)H(S/\mathbf{X}=x) \\ &= \sum_{\substack{x\in\mathbb{F}_2^n \\ f(x)=1}} p(x)H(S/\mathbf{X}=x) + \sum_{\substack{x\in\mathbb{F}_2^n \\ f(x)=0}} p(x)H(S/\mathbf{X}=x). \end{aligned}$$

Now, $H(S/\mathbf{X}=x)$ can be written as follows

$$\begin{aligned} H(S/\mathbf{X}=x) &= H((X_0 f(x) + g(x))/\mathbf{X}=x) \\ &= H(X_0 f(x)/\mathbf{X}=x). \end{aligned}$$

Therefore,

$$H(S/\mathbf{X}=x) = \begin{cases} H(X_0/\mathbf{X}=x) & \text{if } f(x)=1 \\ 0 & \text{if } f(x)=0. \end{cases}$$

Hence proved. □

For the case where the random variables X_0 and X are independent, the above lemma results in the following corollary.

Corollary 4. *If the random variables X_0 and $\mathbf{X}$ in Lemma (4) are independent and the probability that the function f takes value 1 is p, then the mutual information between S and X_0 is given by*

$$I(S;\mathbf{X}) = H(S) - pH(X_0).$$

In addition, if S and X_0 are balanced i.e. the probability of them taking value 1 is 0.5, then

$$I(S;X) = 1 - p.$$

Proof. If $\mathbf{X}$ and X_0 are independent random variables, then $H(X_0/\mathbf{X}=x) = H(X_0)\forall x$. Therefore,

from Equation (3.7)

$$\begin{aligned} I(S;\mathbf{X}) &= H(S) - \sum_{\substack{x\in\mathbb{F}_2^n \\ f(x)=1}} p(x)H(X_0/\mathbf{X}=x) \\ &= H(S) - H(X_0)\sum_{\substack{x\in\mathbb{F}_2^n \\ f(x)=1}} p(x) \\ &= H(S) - pH(X_0). \end{aligned}$$

Now, if S and X_0 are balanced, then $H(S) = H(X_0) = 1$. Hence, $I(S;\mathbf{X}) = 1 - p$. □

Lemma 5. *Consider a set of boolean random variables $X_0, X_1, \ldots, X_n$. Let $\mathbf{X} = (X_1, X_2, \ldots, X_n)$. Let S and S' be random variables satisfying the following linear equations,*

$$\begin{aligned} S &= X_0 f(\mathbf{X}) + g(\mathbf{X}) \\ S' &= (X_0 + 1) f(\mathbf{X}) + g(\mathbf{X}), \end{aligned}$$

where f and g are functions that map $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then,

$$I(S;(S',X_0)) = H(S) - H(f(X)/(S',X_0)).$$

Proof. Subtracting the expression for S' from the expression of S, we get the following;

$$S - S' = -f(\mathbf{X}) \implies S = S' - f(\mathbf{X}).$$

Therefore, $H(S/(S',X_0)) = H(f(\mathbf{X})/(S',X_0)$. Hence, $I(S;(S',X_0)) = H(S) - H(S/(S',X_0)) = H(S) - H(f(\mathbf{X})/(S',X_0))$. □

3.3 Secret Sharing Schemes based on Z_4 Linear Codes

As seen in the previous section, linear equations over $\mathbb{Z}_4$ lead to nonlinear binary equations. Consequently, linear codes over $\mathbb{Z}_4$ can be converted to nonlinear binary codes using the Gray map. In this section, we explore the application of such codes in secret sharing.

A linear code $\mathfrak{C}$ of length $n+1$ over $\mathbb{Z}_4$ can be converted to a binary code $\mathfrak{C}_1$ by replacing each symbol in $\mathbb{Z}_4$ by its image under the Gray map. The length of each such binary codeword is $2n+2$. Removing the first entry of codewords in $\mathfrak{C}_1$ gives rise to a code $\mathfrak{C}_2$ in $\mathbb{F}_2^{2n+1}$. This code can be used for secret sharing by considering the first binary symbol as the secret and the other symbols as shares that are distributed to the participants. The rest of this section analyzes such secret sharing schemes with respect to 'perfectness' and the ability of a participant to cheat. We begin by considering a secret sharing scheme with a singleton access structure.

3.3.1 Secret Sharing Scheme with a Single Element Access Structure

Consider the equation, $c_0 = a_1c_1 + a_2c_2 + \cdots + a_nc_n$ where $c_0, a_1, a_2, \ldots, a_n, c_1, c_2, \ldots, c_n \in \mathbb{Z}_4$. Further, let $a_1, a_2, \ldots, a_n$ be units in $\mathbb{Z}_4$. The set of all $n+1$-tuples $(c_0, c_1, c_2, \ldots, c_n)$ that satisfy this equation constitute a linear code $\mathfrak{C}$ in $\mathbb{Z}_4$. Using the procedure explained above, a binary code $\mathfrak{C}_2$ is generated by replacing the symbols of $\mathfrak{C}$ with their Gray code representations and discarding the first symbol of the resulting code.

Using the code $\mathfrak{C}_2$, a secret bit s can be shared among $2n$ participants by randomly sampling a codeword from the uniform distribution on the set of codewords having first entry s. The other entries of the sampled codeword are distributed among the participants as shares. Let the random variable S denote the secret. Note that the number of codewords in $\mathfrak{C}_2$ with first entry 0 and first entry 1 are equal. Therefore, the uniform distribution of the secret corresponds to a uniform distribution of the codewords of $\mathfrak{C}_2$. This, in turn, corresponds to a uniform distribution of the codewords of $\mathfrak{C}$.

Let the random variables $C_0, C_1, \ldots, C_n$ correspond to the respective entries of codewords in $\mathfrak{C}$. For $1 \leq i \leq n$, let the two tuple X_{i1}, X_{i2} denote the Gray code representation of C_i. As the first entry of codewords in $\mathfrak{C}_2$ corresponds to the secret it is denoted by the random variable S. Thus the values taken by the $2n+1$-tuple of random variables $S, X_{11}, X_{12}, X_{21}, X_{22}, \ldots, X_{n1}, X_{n2}$ correspond to codewords in $\mathfrak{C}_2$. The uniform distribution of the codewords in $\mathfrak{C}$ leads to the following:

- The random variables X_{ij} are i.i.d. with uniform distributions. Therefore, each X_{ij} is statistically independent of the random vector

$$\mathcal{X}_{ij} = (X_{11}, X_{12}, \ldots, \widehat{X_{ij}}, \ldots, X_{n1}, X_{n2}),$$

  where $(X_{11}, X_{12}, \ldots, \widehat{X_{ij}}, \ldots, X_{n1}, X_{n2})$ is the (random)vector obtained after eliminating X_{ij} from $(X_{11}, X_{12}, \ldots, X_{ij}, \ldots, X_{n1}, X_{n2})$. Further, $H(S) = H(X_{ij}) = 1 \; \forall 1 \leq i \leq n$ and $j \in \{1, 2\}$.

- The random variables S and X_{ij} are mutually independent for all $1 \leq i \leq n$ and $j \in \{1, 2\}$.

Further, By Theorem (5), S can be written as a function of $(X_{11}, X_{12}, \ldots, X_{n1}, X_{n2})$ as follows:

$$\begin{aligned} S &= R(X_{11}, X_{12}, \ldots, X_{n1}, X_{n2}) \\ &= \sum_{1 \leq i < j \leq n} (X_{i1} + X_{i2})(X_{j1} + X_{j2}) + \sum_{i=1}^{n} (l_{i1}X_{i1} + l_{i2}X_{i2}), \end{aligned} \tag{3.8}$$

where

$$(l_{i1}, l_{i2}) = \begin{cases} (0,1) & \text{if } a_i = 1 \\ (1,0) & \text{if } a_i = 3. \end{cases}$$

The closeness of this secret sharing scheme to 'perfectness' can be assessed by looking at the amount of information about S that can be extracted from a subset of shares of cardinality $2n-1$. Without loss of generality, $\mathcal{X}_{11}$ can be considered.

