Republic of Iraq

Ministry of Higher Education and Scientific Research

University of Anbar

College of Computer Science and Information Technology

Department of Computer Science

Secret Sharing Key Management Based on Magic Cube

A thesis
Submitted to the Department of Computer Science College of Computer Science and Information Technology-University of Anbar in partial fulfillment of the Requirements for the Degree of Master in Computer Science

By

Rafid Sayhood AbdulAziz

Supervised by

Dr. Ali Makki Sagheer **Dr. Omar Abdulrahman Dawood**

1441 A.H. 2019 A.D.

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

(نَرْفَعُ دَرَجَٰتٍ مَّن نَّشَآءُ ۗ وَفَوْقَ كُلِّ ذِى عِلْمٍ

عَلِيمٌ ﴿٧٦﴾)

صَدَقَ اللَّهُ العَظِيم

سورة يوسف

(من الآيه 76)

Supervisor Certificate

We certify that the preparation of this thesis entitled "***Secret Sharing Key Management Based on Magic Cube***" by "***Rafid Sayhood Abdul-Aziz***" was written under our supervision at the Department of Computer Science – College of Computer Science and Information Technology – University of Anbar, as a partial fulfillment of the requirements for the degree of master in Computer Science.

Signature:
Name: ***Prof. Dr. Ali Makki Sagheer***
Title: ***Supervisor***
Date: /   / 2019

Signature:
Name: ***Dr. Omar Abdulrahman Dawood***
Title: ***Supervisor***
Date: /   / 2019

Linguist Certificate

I certify that, I read this thesis entitled ***(Secret Sharing Key Management Based on Magic Cube)*** and I found it linguistically adequate.

Signature:
Name: ***Dr. Omar Munthir Al-Okashi***
(Linguist Authority)
Date: /   / 2019

Certification of the Examination Committee

We the examination committee certify that we have read this thesis entitled "***Secret Sharing Key Management Based on Magic Cube***" and have examined the student "***Rafid Sayhood Abdul-Aziz***", in its contents and what is related to it, and that in our opinion it is adequate to fulfill the requirement for the degree of ***Master of Science in computer science***.

Signature:
Name: ***Prof. Dr. Ziyad Tariq Mustafa Al-Ta'i*** ***(Chairman)***
Date: / / 2019

Signature:
Name: ***Assist. Prof. Dr. Ali Jbaeer Dawood*** ***(Member)***
Date: / / 2019

Signature:
Name: ***Dr. Foad Salem Mubarek*** ***(Member)***
Date: / / 2019

Signature:
Name: ***Prof. Dr. Ali Makki Sagheer***
Title: ***Supervisor***
Date: / / 2019

Signature:
Name: ***Dr. Omar Abdulrahman Dawood***
Title: ***Supervisor***
Date: / / 2019

Approved by the Dean of the College of Computer Science and Information Technology, University of Anbar.

Signature:
Name: Prof. ***Dr. Belal Al-Khateeb***
Title: Dean of the College
Date: / / 2019

Dedication

I would like to dedicate this work

To

My generous Prophet …

My dear parents and brothers …

My beloved wife and my children …

All my friends …

Rafid Alhadithy

Acknowledgements

First of all, thanks to Allah for His guidance that enables me to complete my research.

In submitting the thesis, I have completed an important part of my life, one in which I had the fortune to interact with several great people, who provided me with knowledge, insight, and perseverance.

I would like to express my appreciation and gratitude to my supervisors Prof. Dr. ***Ali M. Sagheer*** (Dean of al-qalam University College) and Teacher. Dr. ***Omar A. Dawood*** (college of computer science and information technology, University of Anbar) for their continuous support, interest, patience and guidance throughout my Studies.

I would like to present my thanks to Computer Science Department, University of Anbar where I completed my research.

I would like to thank Prof. Dr. ***Ali. O. Mohesen***, Assist. Prof. Dr. ***Refa't S. Abdul-Jabbar***, and Assist. Teacher. ***Montaser. I. Adwan*** (Mathematics department, college of education for pure sciences, university of Anbar), and all my friends for their interest and encouragement and I wish to them very happy life.

Finally, I especially want to thank my parents and my family. Over the years they have continuous to support and motivate me in my studies.

Rafid Alhadithy

Publication Paper	Status
1. **Rafid S. Abdulaziz, Omar A. Dawood and Ali M. Sagheer** *“Developing a Secret Sharing Scheme Depending on Magic Cube and Linear Lagrange Interpolation Mathematical Basis”.*	**Published in REVISTA - AUS Journal, Scopus Q4.**
2. **Rafid S. Abdulaziz, Ali M. Sagheer and Omar A. Dawood** *“Conditional Secure Reconstruction of Embedded Secret Approach in Folded Magic Cube with Six Dimensions”.*	**Published in REVISTA - AUS Journal, Scopus Q4.**

Abstract

The protection of secret and sensitive data shared through internet network is one of the most important issues that faces internet users. Despite the advance technology emerged lots of solutions to secure secret data sharing, but still the data sharing matter through an open environment is the main challenge. The sharing secret methods play great role in the key management strategy for the sensitive data and the cryptographic keys in terms of generation, exchange and managing in a secure method. The secret sharing scheme built based on proven mathematical concepts that allows the dealer to distribute the secret keys among several participants securely. In this thesis four new mathematical algorithms were proposed which completely based on the magic cube's principles and the Lagrange mathematical background. The first algorithm relied on generation an odd order folded magic cube that exploits the pivot element of the first magic square in magic cube to be the secret and then embedded in polynomial equation. The pivot element will support in transfer the magic cube properties to the participants to be able to reconstruct the original magic cube again. The Hermite interpolation mathematical method was used in the second algorithm which considers more complex than the Lagrange interpolation method. Because, it depends on the derivative of polynomial and Lagrange derivative in the process of constructing and reconstruction the secret by the dealer and the participants. The third algorithm assumes that the dimension order (N) of the magic cube is the secret key that will be embedded within the polynomial equation and sent to the trusted subscribers. The participants will be able to get the secret (cube dimensions) after using the Lagrange interpolation. The algorithm requires finding the start number and the difference value between the magic cube elements to reconstruct it again. The third algorithm can work with different types of magic cubes of (odd order, singly or doubly even order). The fourth proposed algorithm is newton's divided difference numerical analysis mathematical method. The newton interpolation was applied on the second polynomial algorithm and showed good results compared with its predecessor in the process of protecting the secret keys. The process of integrating the secret sharing methods with the mathematical characteristics of magic cubes gave a great flexibility in dealing with different numerical analysis methods. The proposed secret sharing methods have been tested and measured according to some important metrics like the elapsed time and the computational complexity factor. The implemented tests indicated a reasonable and accepted results for the secret computation. All adopted numerical analysis methods provided good results during the process of sharing the secret and gave the necessary protection in trusting the sensitive information. The proposed methods produced distinct results and put the users in front of multi-options in choosing the appropriate way to transfer their confidential and sensitive information to the trusted subscribers in order to protect them from theft, loss or the risk of cryptanalysis. The proposed methods were programmed by Visual Studio 2016 C# programming language under Windows-10 Ultimate version of 64-bit operating system using processor core (TM) i7-77HQ CPU @ 2.80 GHz, Ram 16.0 GB, HD 1TB, and 4GB VGA.

Key Words: *Secret Sharing, Magic Cube, Magic Square, Key Management Protocol, Lagrange Interpolation, Threshold Encryption, Shamir's Secret Sharing, Secure Computation, Conditional Secure Secret, Secret Reconstruction Schemes.*

List of Abbreviations

Abbreviation	Explanation
A-SSS	Asymmetric Secret Sharing Scheme
DLP	Discrete Logarithm Problem
Fact	Factorial
IFP	Integer Factorization Problem
KG	Key Generation
$L_{n, j}$	Degree of the Polynomial
Log	Logarithm
M.C	Magic Constant
M.S	Magic Sum
Mod	Modulo (reminder of division)
MCDB	Multi – Cloud Data Bases
Pow	Power
P-SSS	Proactive Secret Sharing Scheme
RGB	Red, Green and Blue
SS	Secret Sharing
SSS	Secret sharing Scheme
SSSS	Shamir's Secret Sharing Scheme
X_i	Variable

List of Algorithms

Algorithm No.	Title	Page No.
3.1	First Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)	40
3.2	Second Proposed Algorithm (Secret Sharing with Magic Cube using Hermite Interpolation)	46
3.3	Third Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)	53
3.4	Fourth Proposed Algorithm (Secret Sharing with Magic Cube using Newton Divided Difference Interpolation)	60

List of Figures

Figure No.	Title	Page No.
2.1	Secret Sharing Scenario	11
2.2	Polynomial Interpolation Q(x) to Appreciation values Between x_0, x_1, and x_2	20
2.3	Third-Order Magic Square	23
2.4	Three of Magic Square with Different Pivot Element	24
2.5	Odd Order Magic Square (De la Loubère’s Methods)	26
2.6	The Complete Square of De la Loubère’s Method	26
2.7	De la Loubère’s Square	27
2.8	Stairstep Method	28
2.9	Third-Order Magic Square	28
2.10	Staircase Before “infolding”	28
2.11	Final form of 5 * 5 Stair Step Magic Square	29

2.12	Strachey’s Method	29
2.13	Singly Even Strachey’s Method	30
2.14	Ralph Strachey’s Method Before Swapping	31
2.15	Ralph Strachey’s Method After Swapping	31
2.16	Doubly Even Durer's Method	32
2.17	Magic Cube	33
2.18	Magic Cube of Order 3	34
2.19	Magic Cube of Three Layers	34
2.20	Six Faces of Folding Magic Cube	35
2.21	The Magic Constant of the Six Squares	36
2.22	The Magic Sum of the Six Squares	36
2.23	Eleven Distinct Shapes for the Magic Cubes	37
3.1	Odd Order Magic Cube with Six Dimensions	41
3.2	The Reconstruction of Original Odd Order Magic Cube	43
3.3	First Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)	44
3.4	The Odd Order Magic cube of 5*5 Dimension	47
3.5	The Reconstruction of 5*5 Odd Order Magic Cube	50
3.6	Second Proposed Algorithm (Secret Sharing with Magic Cube using Hermite Interpolation)	51
3.7	Doubly Even Magic Cube	55
3.8	The Reconstructed Magic Cube	57
3.9	Third Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)	58
3.10	Singly Even Magic Cube	62

3.11	The Reconstructed Singly Even Magic Cube	64
3.12	Fourth Proposed Algorithm (Secret Sharing with Magic Cube using Newton Divided Difference Interpolation)	65
4.1	Secret Sharing with Magic Cube algorithms (Building the Secret Keys)	68
4.2	Secret Sharing with Magic Cube algorithms (Rebuilding the Secret Keys)	68
4.3	Comparison of Key Space for (x) Values Mod Prime	80
4.4	Comparison of Key Space for (x) Values Mod Prime	81
4.5	Comparison of Key Space for (x) Values Mod Prime	82

List of Tables

Table No.	Title	Page No.
3.1	Generated Points of 1st Algorithm According to (*x*) And (*f* (*x*)) axes	42
3.2	Generated Points of 2nd Algorithm According to (*x*) And (*f* (*x*)) axes	48
3.3	Generated Points of 3rd Algorithm According to (*x*) And (*f* (*x*)) axes	55
3.4	Generated Points of 4th Algorithm According to (*x*) And (*f* (*x*)) axes	62
3.5	Comparison among the Proposed Algorithms According to (Secret Sharing and Magic Cube Properties)	66
4.1	A Comparison of the Strength and Complexity Analysis of the Implemented Algorithms with Shamir's model	74
4.2	Selected Values Where the (x = 1, 2, 3)	80
4.3	Selected Values Where the (x = 4, 5, 6)	80
4.4	Selected Values where the (x = 2, 4, 6)	81
4.5	Elapsed Time According to (x) Values	83
4.6	Elapsed Time According to (x) Values	83
4.7	Elapsed Time According to (x) Values	83
4.8	Elapsed Time According to (x) Values	83

Table of Contents

Caption	Page No.
Abstract	IX
List of Abbreviations	XI
List of Algorithms	XII
List of Figures	XII
List of Tables	XV
Table of Contents	XVI
Chapter One **General Introduction**	
1.1 Overview	1
1.2 Related Works	2
1.2.1 Related Works about Secret Sharing	2
1.2.2 Related Works about Magic Square	4
1.2.3 Related Works about Magic Cube	5
1.3 Problem Statement	7
1.4 The Aim of Thesis	7
1.5 The main Contribution	8
1.6 Thesis Outline	8
Chapter Two	

Theoretical Background

2.1 Introduction	**10**
2.2 Shamir’s Secret Sharing Scheme	**11**
2.3 Blakley’s Secret Sharing Scheme	**12**
2.4 Threshold Secret Sharing Schemes	**12**
2.5 Shamir’s Threshold Secret Sharing Scheme	**15**
2.6 Adversary Model	**17**
2.7 Some Attacks on Shamir’s Secret Sharing Scheme	**18**
2.8 Mathematical Preliminaries of Numerical Analysis Definition	**19**
2.8.1 Lagrange Interpolation Concept	**19**
2.8.2 Hermite Interpolation Concept	**20**
2.8.3 Newton’s Divided Difference Interpolation Formula	**21**
2.9 Evolution of Magic Square	**22**
2.10 Principles of Magic Square	**22**
2.11 Magic Square Construction	**25**
2.11.1 Magic Squares of Odd Order	**25**
2.11.2 Magic Squares of a Singly Even Order	**29**
2.11.3 Magic Squares of a Doubly Even Order	**31**
2.12 Some Significant Properties of Magic Squares	**32**
2.13 Introduction to Magic Cube	**33**

2.14 The Construction of a Magic Cube	35
2.15 Applications of Magic Cube	37
Chapter Three **Design and Implementation of the Proposed Secret Sharing Algorithms**	
3.1 Introduction	38
3.2 First Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)	38
3.3 Second Proposed Algorithm (Secret Sharing with Magic Cube using Hermite Interpolation)	45
3.4 Third Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)	52
3.5 Fourth Proposed Algorithm (Secret Sharing with Magic Cube using Newton Divided Difference Interpolation)	59
Chapter Four **Results and Analysis**	
4.1 Introduction	67
4.2 Graphical User Interface (GUI)	67
4.3 The Analysis of Interpolation Methods	69
4.4 Security Analysis for the Implemented Secret Sharing Algorithms	70
4.4.1 The Security Analysis of the First Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)	70

4.4.2 The Security Analysis of the Second Algorithm (Secret Sharing with Magic Cube using Hermite Interpolation)	**71**
4.4.3 The Security Analysis of the Third Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)	**72**
4.4.4 The Security Analysis of the Fourth Algorithm (Secret Sharing with Magic Cube using Newton Divided Difference Interpolation)	**73**
4.5 Investigation and Analysis about Prime Number Affect	**76**
4.6 The Comparison of Implemented Algorithms According to Prime Number usage	**79**
4.7 Comparison of Elapsed Times to Reconstruct the Implemented Algorithms	**82**
4.8 Pros and Cons of the Implemented Secret Sharing Algorithms	**84**
4.8.1 The Pros of the Implemented Algorithms	**84**
4.8.2 The Cons of the Implemented Algorithms	**84**
4.9 Applications of the Implemented Secret Sharing Algorithms	**85**
Chapter Five **Conclusions and Suggestions for Future Works**	
5.1 Introduction	**87**
5.2 Conclusions	**87**
5.3 Suggestions for Future Works	**88**
References	**90**

Chapter One
General Introduction

Chapter One
General Introduction

1.1 Overview

The advanced technology in the digital world creates a large volume of the daily information exchanged within an open environment. This information may contain some sensitive data likewise: secret passwords, credential data, personal secret information, high importance information, institutional secret data records and so on. The secret sharing dilemma becomes a necessary demand for all sectors to prevent the modern approaches in the cryptanalysis attacks. Furthermore, when trusting single authority becomes unacceptable, the secret sharing and the threshold encryption will be a good choice. Numerous security systems protocols were proposed to satisfy the current needs for different applications[1]. There is an urgent need to safely store much secret information in order to avoid information theft, information leakage and information loss. The schemes of secret sharing are known as a process of distributing and managing the secret information among multi-parties securely. Therefore, the smaller subset parities which are less than the threshold number will be unable to retrieve the secret unless they satisfy the computational conditions. In 1979, Blakley[2] and Shamir[3] freely presented the main idea of a (*k*, *n*) threshold secret sharing scheme. They submitted a novel scheme with an interesting idea that involves sharing the secret key with different parties. The retrieving of secret key will require multi-party computations for trusted subsets of parties according to the specific threshold. Thus, the secret key can be regained with any *k* out of *n* shares. However, it cannot be gotten back with every group other than *k* shares. Moreover, any information about the secret cannot be acquired with every group of other than (*k*- participants). Accordingly, the original secret will be protected in spite of information shares leakage. In addition, those shares can be regained even if some of them are lost[4] .