Lemma 6. *Consider binary random variables $X_{11}, X_{12}, \ldots, X_{n1}, X_{n2}$ that are i.i.d with uniform distributions. Let $\mathcal{X}_{11} = (\widehat{X_{11}}, X_{12}, \ldots, X_{ij}, \ldots, X_{n1}, X_{n2})$. Let the random variable S be given as*

$$S = \sum_{1 \le i < j \le n} (X_{i1} + X_{i2})(X_{j1} + X_{j2}) + \sum_{i=1}^{n} (l_{i1} X_{i1} + l_{i2} X_{i2}),$$

where (l_{i1}, l_{i2}) is either $(0,1)$ or $(1,0)$.

The mutual information between the random variables S and $\mathcal{X}_{11}$ is 0.5.

Proof. Equation (3.8) can be rewritten as follows.

$$S = X_{11} f(\mathcal{X}_{11}) + g(\mathcal{X}_{11}), \tag{3.9}$$

where

$$\begin{aligned} f(\mathcal{X}_{11}) &= \sum_{j=2}^{n} (X_{j1} + X_{j2}) + l_{11}, \\ g(\mathcal{X}_{11}) &= X_{12}(f(\mathcal{X}_{11}) - l_{11}) + \sum_{2 \le i < j \le n} (X_{i1} + X_{i2})(X_{j1} + X_{j2}) \\ &\quad + \sum_{i=2}^{n} (l_{i1} X_{i1} + l_{i2} X_{i2}) + l_{12} X_{12}. \end{aligned}$$

As X_{ij}s are i.i.d. with uniform distributions, $f(\mathcal{X}_{11})$ is uniformly distributed and independent of X_{11}. Therefore, by Corollary (4)

$$I(S; \mathcal{X}_{11}) = H(S) - 0.5 H(X_{11}).$$

Further, as $H(S) = H(X_{11}) = 1$,

$$I(S; \mathcal{X}_{11}) = 1 - 0.5 = 0.5.$$

□

We claim that, in the above described scheme, a single cheating participant gets no information about the secret in a 'Tompa-Woll' like attack. This claim is proved in the remaining part of this section. Without loss of generality it is assumed that the first participant is the cheater. We start by proving that $f(\mathcal{X}_{11})$ and $g(\mathcal{X}_{11})$ in Equation (3.9) are both independent and uniformly distributed.

Lemma 7. *Consider uniform i.i.d. random variables $C_1, C_2, \ldots, C_n$ that take their values from $\mathbb{Z}_4$. Let C_0 be given by $C_0 = a_1 C_1 + a_2 C_2 + a_3 C_3 + \cdots + a_n C_n$ where $a_1, a_2, \ldots, a_n$ are units in $\mathbb{Z}_4$. For*

$1 \leq i \leq n$, let X_{i1}, X_{i2} be the image of C_i under the Gray map. Let $\mathcal{X}_{11} = (\widehat{X_{11}}, X_{12}, \ldots, X_{n1}, X_{n2})$ and S be the second bit in the Gray map image of C_0. If $S = X_{11}f(\mathcal{X}_{11}) + g(\mathcal{X}_{11})$, then $f(\mathcal{X}_{11})$ and $g(\mathcal{X}_{11})$ are independent and uniformly distributed.

Proof. Consider the equation $C_0 = a_1C_1 + a_2C_2 + a_3C_3 + \cdots + a_nC_n$ where $a_1, a_2, \ldots, a_n$ are units in $\mathbb{Z}_4$. From Equation (3.9),

$$f(\mathcal{X}_{11}) = \sum_{j=2}^{n}(X_{j1} + X_{j2}) + l_{11},$$

$$g(\mathcal{X}_{11}) = X_{12}(f(\mathcal{X}_{11}) - 1) + \sum_{2\leq i<j\leq n}(X_{i1} + X_{i2})(X_{j1} + X_{j2}) + \sum_{i=2}^{n}(l_{i1}X_{i1} + l_{i2}X_{i2}) + l_{12}X_{12},$$

where

$$(l_{i1}, l_{i2}) = \begin{cases} (0,1) & \text{if } a_i = 1 \\ (1,0) & \text{if } a_i = 3 \end{cases}$$

for $i = 1, 2, 3, \ldots, n$.

Let $Z_1 = a_1C_1$ and $Z_2 = a_2C_2 + a_3C_3 + \cdots + a_nC_n$. Z_1 and Z_2 have uniform distributions and are mutually independent. For $i \in \{1, 2\}$, let (Z_{i1}, Z_{i2}) be the Gray code representation of Z_i. By Theorem (5)

$$Z_{21} = \sum_{2\leq i<j\leq n}(X_{i1} + X_{i2})(X_{j1} + X_{j2}) + \sum_{i=2}^{n}(k_{i1}X_{i1} + k_{i2}X_{i2}),$$

$$Z_{22} = \sum_{2\leq i<j\leq n}(X_{i1} + X_{i2})(X_{j1} + X_{j2}) + \sum_{i=2}^{n}(l_{i1}X_{i1} + l_{i2}X_{i2}),$$

where

$$(k_{i1}, k_{i2}) = \begin{cases} (1,0) & \text{if } a_i = 1 \\ (0,1) & \text{if } a_i = 3 \end{cases}$$

for $i = 2, 3, \ldots, n$.

Adding the expressions for Z_{21} and Z_{22}, we get the following

$$\begin{aligned} Z_{21} + Z_{22} &= \sum_{i=2}^{n}((k_{i1} + l_{i1})X_{i1} + (k_{i2} + l_{i2})X_{i2}) \\ &= \sum_{i=2}^{n}(X_{i1} + X_{i2}). \end{aligned}$$

Therefore,

$$\begin{aligned} f(\mathcal{X}_{11}) &= Z_{21} + Z_{22} + l_{11} \text{ and} \\ g(\mathcal{X}_{11}) &= X_{12}(Z_{21} + Z_{22}) + Z_{22} + l_{12}X_{12}. \end{aligned}$$

As Z_{21} and Z_{22} are independent and uniformly distributed, $f(\mathcal{X}_{11})$ is uniformly distributed.

If $X_{12} = 0$, then $g(\mathcal{X}_{11}) = Z_{22}$. In this case, as Z_{21} is uniformly distributed and statistically independent of Z_{22}, $g(\mathcal{X}_{11})$ is uniformly distributed and independent of $f(\mathcal{X}_{11})$.

On the other hand, if $X_{12} = 1$, then $g(\mathcal{X}_{11}) = Z_{21} + l_{12}$. Here, as Z_{21} is uniformly distributed so is $g(\mathcal{X}_{11})$. Further, as Z_{22} is uniformly distributed and independent of Z_{21}, $g(\mathcal{X}_{11})$ is independent of

$f(\mathcal{X}_{11})$.

Thus $g(\mathcal{X}_{11})$ is always uniformly distributed and independent of $f(\mathcal{X}_{11})$. □

Suppose the participant whose share corresponds to the random variable X_{11} decides to launch a 'Tompa-Woll' like attack. Here, the participant changes the value of his/her share before declaring it. Let the recovered secret be denoted by the random variable S'. Therefore,

$$S' = (X_{11} + 1)f(\mathcal{X}_{11}) + g(\mathcal{X}_{11}) = S + f(\mathcal{X}_{11}).$$

In the following theorem, it is shown that by changing his/her share, the first participant gains no information about the actual secret from the erroneously recovered secret

Lemma 8. *Consider random variables $X_{11}, X_{12}, \ldots, X_{n1}, X_{n2}$ that are i.i.d with uniform distributions. Let $\mathcal{X}_{11} = (\widehat{X_{11}}, X_{12}, \ldots, X_{n1}, X_{n2})$. Let S and S' be given by the following equations,*

$$\begin{aligned} S &= X_{11}f(\mathcal{X}_{11}) + g(\mathcal{X}_{11}), \\ S' &= (X_{11} + 1)f(\mathcal{X}_{11}) + g(\mathcal{X}_{11}), \end{aligned}$$

where $f(\mathcal{X}_{11}) = \sum_{j=2}^{n}(X_{j1} + X_{j2}) + l_{11}$ and

$$g(\mathcal{X}_{11}) = X_{12}(f(\mathcal{X}_{11}) - l_{11}) + \sum_{2 \le i < j \le n}(X_{i1} + X_{i2})(X_{j1} + X_{j2}) + \sum_{i=2}^{n}(l_{i1}X_{i1} + l_{i2}X_{i2}) + l_{12}X_{12},$$

where (l_{i1}, l_{i2}) is either $(0,1)$ or $(1,0)$ for $i = 1, 2, 3, \ldots, n$.
Then, the mutual information between S and (S', X_{11}) is 0, i.e. $I(S; (S', X_{11})) = 0$.