A magic square is a matrix square sketched as a checkerboard. This is filled with the numbers or alphabets in unique patterns. The arithmetic squares which are mostly interesting for mathematicians, consist of N^2 boxes, called cells, with different integers. This square is called magic if the sum numbers are equal horizontally, vertically and diagonally. The square is said to be as *n*Th order when the integers are consecutive numbers from 1 to N^2. The square is called *n*Th order, magic number, or the sum of every row is symbolized as *S* continually (the magic constant)[5, 6].

The magic cube is similar to the magic square in the feature of probability construction which expands significantly with dimension order. The bigger dimension will require a higher probability for searching space in guessing and estimation. Within the diagonal cube, the starting element starts from one corner which covers the upper layer dimensions to the lower left corner. This element represents the smallest normal magic cube of (3*3*3) dimensions with sequential numbers from 1 to 27. These numbers are organized in such a way that every three layers are composed of nine numbers. However, the (Magic Constant) for this magic cube is sum to 42. These layers are arranged magically to express the dimension or face for the (Magic Cube).

The magic cubes are higher than playing games with similar numbers of the chessboard or Rubik cube. They are considerably relied on mathematical rules in their building, They are represented in a number of mathematical domains such as the number theory, matrices and combinatory etc [7].

1.2 Related Works

There are many previously mentioned works and ideas relating to the subject matter of this thesis, Therefore, these contributions will be clarified in three parts, including the secret sharing, the magic square and the magic cube.

1.2.1 Related Works about Secret Sharing

Secret sharing is one of the most important key management protocols developed over the years. Researchers have developed secret sharing to be used in many areas of their own. Some works will be mentioned in this section.

Vyas, in 2015 [8] pointed out protect sensitive information can be achieved by developing an algorithm to share and use secret sharing technique securely. This technique begins with a secret, then, particular secrets are derived from it to be distributed securely among the users. This method can be employed in an environment where the system is open to all users who have individual passwords. Accordingly, the findings of the experiment and verification proved that the results of the algorithm are satisfactory.

Pundkar & Shekokar, in 2016 [9] have introduced a new method using Shamir’s secret sharing for images and videos in MCDB. The multimedia is protected in the multi-cloud database by Shamir’s secret sharing. In essence, companies provide personal data and information that may be sensitive and secret to the provider of the service. By using secret sharing schemes, data integrity can be secured. Compared to a single cloud security and cloud storage, multi-cloud systems have significantly reduce the protection risk. In this respect, they optimize scalability and performance. Thus, data integrity and confidentiality in multi-cloud systems are enhanced by using Shamir's secret sharing scheme.

Muthukumar & Nandhini, in 2016 [10] proposed the execution of two algorithms by comparing a secret sharing algorithm and information transmission algorithm; then the secret sharing algorithm was modified to propose a scheme for sharing medical data. The compared algorithms were deployed for securing medical data transfer in a cloud environment while their respective drawbacks were evaluated with different difficulties. The proposed modified secret sharing algorithm was put forward to solve the problems of the existing algorithms. This algorithm facilitated a secured distribution of medical data based on clients’ data request. This scheme addressed the existing challenges and can be deployed for dynamic database without having any impact on the users. The scheme is suited for highly sensitive data distribution in a multi-cloud environment; however, it is recommended to enhance the systems’ performance and increase its flexibility.

Kaneko & Iwamura, in 2017 [11] suggested two Proactive Secret Sharing Schemes (P-SSSs) which are fit for an A-SSS. The study proved the capability of the schemes to substantially reduce communication compared to the traditional P-SSS. They further suggested three P-SSSs with varying features; where the 1st and 2nd schemes were ideal for A-SSS and ensured a reduced level of communication compared to Herzberg’s scheme. The 2nd scheme particularly ensured the same level of security as obtainable with Herzberg’s scheme. The 3rd scheme reinforced the security of Herzberg’s scheme by including the verification protocol for updated shares. Meanwhile, it uses the discrete algorithm, hence, it is not effective.

1.2.2 Related Works about Magic Square

The use of magic squares in the protection of confidential information is still evolving. Because Magic Squares are used as an additional security layer in some algorithms to protect sensitive information, some related works will be mentioned.

Tomba, in 2012 [6] suggested a method for the use of the basic Latin square to construct (n x n) magic squares (where *n* = doubly even). To construct doubly even magic squares, the column related with the elements is fixed next to the pivot element, followed by the arrangement in a logical manner to generate a magic parametric constant T (known as Tomba's constant) and sub-magic parametric constants (Ti). Lastly, the magic squares are derived by slightly adjusting the values of Ti. The magic squares generated by this technique are weak and for singly even cases. The construction process is demonstrated with appropriate illustrations. The technique is suitable for finding magic squares from basic Latin Squares of any order (n ≥ 1, for *n,* is doubly even). The process of this construction involves fixing the column related to the adjacent elements to the pivot element and assigning it as a diagonal element. The other elements are arranged orderly with slight alterations on the elements that correspond to the magic parametric and sub parametric constants.

Kheiri & Özcan, in 2013 [12] proposed a system for the construction of the constrained type of magic squares. The system consists of a set of effective selection hyper-heuristics and perturbative low-level heuristics. This system combined different hyper-heuristics with different selection methods. The move acceptance methods were used in the system as the search method to resolve the constraint magic square problem. Contrary to the preceding hyper-heuristics-related studies, the hyper-heuristic performance in this study was measured based on its execution time rather than the problem-specific solution quality. However, the outcome of the study confirmed the previous submissions by showing that even the non-learning selection hyper-heuristics can outperform the best-known heuristic solution on the average.

Farhan et al., in 2018 [13] have presented a new method of encrypting color digital images using magic square. The proposed method generates an encryption key by using magic square and encrypts images using the generated key. The encryption method changes the RGB (Red, Green, and Blue) values of each pixel of the plain-text image using the generated key. The process starts by splitting the plain-text image into three arrays that hold RGB values. After encrypting each segment of 256 pixels of the RGB arrays, the encrypting key is permuted by using magic square. At the end, the encrypted image is generated by merging all three encrypted RGB arrays together. For the decryption of the cipher-image, the same process of encryption used but with the encrypted images as the input. The aim of this study is to generate a strong encryption key and use it to encrypt digital color images using a proposed symmetric cipher. The results of encrypting and decrypting images using the proposed encrypting method show that cipher-text image has a significant distribution of RGB components compared with the plain-text image regardless the encrypting process when the size of plain-text is very large.

1.2.3 Related Works about Magic Cube

Many researchers have invented many works that belong to magic squares and magic cubes in various fields. Some related works will be mentioned.

Jamel et al., in 2010 [14] have suggested a modern cryptographic algorithm which depends on the mixtures of hybrid magic cubes produced from two orthogonal Latin squares and a magic square. The produced cipher texts lack any predicted model which might be used to decode the initial message if using randomly two functions, i.e, choice of thirteen magic cubes and key choice from layers of hybrid. In such mathematical application, the data structure is built from hybrid layers while its related inverses become the encryption and decryption keys. These two random functions were presented to ensure that all the potential models which can be deployed by a cryptanalyst to solve the initial message are avoided. The outcome of this work can be further applied for the development of hybrid cubes of order 8, 16, 32 and 64 depending on a combination of "magic cubes" order 4 which can produce the base for the modern cryptographic algorithm with multiple matric sizes.