Proof. If $X_{11} = 0$, then

$$S' = f(\mathcal{X}_{11}) + g(\mathcal{X}_{11}).$$

By Lemma (7), $g(\mathcal{X}_{11})$ and $f(\mathcal{X}_{11})$ are uniformly distributed and mutually independent. Hence, in this case, S' is uniformly distributed and independent of $f(\mathcal{X}_{11})$.

On the other hand, if $X_{11} = 1$, then $S' = g(\mathcal{X}_{11})$. Hence, S' is uniformly distributed and independent of $f(\mathcal{X}_{11})$.

Thus S' and $f(\mathcal{X}_{11})$ are independent for each value of X_{11}. Consequently,

$$H(f(\mathcal{X}_{11})/(S', X_{11})) = H(f(\mathcal{X}_{11})).$$

Therefore,

$$H(f(\mathcal{X}_{11})/(S', X_{11})) = H(f(\mathcal{X}_{11})) = 1. \tag{3.10}$$

Hence, by Lemma (5),

$$\begin{aligned} I(S; (S', X_{11})) &= H(S) - H(f(\mathcal{X}_{11}/(S', X_{11})) \\ &= H(S) - H(f(\mathcal{X}_{11}) = 0. \end{aligned}$$

By Equation (3.10), $H(S) = H(f(\mathcal{X}_{11})/(S', X_{11})) = H(f(\mathcal{X}_{11})) = 1$. Therefore, $I(S; (S', X_{11})) = 0$. □

The above results can be verified from Truth Tables 2 and 3.

Z_1	Z_2	X_{11}	$f(\mathcal{X}_{11}) = Z_{21} + Z_{22}$	C_0	S	$S' = S + f(\mathcal{X}_{11})$
0	0	0	0	0	0	0
0	1	0	1	1	1	0
0	2	0	0	2	1	1
0	3	0	1	3	0	1
1	0	0	0	1	1	1
1	1	0	1	2	1	0
1	2	0	0	3	0	0
1	3	0	1	0	0	1
2	0	1	0	2	1	1
2	1	1	1	3	0	1
2	2	1	0	0	0	0
2	3	1	1	1	1	0
3	0	1	0	3	0	0
3	1	1	1	0	0	1
3	2	1	0	1	1	1
3	3	1	1	2	1	0

Table 3.1: Truth Table when $a_1 = 1$

The above lemma implies that when a participant declares his/her share wrongly, he/she gets no information about the actual secret from the recovered erroneous one.

However, two participants, whose shares are derived from the same symbol in $\mathfrak{C}$, can collaborate and cheat. Suppose, the participants whose shares correspond to the random variables X_{i1} and X_{i2} both change their shares without informing the other participants, then by Theorem (5) the value of the output will change irrespective of the values of the other shares. Hence, these participants can retrieve the actual secret by flipping the recovered erroneous value.

In the following section, the secret sharing scheme described in this section is extended to one where the access structure has multiple elements.

Z_1	Z_2	X_{11}	$f(\mathcal{X}_{11}) = Z_{21} + Z_{22}$	C_0	S	$S' = S + f(\mathcal{X}_{11})$
0	0	0	0	0	0	0
0	1	0	1	1	1	0
0	2	0	0	2	1	1
0	3	0	1	3	0	1
1	0	1	0	1	1	1
1	1	1	1	2	1	0
1	2	1	0	3	0	0
1	3	1	1	0	0	1
2	0	1	0	2	1	1
2	1	1	1	3	0	1
2	2	1	0	0	0	0
2	3	1	1	1	1	0
3	0	0	0	3	0	0
3	1	0	1	0	0	1
3	2	0	0	1	1	1
3	3	0	1	2	1	0

Table 3.2: Truth Table when $a_1 = 3$

3.3.2 A Secret Sharing Scheme with a Multi-Element Access Structure

Consider the code $\mathfrak{C}$ described in the previous subsection. The random variable C_0 is given by the following linear combination of $C_1, C_2, \ldots, C_n$.

$$C_0 = a_1C_1 + a_2C_2 + \cdots + a_nC_n. \tag{3.11}$$

Extend this code by adding an entry C_{n+1} given by the following linear combination of the existing entries.

$$C_{n+1} = \lambda_1C_1 + \lambda_2C_2 + \cdots + \lambda_nC_n, \tag{3.12}$$

where $\lambda_1, \lambda_2, \ldots, \lambda_{n-1} \in \mathbb{Z}_4$ are non-units and $\lambda_n \in \mathbb{Z}_4$ is a unit. Therefore,

$$C_0 = b_1 C_1 + b_2 C_2 + b_{n-1} C_{n-1} + b_{n+1} C_{n+1}, \tag{3.13}$$

where $b_i = a_i - \lambda_n^{-1} \lambda_i a_n$ for $1 \leq i \leq n-1$ and $b_{n+1} = \lambda_n^{-1} a_n$ As $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ are non-units, all b_is are units in $\mathbb{Z}_4$.

The set of $n+2$-tuples in $\mathbb{Z}_4$ that satisfy Equations (3.11) and (3.13) constitute a linear code $\mathfrak{C}'$ over $\mathbb{Z}_4$. Taking the Gray code representation of each element of codewords in $\mathfrak{C}'$ generates a code $\mathfrak{C}'_1$ over $\mathbb{F}_2$. Eliminating the first entry of codewords in $\mathfrak{C}'_1$ gives rise to a code $\mathfrak{C}'_2$.

As in the previous section, codewords in $\mathfrak{C}'_2$ can be used to share a secret by sampling codewords whose first entry equals the secret and distributing the remaining entries as shares. Again, let X_{i1}, X_{i2} be the Gray code representation of the corresponding C_i. Clearly, the access structure in such a scheme has elements corresponding to the following sets of random variables and their super sets,

$$\mathfrak{S}_1 := (X_{11}, X_{12}, \ldots, X_{n1}, X_{n2}),$$
$$\mathfrak{S}_2 := (X_{11}, X_{12}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{(n+1)1}, X_{(n+1)2}).$$

Observe that the random variables in the first two sets are mutually i.i.d.. Therefore, the corresponding secret recovery functions are similar to those in the previous section. For the first set, the secret recovery function is given by Equation (3.8). For the second set, the secret is recovered by the following equation:

$$\begin{aligned} S \quad &= \textstyle\sum_{1 \leq i \neq n < j \neq n \leq (n+1)} (X_{i1} + X_{i2})(X_{j1} + X_{j2}) \\ &\quad + \textstyle\sum_{1 \leq i \neq n \leq n+1} (r_{i1} X_{i1} + r_{i2} X_{i2}), \end{aligned} \tag{3.14}$$

where

$$(r_{i1}, r_{i2}) = \begin{cases} (0,1) & \text{if } b_i = 1 \\ (1,0) & \text{if } b_i = 3. \end{cases}$$

Using the arguments given in the previous section, it can be shown that the maximum mutual information between any subset of $\mathfrak{S}_1$ or $\mathfrak{S}_2$ and the secret S is 0.5. Further, when the secret is recovered from either $\mathfrak{S}_1$ or $\mathfrak{S}_2$, no lone cheating participant gets any information about the secret in a 'Tompa-Woll' like attack.

It remains to be investigated if there are minimal elements in the access structure other those already described. We claim the set $\mathfrak{S}_1 \cap \mathfrak{S}_2$ is contained in every subset of shares that the secret can be calculated from. In the following theorem, it is proved that X_{11} is contained in all sets of shares corresponding to elements of the access structure. The same can be similarly proved for other elements in $\mathfrak{S}_1 \cap \mathfrak{S}_2$.