Feng et al., in 2011 [15] developed an improved Rubik's cube rotation and logistic sequence-based image scrambling algorithm which generates cubes by resizing the original image and partitioning the resized images into 6 blocks. These cubes are rotated in 25 steps using 30 different rotating approaches which are guided by a chaotic system. These cubes are remapped after rotation to a chaotic image before using a Chebyshev chaotic system to produce the rotating methods for further scrambling of the chaotic image to achieve better results. Being that the rotation methods are completely produced by the chaotic system, it is not possible to retrieve the encrypted image unless the arguments of the chaotic system are the same. This algorithm provided a better scrambling degree compared to Arnold transform-based algorithm and Rubik's cube rotation-based algorithm. The system also achieved better logistic sequence and less correlation between adjacent pixels. It also has a relatively large key space and highly sensitive to the keys.

Dawood et al., in 2015 [16] have proposed a distinct modern asymmetric (public key) frameworks that depend on the Diffie-hellman key exchange protocol and the magic square and cubes mathematical principles. These principles are employed as a substitute for the conventional Discrete Logarithm Problem (DLP) and the Integer Factorization problems (IFP). The suggested idea just employs the Diffie-hellman matrix to decide the constructive of magic cubes dimension through which the kind of magic square is determined in the construction method. In addition, the starting number, the difference value and the number of face or dimension that will produce the ciphering key to both exchanged parties will be designated. So, the suggested model is insightful and effective at different levels. Firstly, it introduces a smart way to design particular processes that make it easier for the new mathematical understanding to be related to the possibility of dimension for the construction of the magic square and cube. This may be attributed to the complexity and the magic cube space which increases significantly with the increasing dimension. The pivotal mathematical problem of a magic cube has been manipulated to play an important role in signing/verifying and encryption/decryption processes in two different ways. It provides a prominent and important speed. Moreover, it reduces costs and improves efficiency and security margin.

Dawood et al., in 2016 [17] have proposed the folded magic square technique which is a new method for building magic cubes. This method generalizes the magic cube design with any order despite the magic square type (either odd singly or doubly even order). This method is quite simple as it depends fundamentally on the construction of magic square methods. In this sense, a designer needs to construct six magic squares successively or with any different number pairs in the square matrix. These magic squares individually represent the surface of the cube or the magic dimensions. To maintain the magic cube features, each square should be arranged in the correct order (such that the sum of the rows, columns, and diagonals in any direction is the same) to form the regular cube.

1.3 Problem Statement

Several methods and algorithms have been emerged to trust the secret key management scheme. These methods are concerned with distribution the parts of the secret key to group of participants securely. Each of these existing methods has its own limitations and benefits that protects the secret information in different mathematical ways. Providing protection for secret data can be very difficult challenge which faced by big companies. In this thesis new approaches of secret sharing methods have been developed based on some new mathematical ideas. The proposed methods provide ideal solution for the keys management mechanism of sharing the secret. The sharing process allows distributing certain secret data among several authorized persons securely according to concrete mathematical computation.

1.4 The Aim of Thesis

This thesis aims to suggest new secret sharing schemes using the Lagrange secret sharing and magic cubes notations for the purpose of maintaining the keys management steps among dealer and the trusted subscribers. The core aim of the presented thesis is to apply a real security solution of key management process between the transmitter and the receivers' parties. The essence of the study is to give the users multiple options with different polynomial sharing methods to exchange the secret in a secure way completely. The exchange process depends on proved mathematical methods that do not allow any information leakage through reconstruction the secret between the dealer and the participants.

1.5 The Main Contribution

The main contribution involves suggestion four secret sharing algorithms that are used to trust the transmitted sensitive information over the network. The most important contributions made in this thesis can be summarized in the following:

The present algorithms proposed to integrate the mathematical characteristics of the magic cubes with the secret sharing scheme to secure the exchange for the secret and sensitive keys between the dealer and the trusted subscribers. The secure key management has adopted multiple methods of mathematical numerical analysis (Lagrange, Hermite and divided difference interpolation) for the purpose of providing maximum protection for the secret key. The effectiveness and compatibility of all methods of numerical analysis proposed in the protection of cryptographic keys have been demonstrated and performed in the same way as the Shamir secret sharing (*k*, *n*) Threshold. The mathematical properties of the magic cubes have proven high computational complexity in protection the secret keys transferred between the participants, especially when combined with the secret sharing scheme to reduce the cheating rate (Send Wrong Shadows) that may appear on both ends (dealer or subscribers). In addition to, distributing of unlimited numbers of confidential information via the properties of magic cubes. Because, the mathematical characteristics possessed by these cubes enable to transmit large secrets through transmitting process. Unlike the Shamir secret sharing scheme through which only one key can be transferred to all reliable subscribers.

1.6 Thesis Outline

The present thesis is organized in five chapters. In addition to this chapter, the overview of the other chapters is briefly illustrated as follows:

Chapter Two is entitled by "Theoretical Background"

It discusses the theoretical Background of the thesis. The theoretical Background include covering the basics of secret sharing schemes, magic squares and magic cubes principles. Secret sharing schemes are explained through: Shamir’s secret sharing scheme and Blackley secret sharing scheme. The magic squares construction types (odd order, singly and doubly even order) and the construction of magic cubes by (folded magic squares).

Chapter Three is entitled "Design and Implementation of the Proposed Secret Sharing Algorithms"

It presents the design and implement of "secret sharing with magic cubes" techniques. The design of each technique is started with an overview and followed by the details of the design stages and ended with important algorithms.

Chapter Four is entitled "Results and Analysis"

It presents the results and analysis of the implemented techniques. The implementation is shown through figures and the implementation includes the experimental results and security analysis.

Chapter Five is entitled "Conclusions and Suggestion for Future Works"

It presents the conclusions and suggestions for future works.

Chapter Two

Theoretical Background

Chapter Two
Theoretical Background

2.1 Introduction

The access operation to the important information in open environment must be restricted and under control. The authorized access can be achieved by cryptographic secret identifier that permits the reaching to the private information. Most modern cryptographic management systems manage the secret keys in a flexible form and high secure level. The main challenge is how to distribute the secret key among number of shareholders securely[18]. The Secret Sharing (*SS*) scheme is a protocol through which the secret information is distributed by a dealer to a number of (*n*) shareholders. The reconstruction of secret key can be implemented via group of participants according to threshold secret sharing. The threshold secret scheme determines the allowed number of participants for retrieving the secret key. The threshold (*n*, *t*) scenario refers to n participants with t or more subscribers can retrieve the secret properly, as shown in figure (2.1). Shamir's [19] and Blakely [2] independently proposed the first Secret Sharing Scheme (*SSS*) threshold that distributes the secret parts to several parities and then reconstruct it easily. These schemes are fully secure, which means there is no leakage information and the unauthorized group cannot find information about the secret. Shamir's secret sharing threshold was widely researched and investigated deeply by the researchers with different categories of secret sharing schemes[20].

The authenticated dealer provides separate secret fragments to a number of participants in regarding to the planned threshold. A minimum of (*t*) or more participants may pool their shares and rebuild the secret. Since the number of shares with (*t*-1) or less will be unable to reassemble the secret parts with insufficient participants. The threshold computing technique has many workable applications with different utilizations such as launching a nuclear system, opening a bank vault or authenticating a transfer of electronic funds. Such sensitive applications require a common access by several authorized people to ensure that the decision is made in a consensual and collective manner. Several secret sharing schemes have been proposed across different scenarios and strategies such as the integer ring that established a polynomial interpolation, the intersection of affine hyper planes, elliptic curves, bilinear maps, and the theorem of Chinese remainder[21, 22] .

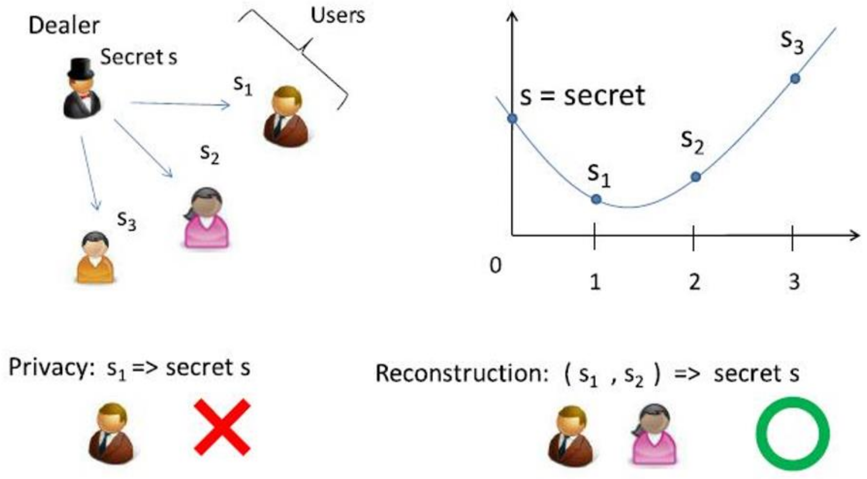

Dealer
Secret s
Users
s_1
s_2
s_3
s = secret
s_1
s_2
s_3
0
1
2
3
Privacy: s_1 => secret s
Reconstruction: (s_1 , s_2) => secret s

Figure 2.1 Secret Sharing Scenario

2.2 Shamir's Secret Sharing Scheme

The secret sharing scheme describes the secret key distribution process by a dealer to a group of trusted subscribers. The processes going through this scheme will be explained in detail by two phases as it can be seen in[23] :

- Setup process:

For this (n, t)-scheme, where $2 \leq n \leq t$, let U_1, ..., U_t be the participants and let $S \in N$ be the secret information (where N denotes the set of integer numbers, including 0).

The scheme works with polynomials over the finite field F_P, where p is some prime larger than both n and S. The dealer defines an (n−1) degree polynomial $f(x) \in F_p [x]$, with coefficients chosen randomly and uniformly, except that the constant term is taken to be S. Thus, $f(x) = a_{n-1} x^{n-1} +\cdots+ a_1 x + a_0$, and $a_0 = S$. The dealer then evaluates $y_r = f(r)$ for $r = 1,...,t$, and privately sends (r, y_r) to participant U_r, for every r.

- Reconstruction process:

Supposing that for some $\{x_1,...,x_n\} \subseteq \{1,...,t\}$, that $U_{x1},...,U_{xn}$ wish to reconstruct S, they then pool their shares, giving each U_{xi}, $1 \leq i \leq n$, the complete sequence

(x_1,y_{x1}),...,(x_n, y_{xn}) from which he obtains $f(x)$ by the well-known Lagrange interpolation model, as shown in equation (2.1):

$$f\ (x) = \sum_{j=1}^{n} y_{xj} \prod_{\substack{i=1 \\ i\neq j}}^{n} \frac{(x-x_i)}{(x_j-x_i)} \qquad \ldots (2.1)$$

Lastly, U_{xi} evaluates f (0) = S.

2.3 Blakley's Secret Sharing Scheme

Just as Shamir developed his polynomials-based secret sharing scheme, Blakley introduced a different hyperplane/linear algebra-based method. Assume there are n people, and we intend to allow a group of k people to figure out the secret $S \in$ Fp. Doing this will require us constructing n linear equations in k variables over F_P. This can be done by fixing the not-necessarily-distinct elements c_1, ..., $c_k \in F_P$, with $c_1 = S$. Then, we can find n linear equations in k variables x_1, ..., x_k with coefficients in F_P, such that each equation will be satisfied by setting $x_j = c_j$ for $1 \leq j \leq k$. To be more specific; we randomly select a_{11}, a_{12}, ..., a_{nk}, b_1, ... , $b_n \in F_{P,}$ subject to the condition that for every i, $a_{i1}\ c_1 + a_{i2}\ c_2 +\cdots+ a_{ik}\ c_k = b_i$. Then, we assign the i th equation to person i. However, this cannot be completely done randomly, but most of the choices are acceptable, at least when there is a large p. Few things must be ensured; first, it is not ideal to say that an equation is $a_{i1}\ x_1 = b_i$ simply because the solution for x_1 can be singlehandedly determined by person i. Similarly, it is necessary to ensure that the unique solution c_1 for x_1 is not determined by any coalition of $k - 1$ people. It should also be ensured that any set of k people can determine c_1 .[24]

2.4 Threshold Secret Sharing Schemes

The only important component of the first Secret Sharing Schemes for the recovery of the secret is the number of the participants in the reconstruction phase. Hence, these schemes are often called threshold secret sharing schemes. Let $n \geq 2$, $2\leq k \leq n$. The access structure A = {A ∈ P ({1, 2, ... , n}) | $|A| \geq k$ } will be referred to as the (k, n) -threshold access structure .We obtain A_{min}= {A ∈ P ({1, 2, ... , n}) | $|A| \geq k$}, Á= {A ∈ P({1, 2, . . . , n}) | $|A| \leq k - 1$}, and $Á_{max}$= {A ∈ P({1, 2, . . . , n}) | $|A| = k - 1$}. In this, an Á secret sharing scheme will be shown as (k, n) threshold secret sharing scheme. If *P*(*x*) = a_{k-1} x^{k-1} + · · · + a_1 x^1 + a_0, the secret can also have the shares Ii_1, . . . , Ii_k by solving the system of equations, as shown in equation (2.2):

$$\begin{cases} a_{k-1}x_{i1}^{k-1} + \cdots + a_1x_{i1}^1 + a_0 = I_{i1} \\ \quad\quad\quad\quad . \\ \quad\quad\quad\quad . \\ a_{k-1}x_{ik}^{k-1} + \cdots + a_1x_{ik}^1 + a_0 = I_{ik} \end{cases} \quad \dots (2.2)$$

where has *k* unknowns (a_{k-1}, …. , a_1, a_0) and it has a different solution because the determinant of as illestrate in equation (2.3):

$$\begin{vmatrix} x_{i1}^{k-1} \cdots x_{i1}^1 & 1 \\ x_{i2}^{k-1} \cdots x_{i2}^1 & 1 \\ \cdots & \\ \cdots & \\ x_{ik}^{k-1} \cdots x_{ik}^1 & 1 \end{vmatrix} \quad \dots (2.3)$$

The point in the non-zero Vandermonde determinant can be view while the polynomial *P*(*x*) can be of a chosen degree of at most *k* − 1. Having only *k*−1 shares, the equations in Shamir's equation are shown in equation (2.4):

$$\begin{cases} a_{k-1}x_{i1}^{k-1} + \cdots + a_1x_{i1}^1 = I_{i1} - a_0 \\ \quad\quad\quad\quad . \\ \quad\quad\quad\quad . \\ a_{k-1}x_{ik}^{k-1} + \cdots + a_1x_{ik}^1 = I_{ik} - a_0 \end{cases} \quad \dots (2.4)$$

With the solutions to *k*−1 equations and *k*−1 unknowns (a_{k-1}, …… , a_1) being different for any a_0. Thus, all the possible secret values are likely equal.

The degree of the polynomial *p*(*x*) is taken as *k*-1 and when it is equivalent to $a_{k-1} \neq 0$, the scheme is not perfect. Hence, any *k* − 1 user can determine an element b_0 which is not the secret, i.e., $b_0 \neq a_0$. The Lagrange interpolation formula can be used to determine a polynomial *Q*(*x*) = b_{k-2} x^{k-2} + · · · + b_1 x^1 + b_0, such that *Q* (x_{ij}) = I_{ij} = *P* (x_{ij}), for all $1 \leq j \leq k - 1$, leading to the system, as shown in equation (2.5).

$$\begin{cases} a_{k-1}x_{i1}^{k-1} + (a_{k-2} - b_{k-2})x_{i1}^{k-2} + \cdots + (a_1 - b_1)\,x_{i1}^1 + (a_0 - b_0) = 0 \\ a_{k-1}x_{ik-1}^{k-1} + (a_{k-2} - b_{k-2})x_{ik-1}^{k-2} + \cdots + (a_1 - b_1)\,x_{ik-1}^1 + (a_0 - b_0) = 0 \end{cases} \quad \dots (2.5)$$

Consider the contradiction that $a_0 = b_0$; from the above function, *k* −1 equations and *k* − 1 unknowns (a_{k-1}, ... , a_1) have different solution, viz $a_{k-1} = 0$, $a_{k-2} = b_{k-2}$, . . . , $a_1 = b_1$

which contradicts that $a_{k-1} \neq 0$. Thus, an element b_0 which is not the secret can be determined by any $k - 1$ users and their uncertainty regarding the secret does not eventually align with that of an outsider.