Lemma 9. *Consider the ordered sets of binary random variables* $\mathcal{X}_{11}^1 := (\widehat{X_{11}}, X_{12}, \ldots, X_{n1}, X_{n2})$ *and* $\mathcal{X}_{11}^2 := (\widehat{X_{11}}, X_{12}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{(n+1)1}, X_{(n+1)2})$ *such that the random variables in each set are mutually i.i.d. with uniform distributions. Further, let* $\mathcal{X}_{11}^1$ *and* $\mathcal{X}_{11}^2$ *be such that*

$$X_{11} f_1(\mathcal{X}_{11}^1) + g_1(\mathcal{X}_{11}^1) = X_{11} f_2(\mathcal{X}_{11}^2) + g_2(\mathcal{X}_{11}^2) = S, \tag{3.15}$$

where

$$f_1(\mathcal{X}_{11}^1) = \sum_{j=2}^{n} (X_{j1} + X_{j2}),$$

$$g_1(\mathcal{X}_{11}^1) = X_{12} f_1(\mathcal{X}_{11}^1) + \sum_{2 \le i < j \le n} (X_{i1} + X_{i2})(X_{j1} + X_{j2}) + \sum_{i=2}^{n} (l_{i1} X_{i1} + l_{i2} X_{i2}) + l_{12} X_{12},$$

$$f_2(\mathcal{X}_{11}^2) = \sum_{2 \le j \ne n \le n+1} (X_{j1} + X_{j2}),$$

$$g_2(\mathcal{X}_{11}^2) = X_{12} f_2(\mathcal{X}_{11}^2) + \sum_{2 \le i \ne n < j \ne n \le n+1} (X_{i1} + X_{i2})(X_{j1} + X_{j2}) + \sum_{2 \le j \ne n \le n+1} (r_{i1} X_{i1} + r_{i2} X_{i2}) + r_{12} X_{12}.$$

Then, X_{11} *is contained in every ordered subset* $\bar{\mathcal{X}}$ *of* $\mathfrak{S}_3 := (X_{11}, X_{12}, \ldots, X_{n1}, X_{n2}, X_{(n+1)1}, X_{(n+1)2})$ *such that* $S = \mathfrak{H}(\bar{\mathcal{X}})$ *for some function* $\mathfrak{H}$.

Proof. Equation (3.15) can be expressed as the following pair of equations:

$$S = X_{11} f_1(\mathcal{X}_{11}^1) + g_1(\mathcal{X}_{11}^1), \tag{3.16}$$

$$S = X_{11} f_2(\mathcal{X}_{11}^2) + g_2(\mathcal{X}_{11}^2). \tag{3.17}$$

Let $\mathcal{Y}$ and $\bar{\mathcal{Y}}$ denote the ordered sets of variables $(X_{11}, X_{12}, \ldots, X_{n1}, X_{n2}, X_{(n+1)1}, X_{(n+1)2})$ and $(\widehat{X_{11}}, X_{12}, \ldots,$ respectively. If there exists an expression for S without X_{11}, then there exists an algebraic combination of Equations (3.16) and (3.17) which eliminates X_{11} in the RHS and gives S in the LHS. In other words, there exist polynomials $p(\mathcal{Y})$ and $h(\mathcal{Y})$ such that $p(\mathcal{Y}) + h(\mathcal{Y}) = 1$ and $p(\mathcal{Y})(X_{11} f_1(\mathcal{X}_{11}^1) + g_1(\mathcal{X}_{11}^1)) + h(\mathcal{Y})(X_{11} f_2(\mathcal{X}_{11}^2) + g_2(\mathcal{X}_{11}^2))$ is independent of X_{11}. Let $p(\mathcal{Y}) = X_{11} f(\bar{\mathcal{Y}}) + g(\bar{\mathcal{Y}})$. Observe that

$$\begin{aligned} &p(\mathcal{Y})(X_{11} f_1(\mathcal{X}_{11}^1) + g_1(\mathcal{X}_{11}^1)) + (1 + p(\mathcal{Y}))(X_{11} f_2(\mathcal{X}_{11}^2) + g_2(\mathcal{X}_{11}^2)) \\ &= X_{11} f_2(\mathcal{X}_{11}^2) + X_{11}(f(\bar{\mathcal{Y}}) + g(\bar{\mathcal{Y}}))(f_1(\mathcal{X}_{11}^1) + f_2(\mathcal{X}_{11}^2)) \\ &+ X_{11} f(\bar{\mathcal{Y}})(g_1(\mathcal{X}_{11}^1) + g_2(\mathcal{X}_{11}^2)) + k(\bar{\mathcal{Y}}), \end{aligned}$$

where k is polynomial function whose monomials do not contain X_{11}. Therefore, if an expression for

S not containing X_{11} exists, then

$$M = f_2(\mathcal{X}_{11}^2) + (f(\bar{\mathcal{Y}}) + g(\bar{\mathcal{Y}}))(f_1(\mathcal{X}_{11}^1) + f_2(\mathcal{X}_{11}^2)) + f(\bar{\mathcal{Y}})(g_1(\mathcal{X}_{11}^1) + g_2(\mathcal{X}_{11}^2)) = 0. \tag{3.18}$$

Observe that

$$\begin{aligned}
&f_1(\mathcal{X}_{11}^1) + f_2(\mathcal{X}_{11}^2) = X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2},\\
&g_1(\mathcal{X}_{11}^1) + g_2(\mathcal{X}_{11}^2) = X_{12}(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2})\\
&+ \sum_{2\le i\le n-1} (X_{i1} + X_{i2})(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2})\\
&+ \sum_{2\le i\le n-1} ((l_{i1} + r_{i1})X_{i1} + (l_{i2} + r_{i2})X_{i2}) + l_{n1}X_{n1} + l_{n2}X_{n2} + r_{(n+1),1}X_{(n+1)1}\\
&+ r_{(n+1)2}X_{(n+1)2} + (l_{12} + r_{12})X_{12}.
\end{aligned}$$

For M to be uniformly 0, all terms with X_{12} in the expression for M (Equation (3.18))should sum to 0. Hence,

$$f(\bar{\mathcal{Y}})(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2} + l_{12} + r_{12}) = 0.$$

This is possible if and only if $f(\bar{\mathcal{Y}}) = \ell(\bar{\mathcal{Y}})(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2} + l_{12} + r_{12} + 1)$ for some polynomial $\ell(\bar{\mathcal{Y}})$, i.e., $f(\bar{\mathcal{Y}})$ is a multiple of $(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2} + l_{12} + r_{12} + 1)$. Therefore, $f(\bar{\mathcal{Y}})$ is given as follows,

$$f(\bar{\mathcal{Y}}) = \begin{cases} \ell(\bar{\mathcal{Y}})(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2}) \text{ if } l_{12} + r_{12} = 1 \\ \ell(\bar{\mathcal{Y}})(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2} + 1) \text{ if } l_{12} + r_{12} = 0. \end{cases}$$

If $f(\bar{\mathcal{Y}}) = \ell(\bar{\mathcal{Y}})(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2})$, then

$$M = f_2(\mathcal{X}_{11}^2) + R,$$

where

$$\begin{aligned}
R= &(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2})(g(\bar{\mathcal{Y}}) + \ell(\bar{\mathcal{Y}})(1 + \sum_{2\le i\le n-1} ((1 + l_{i1} + r_{i1})X_{i1} + (1 + l_{i2} + r_{i2})X_{i2})\\
&+l_{n1}X_{n1} + l_{n2}X_{n2} + r_{(n+1)1}X_{(n+1)1} + r_{(n+1)2}X_{(n+1)2})).
\end{aligned}$$

Note that every monomial in R has at least one of the variables $(X_{n1}, X_{n2}, X_{(n+1)1}, X_{(n+1)2})$. Therefore, terms in $f_2(\mathcal{X}_{11}^2) = \sum_{2\le j\ne n\le n+1}(X_{j1} + X_{j2})$ that do not have any of these variables cannot be canceled by terms in R. Hence M cannot be 0.