Shamir [3] has proposed choosing $x_i = i$, for all $1 \leq i \leq n$. In this case, the secret can be reconstructed as for any group A with |A| = k [25], as shown in equation (2.6).

$$S = \sum_{i \in A} \left(Ii \, . \prod_{i \in A \ \{\mathrm{i}\}} \cdot \frac{j}{j-i} \right) \qquad \dots (2.6)$$

Example 1:

Assume $n = 5$ and $k = 3$. Also consider the polynomial $P(x) = 2x^2 + 7x + 10$ over the field Z_{11}. The secret is $S = 10$ with the following corresponding shares:

$P(1) = 2(1)^2 + 7(1) + 10$ => 19 mod 11 = 8

$P(2) = 2(2)^2 + 7(2) + 10$ =>32 mod 11 = 10

$P(3) = 2(3)^2 + 7(3) + 10$ =>49 mod 11 = 5

$P(4) = 2(4)^2 + 7(4) + 10$ =>70 mod 11 = 4

$P(5) = 2(5)^2 + 7(5) + 10$ =>95 mod 11 = 7

Having the shares p (1), p (2), p (3), the secret can be reconstructed as, according to equation (2.6):

$$= 8 \, \frac{2}{2-1} \cdot \frac{3}{3-1} + 10 \, \frac{1}{1-2} \cdot \frac{3}{3-2} + 5 \, \frac{1}{1-3} \cdot \frac{2}{2-3}$$

$$=> \ (-1) \, mod \, 11 = 10$$

Example 2:

Shamir Secret Sharing with $p = 31$. Consider $t = 3$ as the threshold while $7 \in Z/_{31Z}$ be the secret. Choosing the elements at random $a_1 = 19$ and $a_2 = 21$ in $Z/_{31Z}$, and set $f(x) = 7 + 19x + 21x^2$. Being a trusted party, many shares can now be generated and are distributed to the share-holders while the original polynomial f(x) will be destroyed.

$(1, f(1)) = (1, 16)$	$(5, f(5)) = (5, 7)$
$(2, f(2)) = (2, 5)$	$(6, f(6)) = (6, 9)$
$(3, f(3)) = (3, 5)$	$(7, f(7)) = (7, 22)$
$(4, f(4)) = (4, 16)$	$(8, f(8)) = (8, 15)$

The secret can be recovered from the first three shares (1, 16), (2, 5), (3, 5), according to equation (2.6):

$$f(0) = 16\,\frac{2\,.\,3}{(1-2)(1-3)} + 5\,\frac{5\,.\,1\,.\,3}{(2-1)(2-3)} + 5\,\frac{5\,.\,1\,.\,2}{(3-1)(3-2)} = 7$$

By using different calculation for the shares (1, 16), (5, 7), and (7, 22), according to equation (2.6):

$$f(0) = 16\,\frac{2\,.\,3}{(1-2)(1-3)} + 7\,\frac{1\,.\,7}{(5-1)(5-7)} + 22\,\frac{1\,.\,5}{(7-1)(7-5)} = 7$$

Shamir has stated that there are some interesting features in his scheme:

- The scheme is suitable when the size of each share is not more than the size of the secret.
- The scheme is active, suggesting that if the threshold '*k*' is constant, it is easy to remove some of the existing secrets while some novel secrets can be created without significantly affecting the other secrets.

2.5 Shamir's Threshold Secret Sharing Scheme

Authorized sets in a threshold secret-sharing schemes are sets with a bigger size than some threshold, i.e., they achieved the *t*-out-of-*n* access structure $A_t = \{A \subseteq \{p_1, \ldots, p_n\} : |A| \geq t\}$, where $1 \leq t \leq n$ represents an integer. As mentioned in[3] developed a simple but elegant threshold scheme in which the secrets and shares domain is the elements of a finite field F_q for some prime-power $q > n$. Let $\alpha_1, \ldots, \alpha n \in F_q$ be *n* distinct non-zero elements common to all parties (e.g., if $q > n$ is a prime, then, it can be assumed that $\alpha_j = j$). The dealer shares a secret $k \in F_q$ by randomly and independently choosing $t - 1$ elements $a_1, \ldots, a_{t-1}$ from F_q with uniform distribution. Then, these chosen random elements and their secret define a polynomial $P(x) = k +$

$\sum_{i=1}^{t} a_i x^i$. The share of p_j is $s_j = P(\alpha_j)$ (P is evaluated using the arithmetic of F_P). The privacy and correctness of Shamir's scheme are based on the Lagrange's interpolation theorem where, for every every t distinct values $x_1, \ldots, x_t$, every field F, and every t values $y_1, \ldots, y_t$, there is a specific polynomial Q of degree at most $t - 1$ over F, such that $Q(x_j) = y_j$ for $1 \leq j \leq t$. To demonstrate the correctness of Shamir's scheme, it should be observed that each set B of size t has t points of polynomial P, hence, can use Lagrange's interpolation to reconstruct it and compute $k = P(0)$. Normally, a set B = $\{p_{i1}, \ldots, p_{it}\}$ computes, as shown in equation (2.7):

$$Q(x) = \sum_{l=1}^{t} S_{il} \sum_{1 \geq j \geq t, j \neq l} \frac{\alpha_{ij} - x}{\alpha_{ij} - \alpha_{il}} \qquad \ldots (2.7)$$

Observe that Q (α_{il}) = s_{il} = P(α_{il}) for $1 \leq l \leq t$. This means that P and Q are polynomial of degree at most $t - 1$ that agree on t points; thus, P and Q are equal (based on the uniqueness in the interpolation theorem), and, particularly, Q(0) = P(0) = k. Therefore, k can be reconstructed by the parties in B by computing, as illustrate in equation (2.8):

$$k = Q(0) = \sum_{l=1}^{t} S_{il} \sum_{1 \geq j \geq t, j \neq l} \frac{\alpha_{ij}}{\alpha_{ij} - \alpha_{il}} \qquad \ldots (2.8)$$

The reconstruction function for any given set B is a linear combination of the shares, i.e., as shown in equation (2.9):

$$k = \sum_{l=1}^{t} \beta_l \cdot S_{il} \text{ ,} where \ \beta_l = \prod_{1 \geq j \geq t, j \neq l} \frac{\alpha_{ij}}{\alpha_{ij} - \alpha_{il}} \qquad \ldots (2.9)$$

Observe that $\beta_1, \ldots, \beta_t$ does not depend on the secret k but only depends on the set B. Contrarily, any unauthorized set T with $t - 1$ parties has $t - 1$ points of the polynomial, which in conjunction with each possible secret, determines the unique polynomial of degree at most $t-1$. As per the interpolation theorem, every T = $\{p_{i1}, \ldots, p_{it-1}\}$ and every $a \in F_q$ (at most $t - 1$) is associated with a unique polynomial P_a with a degree, such that $P_a(0) = a$ and $P_a(\alpha_{il}) = s_{il}$ for $1 \leq l \leq t - 1$. Therefore, as shown in equation (2.10):

$$\Pr\left[\Pi\,(a, r)_T = \langle s_{il} \rangle\ 1 \leq l \leq t-1\right] = \frac{1}{q^{t-1}} \qquad \ldots (2.10)$$

Being that this probability is equal for every ∈ F_q, the privacy follows[26] .

Shamir's scheme has found application in several threshold cryptographic protocols, such as key distribution/agreement protocols, multiparty computation protocols, digital signature protocols, and Byzantine agreement protocols[27] **.**

2.6 Adversary Model

"A system without an adversary definition cannot possibly be insecure; it can only be astonishing". "Astonishment is a much-underrated security vice" (Principle of Least Astonishment). From these statements, it can be explained that any system without an adversary hardly can be believed. To have a highly secure system, you need also to plan about the adversaries the system may face in the future. The adversary model consists of sets of assumptions, explicit and implicit, which have been made with regard to the adversary in any given situation. While there is a precedence for using such a definition of adversary modeling, it is not widely used in literature and there are some changing properties in this model which are related to the traditional secret sharing model [28].

- Trusted dealer: A fully trusted dealer cannot be corrupted by an adversary.
- Polarized participants: The participants can either be totally honest by following the rules or totally malicious after being captured by an adversary (they will begin to break the rules).

An adversary in all Secret Sharing Schemes may wish to acquire the secret information by learning the information about shares. However, different types of Secret Sharing Schemes have a different goal based on their recoverability. The passive adversary can be only involved in share capturing in the traditional model; hence, they can only strive to secret reconstruction by withholding shares. For the different types of Secret Sharing schemes [2, 3], it is necessary to identify the main recoverability goals of an adversary.

- **Types of Adversary Model**

The adversary model consists of multiple types, each type of them does a different job than the other. These types can be summarized by the following steps [29]:

1- Passive versus active adversary: Every player has a curiosity to know the other players' secret, but players feel they are honest to them. At the same time, they have the curiosity to know the secret, which is an adversary. When players want to form the network or game, they will reconstruct a wrong secret while striving to get the secret of the players.

2- Static versus mobile adversary: A static adversary corrupts the players ahead of time while a mobile adversary corrupts the players while executing the protocol.

3- Computational versus unconditional security: The network protocols are much secured and rely on basic presumptions (the hardness of factoring or discrete logarithm from the adversary has unlimited computational power).

2.7 Some Attacks on Shamir's Secret Sharing Scheme (SSSS)

It is inevitable that some schemes are subject to cheaters, with the motivation of fooling honest participants and keeping the secret to themselves for whatever motive they have. Tompa & Woll [30] discussed how to share a secret with cheaters which makes it possible to cheat Shamir's Secret Sharing Scheme. In this study, the researchers stated that a person or a group is able to succeed in cheating SSSS when they are able to achieve the following goals[31] :

- Type 1 attack: In this type of attack, the cheaters can either be honest shareholders who erroneously present their shares, or they could be dishonest shareholders who, without any form of collaboration, present their faked shares. In this attack, each faked share represents a random integer and is totally independent of the other shares.
- Type 2 attack: In this type of attack, the cheaters are dishonest shareholders who aim to fool the shareholders by modifying their shares. Here, it is assumed that all shareholders synchronously release their shares, thus, the cheaters can only figure out their faked shares before secret reconstruction by collaborating among themselves. However, they cannot modify their shares after getting information about the shares of the honest shareholders (i.e. all the shares are believed to be revealed simultaneously). With this assumption, the cheaters can only successfully execute an attack to fool the honest shareholders when there is a larger/equal number of cheaters compared to the threshold value.
- Type 3 attack: In this type of attack, the cheaters are dishonest shareholders who also aims to fool honest shareholders by modifying their shares. It is assumed in this type of attack that all the shareholders asynchronously release their shares and because the shareholders release their shares one the same time, the cheaters mainly

aim to release their own shares after all the honest shareholders have released their shares so that it can easily modify their shares.

2.8 Mathematical Preliminaries of Numerical Analysis Definition

Numerical analysis is a department of mathematics that prepare tools and methods to solve mathematical problems by numerical formulas. Various problems are encountered in any system that uses mathematical methods and cannot solve all these problems using only one mathematical method. Therefore, many types of numerical analysis methods are used in solving them. A number of them will be addressed next:

2.8.1 Lagrange Interpolation Concept

The mathematical preliminaries for the interpolation terminology can be described as a process of computation to find a value existing between two or more values. The polynomial equation which builds new data points with discrete range is called the polynomial interpolation. The recognized values are arbitrary and keep on changing unsystematically as shown in figure (2.2). Lagrange polynomial interpolation is adapted for generating the main points computationally, as shown in equation (2.11).

$$l_j^n(x) = \prod_{\substack{i=0 \\ i\neq j}}^{n} \frac{x-x_j}{x_i-x_j} \quad , j = 0 , \ldots, n \qquad \ldots \quad (2.11)$$

The Lagrange polynomial interpolation is employed to determine a value between pair known values. Specifically, Lagrange polynomial interpolation of (order 1) is documented in (equation 2.12). For the sake of reaching a value by the use of three values, Lagrange polynomial interpolation of (order 2) is used as stated in (equation 2.13). On the other hand, to determine value by employing four established values, Lagrange polynomial interpolation of (order 3) is used as illustrated in (equation 2.14)[32, 33].

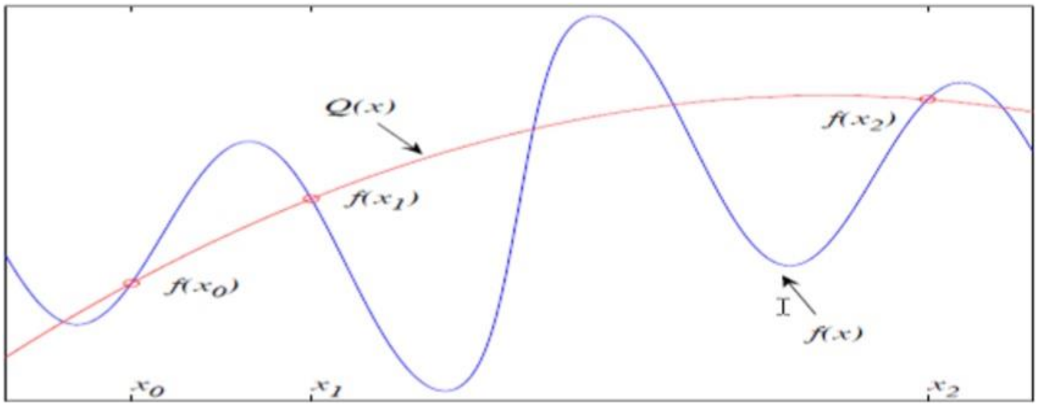


Figure 2.2. Polynomial interpolation Q(x) to appreciation values between x0, x1, & x2

$$f_1\ (x) = \frac{x-x_1}{x_0-x_1} f(x_0) + \frac{x-x_0}{x_1-x_0} f(x_1) \qquad \dots\ (2.12)$$

$$f_1(x) = \frac{x-x_1}{x_0-x_1}\frac{x-x_2}{x_0-x_2} f(x_0) + \frac{x-x_1}{x_0-x_1}\frac{x-x_2}{x_0-x_2} f(x_1) + \frac{x-x_1}{x_0-x_1}\frac{x-x_2}{x_0-x_2} f(x_2) \qquad \dots\ (2.13)$$

$$f_1(x) = \frac{x-x_1}{x_0-x_1}\frac{x-x_2}{x_0-x_2}\frac{x-x_3}{x_0-x_3} f(x_0) + \frac{x-x_0}{x_1-x_0}\frac{x-x_2}{x_1-x_2}\frac{x-x_3}{x_1-x_3} f(x_1) +$$

$$\frac{x-x_0}{x_2-x_0}\frac{x-x_1}{x_2-x_1}\frac{x-x_3}{x_2-x_3} f(x_2) + \frac{x-x_0}{x_3-x_0}\frac{x-x_1}{x_3-x_1}\frac{x-x_2}{x_3-x_2} f(x_3) \qquad \dots\ (2.14)$$

2.8.2 Hermite Interpolation Concept

The Hermite interpolation was developed as a variant of Lagrange's interpolation. The Hermite polynomial of a function *f* is calculated using divided differences[34, 35] .