On the other hand if $f(\bar{\mathcal{Y}}) = \ell(\bar{\mathcal{Y}})(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2} + 1)$, then

$$\begin{aligned}
M &= f_2(\mathcal{X}_{11}^2) + (X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2})(g(\bar{\mathcal{Y}}) \\
&+ \ell(\bar{\mathcal{Y}})(\sum_{2\le i\le n-1}((l_{i1} + r_{i1})X_{i1} + (l_{i2} + r_{i2})X_{i2}) + l_{n1}X_{n1} + l_{n2}X_{n2} + r_{(n+1)1}X_{(n+1)1} \\
&+ r_{(n+1)2}X_{(n+1)2})) + \ell(\bar{\mathcal{Y}})(\sum_{2\le i\le n-1}((l_{i1} + r_{i1})X_{i1} + (l_{i2} + r_{i2})X_{i2}) + l_{n1}X_{n1} + l_{n2}X_{n2} \\
&+ r_{(n+1)1}X_{(n+1)1} + r_{(n+1)2}X_{(n+1)2}) \\
&= (X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2})(g(\bar{\mathcal{Y}}) + \ell(\bar{\mathcal{Y}})(\sum_{2\le i\le n-1}((l_{i1} + r_{i1})X_{i1} + (l_{i2} + r_{i2})X_{i2}) \\
&+ l_{n1}X_{n1} + l_{n2}X_{n2} + r_{(n+1)1}X_{(n+1)1} + r_{(n+1)2}X_{(n+1)2})) \\
&+ \sum_{2\le i\le n-1}((1 + \ell(\bar{\mathcal{Y}})(l_{i1} + r_{i1}))X_{i1} + (1 + \ell(\bar{\mathcal{Y}})(l_{i2} + r_{i2}))X_{i2}) + \ell(\bar{\mathcal{Y}})(l_{n1}X_{n1} + l_{n2}X_{n2}) \\
&+ (1 + \ell(\bar{\mathcal{Y}})r_{(n+1)1})X_{(n+1)1} + (1 + \ell(\bar{\mathcal{Y}})r_{(n+1)2})X_{(n+1)2}.
\end{aligned}$$

In the right hand side of the above equation, the expression $\sum_{2\le i\le n-1}((1 + \ell(\bar{\mathcal{Y}})(l_{i1} + r_{i1}))X_{i1} + (1 + \ell(\bar{\mathcal{Y}})(l_{i2} + r_{i2}))X_{i2}) + \ell(\bar{\mathcal{Y}})$ covers all the terms not involving the variables $X_{n1}, X_{n2}, X_{(n+1)1} + X_{(n+1)2}$. For this expression to go to zero, $\ell(\bar{\mathcal{Y}})$ and the $l_{ij} + r_{ij}$s, for $2 \le i \le n-1$ and $j = 1, 2$, must all be equal to 1. When these conditions are satisfied M is given as follows,

$$\begin{aligned}
M = \quad & (X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2})(g(\bar{\mathcal{Y}}) + \textstyle\sum_{2\le i\le n-1}(X_{i1} + X_{i2}) \\
& + l_{n1}X_{n1} + l_{n2}X_{n2} + r_{(n+1)1}X_{(n+1)1} + r_{(n+1)2}X_{(n+1)2}) \\
& + (l_{n1}X_{n1} + l_{n2}X_{n2}) + (1 + r_{(n+1)1})X_{(n+1)1} + (1 + r_{(n+1)2})X_{(n+1)2}.
\end{aligned}$$

Now, the expression $L = l_{n1}X_{n1} + l_{n2}X_{n2} + (1 + r_{(n+1)1})X_{(n+1)1}(1 + r_{(n+1)2})X_{(n+1)2}$ contains only one element from each of the pairs (X_{n1}, X_{n2}) and $(X_{(n+1)1}, X_{(n+1)2})$. As a result, the zero set of L is not contained in the zero set of $(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2})$. Therefore, L cannot be a multiple of $(X_{n1} + X_{n2} + X_{(n+1)1} + X_{(n+1)2})$. Hence, the terms in M involving the variables $(X_{n1}, X_{n2}, X_{(n+1)1}, X_{(n+1)2})$ do not sum to 0. Consequently, M cannot be 0.

As $M \neq 0$, S cannot be expressed in terms of a set of variables not containing X_{11}. □

As a consequence of Lemma 9 every element of the access structure must contain X_{11}. The same can be similarly proved for $X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1),2}$. Thus, every element of the access structure contains the set $(X_{11}, X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1),2})$. Let $\mathfrak{K}$ be the set of js such that the corresponding λ_j in Equation (3.12) is non-zero. Using Theorem (6), $X_{(n+1)1}$ and $X_{(n+1)2}$ can be expressed as follows:

$$X_{(n+1)1} = \begin{cases} X_{n1} + \sum_{j\in\mathfrak{K}}(X_{j1} + X_{j2}) \text{ if } \lambda_n = 1 \\ X_{n2} + \sum_{j\in\mathfrak{K}}(X_{j1} + X_{j2}) \text{ if } \lambda_n = 3, \end{cases}$$

$$X_{(n+1)2} = \begin{cases} X_{n2} + \sum_{j\in\Re}(X_{j1} + X_{j2}) \text{ if } \lambda_n = 1 \\ X_{n1} + \sum_{j\in\Re}(X_{j1} + X_{j2}) \text{ if } \lambda_n = 3. \end{cases}$$

For the rest of the chapter λ_n is assumed to be 1. The results for the case $\lambda_n = 3$ are similar and can be similarly derived. Substituting the expression for $X_{(n+1)2}$ in Equation (3.14), we get the following:

$$\begin{aligned}
S &= \sum_{1\le i<j\le(n-1)} (X_{i1}+X_{i2})(X_{j1}+X_{j2}) + \sum_{1\le i\le(n-1)} (X_{i1}+X_{i2})(X_{(n+1)1}+X_{(n+1)2}) \\
&+ \sum_{1\le i\le n-1} (r_{i1}X_{i1}+r_{i2}X_{i2}) + (r_{(n+1)1}X_{n+11}+r_{(n+1)2}X_{(n+1)2}) \\
&= \sum_{1\le i<j\le(n-1)} (X_{i1}+X_{i2})(X_{j1}+X_{j2}) \\
&+ \sum_{1\le i\le(n-1)} (X_{i1}+X_{i2})(X_{(n+1)1}+X_{n2}+\sum_{j\in\Re}(X_{j1}+X_{j2})) \\
&+ \sum_{1\le i\le n-1} (r_{i1}X_{i1}+r_{i2}X_{i2}) + (r_{(n+1)1}X_{(n+1)1}+r_{(n+1)2}(X_{n2}+\sum_{j\in\Re}(X_{j1}+X_{j2})) \\
&= \sum_{1\le i\ne j\notin\Re\le(n-1)} (X_{i1}+X_{i2})(X_{j1}+X_{j2}) + \sum_{1\le i\le(n-1)} (X_{i1}+X_{i2})(X_{(n+1)1}+X_{n2}) \\
&+ \sum_{1\le i\notin\Re\le n-1} (r_{i1}X_{i1}+r_{i2}X_{i2}) + \sum_{1\le i\in\Re\le n-1} ((1+r_{i1}+r_{(n+1)2})X_{i1} + (1+r_{i2}+r_{(n+1)2})X_{i2}) \\
&+ (r_{(n+1)1}X_{(n+1)1}+r_{(n+1)2}X_{n2}). \qquad (3.19)
\end{aligned}$$

Thus, S can be written as a function of the set of variables $\mathfrak{S}_3 := (X_{11}, X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{(n+1)1}, X_{n2})$. Similarly, by substituting the expression for $X_{(n+1)1}$ in Equation (3.14), it can be shown that S can be written as function of the set of variables $\mathfrak{S}_4 := (X_{11}, X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{n1}, X_{(n+1)2})$.

Let $\mathcal{X}^3_{11} = (\widehat{X_{11}}, X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{(n+1)1}, X_{n2})$. Similar to the secret recovery functions seen earlier in the chapter, Equation (3.19) can be written as $S = X_{11}f_3(\mathcal{X}^3_{11}) + g_3(\mathcal{X}^3_{11})$. Now,

$$\begin{aligned}
f_3(\mathcal{X}^3_{11}) &= f_3(X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{(n+1)1}, X_{n2}) \\
&= f_3(X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{n1} + \sum_{j\in\Re}(X_{j1}+X_{j2}), X_{n2}) \\
&= f_1(X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{n1}, X_{n2})
\end{aligned}$$

and

$$\begin{aligned}
g_3(\mathcal{X}^3_{11}) &= g_3(X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{(n+1)1}, X_{n2}) \\
&= g_3(X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{n1} + \sum_{j\in\Re}(X_{j1}+X_{j2}), X_{n2}) \\
&= g_1(X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{n1}, X_{n2}).
\end{aligned}$$

Thus, the mutual independence of f_1 and g_1 implies the independence of f_3 and g_3. Also the distributions of f_1 and g_1 being uniform imply that the distributions of f_3 and g_3 are uniform. Therefore, along the lines of Lemma (8), it can be shown that, if $S' = (1 + X_{11})f_3(\mathcal{X}_{11}^3) + g_3(\mathcal{X}_{11}^3)$, then $I(S;(S', X_{11})) = 0$. Therefore, a lone cheater cannot launch a 'Tompa-Woll' like attack on the sets $\mathfrak{S}_3$ and $\mathfrak{S}_4$. Further, on the lines of Lemma (6), it can be shown that $I(S, \mathcal{X}_{11}^3) = 0.5$. Thus, the behaviour of these two additional elements of the access structure is identical to $\mathfrak{S}_1$ and $\mathfrak{S}_2$.

Consider the set $\mathfrak{S}_5 := (X_{11}, X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{n1}, X_{(n+1)1})$. Now, $X_{(n+1)1} = X_{n1} + \sum_{j\in\mathfrak{K}}(X_{j1} + X_{j2})$. Therefore, $I(S;\mathfrak{S}_5) = I(S;(X_{11}, X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{n1}))$. Now, by Lemma (6),

$$I(S;(X_{11}, X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{n1})) = 0.5.$$

(Here X_{n2} is excluded from the set $(X_{11}, X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{n1}, X_{n2})$ instead of X_{11}). Hence, the secret cannot be recovered from the set $\mathfrak{S}_5$. Similarly, it can be shown that the secret cannot be recovered from the set $\mathfrak{S}_6 = (X_{11}, X_{12}, X_{21}, X_{22}, \ldots, X_{(n-1)1}, X_{(n-1)2}, X_{n2}, X_{(n+1)2})$. **Hence, $\mathfrak{S}_1, \mathfrak{S}_2, \mathfrak{S}_3$ and $\mathfrak{S}_4$ constitute the minimal elements of the access-structure for this scheme. Alternatively, the access structure consists of these elements and their super sets**.

3.4 Summary

In this chapter, we have analyzed boolean functions arising from linear equations over $\mathbb{Z}_4$. Conditions for their nonlinearity have been stated and proved. Besides, we have also derived explicit expressions for suc4h functions. Further, we have studied the applications of such functions in secret sharing. We have considered a secret sharing scheme with a single-element access structure and have calculated the amount of mutual information between maximal strict subsets of the access structure and the secret. We have shown that while a single participant can't cheat in such schemes, such schemes are vulnerable to attacks by pairs of participants. This scheme has then been extended to a scheme with a multi-element access structure.

4

Future Research Directions with a few Initial Results.

Contents

This chapter looks at a few directions in which this work can be expanded. It explores the following three principal areas of future research,

(i) Studying the relationship between the access structures of nonlinear code based secret sharing schemes and codes that are formally dual to the corresponding nonlinear codes.

(ii) Expanding the results derived for boolean functions obtained from Z_4-linear functions to the boolean functions obtained from Z_{2^k}-linear functions for arbitrary values of k.

(iii) Exploring secret sharing schemes based on nonlinear codes over large finite fields.

4.1 Secret Sharing Scheme from a Nonlinear Code and it's Formal Dual

It is relatively easy to determine the access structure of a secret sharing scheme based on a linear code. Consider an (n, k, d) linear code V over $\mathbb{F}_q$ and define a secret secret sharing scheme based on this code where the first symbol of any codeword is viewed as the secret and the remaining $n-1$ symbols in it are shares given to $n-1$ participants. The access structure of this scheme is specified by those minimal codewords in the dual code $V^{\perp}$ whose first component is one.

For a nonlinear code, however, the notion of dual code is missing. Instead, we say that two codes C and $C^{\perp}$ are formally dual of each other if the Mac-williams transform of the distance distribution of C is equal to the distance distribution of $C^{\perp}$. Note that $C^{\perp}$ need not be unique in the sense that there may exist two distinct codes C_1, C_2 such that both are formally dual of a code C. A code C is said to be formally self-dual if C is a formally dual of itself. It is well-known that Nordstrom-Robinson code $\mathcal{N}_{16}$ is formally self-dual whereas the code $\mathcal{N}'_{15}$ is a formally-dual code of $\mathcal{N}_{15}$.

It has been observed that the access structure of the secret sharing scheme based on $\mathcal{N}_{15}$ is described by the code $\mathcal{N}'_{15}$ as shown in Table (2.7). Likewise, we observe the connection between the access structure of the secret sharing scheme based on $\mathcal{N}_{14}$ and the code $\mathcal{N}'_{14}$ etc. It is important to explore this relationship further and whether we can establish a similar relationship for nonlinear codes as we have for linear codes.

4.2 Nonlinear Secret Sharing based on Z_{2^k} Linear Equations

As we have seen in the previous chapter, linear expressions over Z_4 give rise to quadratic boolean expressions. As an extension, one can look at linear expressions over Z_{2^k} for arbitrary values of k. As

in the previous chapter, the Gray code is used to convert symbols in Z_{2^k} to binary symbols.

Firstly, Lemma (3) in the previous chapter can be extended to Z_{2^k} as follows.

Lemma 10. *Consider $c_1, c_2 \in \mathbb{Z}_{2^k}$. Let $c \in \mathbb{Z}_{2^k}$ be the sum of c_1 and c_2 i.e., $c = c_1 + c_2$. Let $(z_k, z_{k-1}, ...z_1)$, $(x_k, x_{k-1}, ..., x_1)$ and $(y_k, y_{k-1}, ...y_1)$ be the Gray code representations of c, c_1, and c_2 respectively. Then,*

$$z_1 = (x_k + x_{k-1} + \cdots + x_1).(y_k + y_{k-1} + \cdots + y_1) + x_1 + y_1$$

where $'+'$ and $'.'$ indicate addition and multiplication over $\mathbb{F}_2$ respectively.

Proof. The binary representations of c, c_1, and c_2 are $(z_k, z_k+z_{k-1}, ..., \sum_{i=1}^{k} z_i)$, $(x_k, x_k+x_{k-1}, .. \sum_{i=1}^{k} x_i)$ and $(y_k, y_k + y_{k-1}, .. \sum_{i=1}^{k} y_i)$ respectively. As $c = c_1 + c_2$, the last bit in the binary representation of c is got by EX-ORing the last bits of c_1 and c_2. Therefore,

$$\sum_{i=1}^{k} z_i = \sum_{i=1}^{k} x_i + \sum_{i=1}^{k} y_i \tag{4.1}$$

The carry generated by adding $\sum_{i=1}^{k} x_i$ and $\sum_{i=1}^{k} y_i$ is given by $(\sum_{i=1}^{k} x_i)(\sum_{i=1}^{k} y_i)$. Therefore,

$$\sum_{i=2}^{k} z_i = (\sum_{i=1}^{k} x_i).(\sum_{i=1}^{k} y_i) + \sum_{i=2}^{k} x_i + \sum_{i=2}^{k} y_i \tag{4.2}$$

Hence, by adding Equations (4.1) and (4.2) we get,

$$z_1 = (\sum_{i=1}^{k} x_i).(\sum_{i=1}^{k} y_i) + x_1 + y_1 \tag{4.3}$$

□

For a more general expression of the type $c = a_1c_1 + a_2c_2 + \cdots + a_nc_n$, where the a_is are elements of $\mathbb{Z}_{2^k}$, finding expressions for bits in the Gray code representation of c gets a little more complicated due to the propagation of carry. For the case where all the coefficients are 1, we have calculated the Algebraic Normal Form(ANF) expressions for these bits for different values of k. Based on these expressions, we state the following conjecture.

Conjecture 1. *Consider $c_1, c_2, \ldots, c_n \in \mathbb{Z}_{2^k}$. Let $c \in \mathbb{Z}_{2^k}$ be given by the following linear combination of $c_1, c_2, \ldots, c_n$,*

$$c = c_1 + c_2 + \cdots + c_n,$$

Let $(z_k, z_{k-1}, \ldots, z_1), (x_{1k}, x_{1(k-1)}, \ldots, x_{11}), (x_{2k}, x_{2(k-1)}, \ldots, x_{21}), \ldots, (x_{nk}, x_{n(k-1)}, \ldots, x_{n1})$ be the respective Gray map images of $c, c_1, c_2, \ldots, c_n$. Then,

$$z_1 = \sum_{1 \le i < j \le n} (x_{ik} + x_{i(k-1)} + \cdots + x_{i1})(x_{jk} + x_{j(k-1)} + \cdots + x_{j1}) + \sum_{i=1}^{n} (x_{i1}). \tag{4.4}$$

Proving this expression and deriving closed form formulae for boolean expressions corresponding to more general linear expressions expressions over $\mathbb{Z}_{2^k}$ remains an open problem.

As shown in the previous chapter, boolean secret sharing schemes that are derived from linear expressions over $\mathbb{Z}_4$ are susceptible to cheating by two or more participants who cooperate with each other. Now, consider the equation $c = c_1 + c_2 + \cdots + c_n$, where $c, c_1, \ldots, c_n$ are elements of $\mathbb{Z}_{2^k}$. Now, we can construct a scheme similar to the one described in the previous chapter, where the secret corresponds to the LSB in the Gray code representation of c and the shares correspond to the bits in the Gray code representations of $c_1, c_2, \ldots, c_n$. If the above conjecture is true, then the secret recovery function for such a scheme is given by Equation (4.4). Consider any one of the c_is, say c_1. Suppose the participant whose share corresponds to the LSB of the Gray code representation of c_1 decides to cooperate with another participant whose share corresponds to a different bit of c_1. If both these participants flip their shares before declaring, then observe that recovered secret always gets flipped. Thus both these participants can together cheat the scheme. Hence, the problem of two or more participants being able to cheat remains. We believe that this is also true for other linear equations over $\mathbb{Z}_{2^k}$. This remains to be verified.

4.3 Secret Sharing Schemes over Large Finite Fields

Multiplication over the binary field is an extremely unbalanced operation. In three out of four cases the output is zero. This unbalancedness can be a drawback while designing boolean functions tailored for secret sharing. Multiplication over larger finite fields is comparatively more balanced. For example, if we cansider the multiplication of two numbers over $\mathbb{Z}_{31}$, 0 occurs 61 times and every other element occurs 30 times. Thus, if the two multiplicands are sampled from from a uniform distribution, the probability of zero occuring is nearly double that of any other number. More precisely, for a finite field with a prime cardinality q, the probability of zero occuring is $\frac{2q-1}{q^2}$, while the probability of any other number occuring is $\frac{q-1}{q^2}$. The difference between these two number gets progressively smaller as the value of q increases. This motivates the study of secret sharing schemes where the secret and the shares are elements of a large finite field with a prime cardinality. As a starting point, we consider a couple of schemes with single element access structures. The purpose of this exercise is to compare nonlinear functions over large finite fields with boolean nonlinear functions from a secret sharing point of view.

Consider a secret sharing scheme with three participants and a single element access structure. The secret recovery function is given as $S = S_1S_2+S_2S_3+S_3S_1$, where S, S_1, S_2 and S_3 are random variables corresponding to the secret and the three shares that take their values from $\mathbb{F}_q$. Let the entropy of the secret be $H(S)$. We now proceed to show that if S_1, S_2 and S_3 are uniformly distributed and mutually i.i.d., then the distribution of the secret tends to be uniform as q tends to infinity. This is a direct consequence of the following lemma.

Lemma 11. *For the secret sharing scheme described above, if S_1, S_2 and S_3 are i.i.d. and uniformly distributed, the mutual information between the random variable S and the two tuple $\{S_1, S_2\}$ is given by*

$$I(S, \{S_1, S_2\}) = H(S) - (1 - \frac{1}{q})log(q) \tag{4.5}$$

Proof. Observe that the secret recovery function can be written as $S = S_1S_2 + (S_1 + S_2)S_3$.

The mutual information between the random variable S and the two tuple $\{S_1, S_2\}$ is given by

$$\begin{aligned}
I(S; \{S_1, S_2\}) &= H(S) - H(S/\{S_1, S_2\}) \\
&= H(S) - [\sum_{s_1+s_2=0} p(s_1, s_2)H(S/S_1 = s_1, S_2 = s_2) \\
&+ \sum_{s_1+s_2\neq 0} p(s_1, s_2)H(S/S_1 = s_1, S_2 = s_2)] \\
&= H(S) - [0 + \sum_{s_1+s_2\neq 0} p(s_1, s_2)H(S_3)] \\
&= H(S) - log(q)(1 - \frac{q}{q^2}) \\
&= H(S) - log(q)(1 - \frac{1}{q})
\end{aligned}$$

□

As mutual information is always non-negative $H(S) \geq log(q)(1 - \frac{q}{q^2})$. For very high values of q, the right hand side of the above inequality tends to $log(q)$, which is the maximum value that $H(S)$ can take. Further, this maximum value occurs when S is uniformly distributed. Hence for very high values of q, the distribution of S tends to the uniform distribution. Further the mutual information tends to zero as q tends to infinity. Now, if $q = 2$ and the entropy of the secret is 1 bit, the mutual information between S and the two tuple $\{S_1, S_2\}$ is 0.5 which is significant. Thus, while such a scheme is ineffective for binary secrets, it is much more useful over larger finite fields.

We now consider the case where a single participant cheats by modifying her share. Suppose the first participant changes her share by adding a value δ. Her modified share is denoted by the random variable $S_1' = S_1 + \delta$. Observe that the change in the recovered secret is given by the random variable

$\Delta_S = \delta(S_2 + S_3)$. If S_2 and S_3 are uniformly distributed, then the distribution of Δ_S is also uniform. Hence the cheater has no advantage.

However, the above scheme is vulnerable if two of the participants decide to cooperate and cheat. For example, consider the case where the second and third participant decide to declare their share wrongly. If they change their shares by $+\delta$ and $-\delta$, then the change in the recovered secret is given by the random variable $\Delta_S = \delta(S_3 - S_2) - \delta^2$. Since δ and the values of S_2 and S_3 are known to the malicious participants, they can determine the secret from the recovered value.

Now, let us consider another example of a scheme with a single element access structure but with n participants, where n is an even integer. Let the secret recovery function be $S = S_1S_2 + S_3S_4 + \cdots + S_{n-1}S_n$. Note that, for the binary field this corresponds to the Bent function. As in the previous example, for large values of q, if the shares are assumed to be uniformly distributed, the distribution of the secret also tends towards the uniform distribution. This is the consequence of the following lemma which calculates the mutual information between the secret and a set of $n-1$ shares.

Lemma 12. *Consider a secret sharing scheme with a single element access structure having the following secret recovery function*

$$S = S_1S_2 + S_3S_4 + \cdots + S_{n-1}S_n,$$

where S is the random variable corresponding to the secret and $S_1, S_2, \ldots, S_n$ are the random variables corresponding to the shares. In such a scheme, if $S_1, S_2, \ldots, S_{n-1}, S_n$ are mutually i.i.d and uniformly distributed, the mutual information between the random variable S and the $n-1$ tuple $\{S_1, S_2, \ldots, S_{n-1}\}$ is given by

$$I(S, \{S_1, S_2, \ldots, S_{n-1}\}) = H(s) - (1 - \frac{1}{q})log(q) \tag{4.6}$$

Proof. The mutual information between the random variable S and the $n-1$ tuple $\{S_1, S_2, \ldots, S_{n-1}\}$ is given by

$$\begin{aligned}
I(S; \{S_1, S_2, \ldots, S_{n-1}\}) &= H(S) - H(S/\{S_1, S_2, \ldots, S_{n-1}\}) \\
&= H(S) - [\sum_{s_{n-1}=0} p(s_1, s_2, \ldots, s_{n-1}) H(S/S_1 = s_1, S_2 = s_2, \ldots, S_{n-1} = s_{n-1}) \\
&+ \sum_{s_{n-1}\neq 0} p(s_1, s_2, \ldots s_{n-1}) H(S/S_1 = s_1, S_2 = s_2, \ldots S_{n-1} = s_{n-1})] \\
&= H(S) - [0 + \sum_{s_{n-1}\neq 0} p(s_1, s_2, \ldots s_{n-1}) H(S)] \\
&= H(S) - log(q)(1 - \frac{1}{q})
\end{aligned}$$

□

Using exactly the same set of arguments as the previous example, it can be deduced that the distribution of S tends towards uniformity as the value of q increases.

Observe that for every odd positive integer $i < n$, the secret recovery function is affine as a function of the product S_iS_{i+1}. Therefore, if two such participants cooperate, then they can cheat in a manner similar to linear secret sharing schemes. Hence as with the previous scheme, this scheme is also vulnerable to cooperative cheating by two or more participants.

From the above examples, there seems to be a possibility of designing schemes over large finite fields that are 'asymptotically perfect'. Designing such schemes with complex access structures that are resistant to cooperative cheating is an interesting problem to explore and a potential area of future research.

4.4 Some Other Possible Areas

Besides the problems discussed thus far in this chapter, given below are a few areas that could be potentially important from the point of view of nonlinear secret sharing

- Implementation of nonlinear secret sharing schemes on the physical layer.
- The application of nonlinear secret sharing in blockchains.
- The access structures of boolean schemes derived from $\mathbb{Z}_4$-linear functions described in Chapter 3 are extremely limited. Developing such schemes with a complex access structure and designing $\mathbb{Z}_4$-linear codes specifically for secret sharing remains an open problem.

5

Summary of Thesis and Future Study

Contents

5.1 Summary of the Thesis

This work looks at and analyses a few aspects of nonlinear secret sharing. This includes a study of the access structure of such schemes and analyses the utility of such schemes in resisting 'Tompa-Woll'-like attacks wherein malicious participants use any underlying linearity in the secret recovery function to exclusively access the secret. Given below is a point-wise summary of the main results in this thesis.

- Chapter 2 deals with nonlinear secret sharing schemes based on Nordstrom-Robinson and Hadamard codes. It also looks at a few codes that are derived from these. This chapter gives a broad framework for defining the access structure of nonlinear code based secret sharing schemes and defines the access structures of schemes based on Nordstrom-Robisnson code $\mathcal{N}_{16}$ and codes such as $\mathcal{N}_{15}$ $(15, 256, 5)$, $\mathcal{N}'_{15}$ $(15, 128, 6)$, $\mathcal{N}_{14}$, $\mathcal{N}'_{14}$, $\mathcal{N}_{13}$, $\mathcal{N}'_{13}$, $\mathcal{N}_{12}$, $\mathcal{N}'_{12}$ that are derived from $\mathcal{N}_{16}$. Further, the access structures of the schemes based on the Hadamard codes $(11, 12, 6)$, $(11, 24, 5)$ and $(12, 24, 6)$ have also been defined.

- Chapter 3 looks at nonlinear boolean functions from the secret sharing point of view. In particular, boolean functions derived from $\mathbb{Z}_4$-linear functions have been analysed. Closed form expressions for such functions have been derived. Further, we have proved a few information theoritic results that relate these boolean functions to perfectness in secret sharing and resistance to 'Tompa-Woll'-like attacks. Finally, a couple of secret sharing schemes have been derived based on these results. The first scheme has a single element access structure while the second one is a $n-1, n$-threshold scheme. Both these schemes have been analysed from the point of view of perfectness and the ability of participants to cheat. While these schemes are resistant to attacks by single participants, they are vulnerable to cooperative attacks by two or more participants.

- Chapter 4 briefly describes a few areas of future research. These are areas that have been explored during the course of this work but the research could not completed for the want of time. The first such area is the relationship between formal duals of codes and the access structure of the corresponding secret sharing schemes. Such a relationship is observed in chapter 2 in the context of the Nordstrom-Robinson code. It remains an open question if such a relationship generally holds. We have then explored the generalization of nonlinear secret sharing schemes based on $\mathbb{Z}_4$-linear codes to those that are based on $\mathbb{Z}_{2^k}$-linear codes. In this context, we have

stated a conjecture that generalizes the results in Chapter 3 to $\mathbb{Z}_{2^k}$-linear functions. Finally, this chapter looks at nonlinear secret sharing schemes over large finite fields. This is motivated by the potential benefits of the relative 'balancedness' of multiplication over large finite fields. A couple of simple schemes are analysed for resistance to cheating and proximity to perfectness. Developing a general design framework for such schemes and designing nonlinear functions over such fields that are ideal for secret sharing are left as open problems for future work.

Bibliography

[1] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes,," *Communications of the ACM.*, vol. 24, no. 9, pp. 583–584, 1981.

[2] V. Dijk and Marten, "A linear construction of perfect secret sharing schemes," pp. 23–34, 1995.

[3] A.Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[4] G. R. Blakley, "Safeguarding cryptographic keys," pp. 313–318, 1979, "International Workshop on Managing Requirements Knowledge (MARK), New York, NY, USA,".

[5] M. Bertilsson and I. Ingemarsson, "A construction of practical secret sharing schemes using linear block codes," in *AUSCRYPT*, vol. 718, 1992, pp. 67–79.

[6] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, pp. 133–138, 1988.

[7] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," *in Proc. 26th Annu. Symp. Found.Comput. Sci.*, pp. 383–395, 1985.

[8] C. Tang and Y. H. Dingyi Pei1, Zhuojun Liu, "Non-interactive and information-theoretic secure publicly verifiable secret sharing," *Advances in Cryptology*, vol. 576, pp. 129–140, 1991.

[9] M. Cheraghchi, "Nearly optimal robust secret sharing." *IEEE International Symposium on Information Theory*, pp. 2509–2513, 2016.

[10] S. Maitra, "Boolean functions with important cryptographic properties," *Ph.D. Thesis*, 2000.

[11] D.K.Dalai, "On some necessary conditions of boolean functions to resist algebraic attacks," *Ph.D. Thesis*, 2006.

[12] D. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of boolean functions with maximum possible annihilator immunity," *Designs, Codes and Cryptography*, vol. 40, pp. 41–58, 2006.

[13] P. Sarkar and S. Maitra, "Construction of non linear boolean functions with improtant cryptograhic properties," *International Conference on the Theory and Applications of Cryptogrpahic Techniques, Berlin*, pp. 485–506, 2000.

[14] S. Maity and T. Johansson, "Construction of cryptographically important boolean functions." *INDOCRYPT 2002: Third International Conference on Cryptology in India, Hyderabad*, pp. 234–235, 2002.

[15] Z. Jadda and P. Parraud, "$\mathbb{Z}_4$-nonlinearity of a constructed quaternary cryptographic functions class," in *Sequences and Their Applications–SETA 2010: 6th International Conference, Paris, France, September 13-17, 2010. Proceedings 6*. Springer, 2010, pp. 270–283.

[16] D.Agrawal, S.Das, and S.Krishnaswamy, "Secret sharing schemes based on nonlinear codes," *2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 864–867, 2020.

[17] D. Agrawal, "Nonlinear secret sharing scheme based on z_4 linear code," *Globecom workshop*, pp. 608–611, 2022.

[18] D. Agrawal, S. Das, and S.Krishnaswamy, "On secret sharing schemes based on nonlinear codes," in *National Conference on Communications (NCC)*, 2023, pp. 1–6.

[19] F. J. MacWilliams and N. J. A. Sloane, "The theory of error correcting codes," *Elsevier*, 1977.

List of Publications

Journal Publications

1. Deepak Agrawal, Srinivasan Krishnaswamy and Smarajit Das, "On Boolean functions derived from linear maps Over Z_4 and their application to secret sharing", *Designs, Codes and Cryptography*, https://doi.org/10.1007/s10623-024-01478-8.

International Conferences

1. Deepak Agrawal, Smarajit Das and Srinivasan Krishnaswamy, "Secret sharing schemes based on nonlinear codes," *International Symposium on Information Theory*, pp. 864–867, 2020.
2. Deepak Agrawal, "Nonlinear secret sharing scheme based on Z_4 linear code," *Global Communication Workshop*, pp. 608–611, 2022.
3. Deepak Agrawal, "Construction of substitution box from Nordstrom–Robinson code $\mathcal{N}_{16}$," *ICDSA*, vol. 1, pp. 1–9, 2023.

National Conferences

1. Deepak Agrawal, Smarajit Das and Srinivasan Krishnaswamy, "On secret sharing schemes from nonlinear codes," *National Conference on Communication*, pp. 1–6, 2023.