Suppose that a function *f(x)* is defined on a closed interval [*a*, *b*]; given *n* + 1 data points $x_0, x_1, x_2, \cdots, x_n$, ($a \le x_i \le b$, $x_i \neq x_j$ for $i \neq j$), and values, as shown in equation (2.15):

$$f_k = f\,(x_k),\ f'_k = f'(x_k),\ k = 0, 1, 2, \cdots, n. \qquad \dots\ (2.15)$$

We strive to establish a 2n + 1 dimensional polynomial *P*(*x*) such that *P*(*x*) will satisfy, as shown in equation (2.16):

$$P\ (x_k) = f_k\ ,\ \ p'\,(x_k) = f'_k\ , k = 0, 1, 2, \dots \dots, n. \qquad \dots\ (2.16)$$

The challenge of finding this polynomial P(x) presents a Hermite interpolation. It is evident here that a unique 2n + 1 dimensional polynomial P(x) can be achieved using the following equation, as shown in equation (2.17):

$$P(x) = \sum_{i=0}^{n} f_i h_i\ (x) + \sum_{i=0}^{n} f'_i g_i\ (x) \qquad \dots (2.17)$$

Where two 2n + 1 dimensional polynomial $h_i(x)$, $g_i(x)$ satisfy

$$h_i\,(x_j) = \begin{cases} 1 & i = j \\ 0 & i \neq i \end{cases}$$

$g_i(x_j) = 0$ for any i, j

And

$h'_i(x_j) = 0$ for any i, j

$$g'_i\,(x_j) = \begin{cases} 1 & i = j \\ 0 & i \neq i \end{cases}$$

This is called Hermite interpolation.

2.8.3 Newton’s Divided Difference Interpolation Formula

Newton's Divided Difference is an approach towards finding an interpolation polynomial that suits a given set of data or points. Owing to the exclusivity of interpolation polynomials, Newton's Divided Difference, just like the Lagrange's method, can find the exact interpolation polynomial. This task is accomplished using the Newtons’ divided difference equation as shown in equation (2.18):

$$f\,(x_0, x_1, x_2, \dots \frac{f(x_1, x_2, x_3 \dots\dots x_n) - f(x_0, x_1, x_2}{x_n - x_0} \qquad \dots (2.18)$$

The polynomial is derived from this equation known as Newton's divided difference formula for interpolation polynomial[36, 37], as shown in equation (2.19) :

$$f(x) = f(x_0) + (x - x_0)\ f\ (x_0, x_1) + (x - x_0)\ (x - x_1)\ f\ (x_0, x_1, x_2) + (x - x_0)(x - x_1)\ (x - x_2)\ \mathrm{f}\ (x_0, x_1, x_2, x_3) + \dots . + (x - x_0)\ (x - x_1)\ (x - x_2) \dots (x - x_{i-1}) f(x_0, x_1, x_2, x_3 \dots\dots x_{i-1}) + \dots . + (x - x_0)(x - x_1)(x - x_2) \dots .\ (x - x_{n-1})\ f\ (x_0, x_1, x_2, x_3\ \dots\dots\ x_n) \qquad \dots (2.19)$$

2.9 Evolution of Magic Square

Studies on magic squares have lasted nearly three thousand years with the foremost study reported in China about 2200 B.C. Arab astrologers have used magic squared in the 19th century to calculate horoscopes, and by 1300 A.D., the west has already started using magic squares. The German artist engraved the date 1514 in the bottom row as two consecutive numbers because the magic square concept is not well understood. Magic squares are commonly used by puzzlers and amateur mathematicians. A magic square of order n in recreational mathematics is an arrangement of n numbers, usually different integers, in a square, such that the sum of all the numbers in all rows, columns, and both diagonals amount to the same constant. The construction of magic squares using different methods has been discussed in many types of research[38] .

2.10 Principles of Magic Square

A magic square consists of a square matrix presented as a checkerboard filled with letters or numbers in a specified arrangement. Mathematicians have found interest in arithmetic squares that consists of N^2 boxes (known as cells) which are filled with different integers. Such a manner of numbers arrangement is regarded as a magic square if the sums of the numbers in the vertical columns, horizontal rows, and main diagonals are equal. A magic square is said to be of the *N*th order if it has integers which are the consecutive numbers from 1 to N^2 and the magic number or sum of each row is a constant represented as ***S*** [39], as shown in equation (2.20):

$$S = \frac{N\,(N^2+1)}{2} \qquad \dots (2.20)$$

In the magic square, the pivot element is the center element in the middle square as depicted in Figure 2.3. The following formula can be used to calculate the pivot element in any magic square of odd order with sequential numbers, as shown in equations (2.21):

$$P = \frac{(N^2+1)}{2} \qquad \dots (2.21)$$

According to equation (2.21):

$$P = \frac{(3^2+1)}{2} = 5$$

Sometimes, the magic number is referred to as the *magic sum* or *magic constant*. To derive this expression for ***S***, recall that the sum of the first *m* numbers in the arithmetic series 1+ 2 + 3 + …. + *m* is equal to *m* (*m* + 1) / 2. In our case, *m* = N^2 because we are interested in the sum of all the numbers in the magic square. This means that the sum of the numbers in a magic square is N^2 (N^2 + 1) / 2 = (N^4 + N^2) / 2. To get ***S***, we divide this result by *N*, which gives the sum for each of the *N* rows and *N* columns [40].

A better understanding of these mathematical definitions will be achieved with some examples. The third order magic square with 3 * 3 cells and containing integers 1 – 9 is the simplest magic square. It has a magic sum of 15 along the 3 rows, 3 columns, and 2 diagonals. For a third-order square, the digits and its mirror image can only be arranged in one unique way, as shown in figure (2.3):

4	9	2
3	5	7
8	1	6

Figure 2.3 Third-Order Magic Square

In this case, N^{3} because there are 3 rows and 3 columns, while the magic sum ***S*** is 15 because the summation of the numbers in any direction = 15. For instance, considering the previous square, it will be observed that the sum of 4 + 9 + 2 = 15 (row), the sum of 4 + 3 + 8 = 15 (column), and the sums is 4 + 5 + 6 = 15 (diagonal), etc. The magic sum formula can be compute as shown in equation (2.22):

$$\frac{n\,(n^2+1)}{2} \qquad \text{… (2.22)}$$

According to equation (2.22):

$$\frac{3\,(3^2+1)}{2} = 15$$

A compact formula exists for the calculation of the magic constant for magic squares that start at numbers other than 1 and that make use of an arithmetic series with a constant difference between successive integers. The magic constant for these kinds of squares depends on the order ***N***, the starting integer ***A***, and the difference ***D*** between successive terms [41], as shown in equation (2.23).

$$S = \frac{N(2 * A + D(N^2 - 1))}{2} \qquad \dots (2.23)$$

The consecutive numbers (1 to n^2) in n rows and n columns can be arranged in basic Latin square format. The pivot element lies between two numbers, $\frac{(N^2)}{2}$ and $\frac{(N^2+1)}{2}$, as illustrate in equation (2.21).

Instead of using consecutive integers starting with 1, we might use an arithmetic series starting with, say, 17 and with a difference of 3 between successive integers.

Another formula for the determination of the pivot element in non-sequential odd order numbers which might have indeterminate integer number at the beginning or a period or another word with a difference of more than 1 in-between the numbers, as shown in equation (2.24). Here, N is the square order, A is the starting number, while D is the difference between the successive and the previous numbers. Three instances that respectively explain the notation are presented in Figure (2.4) a, b and c [42].

$$P = \frac{(2 * A + D(N^2 - 1))}{2} \qquad \dots (2.24)$$

63	42	57
48	54	60
51	66	45

(a): N=3, A=42 and D=3

48	13	38
23	33	43
28	53	18

(b): N=3, A=13 and D=5

18	4	14
8	12	16
10	20	6

(c): N=3, A=4 and D=2

Figure 2.4 Three of Magic Squares with Different Pivot Element

The examples of the pivot element as shown below according to equation (2.24):

$$\text{(a)}\, P = \frac{(2*42+3(3^2-1))}{2} = 54$$

$$\text{(b)}\, P = \frac{(2*13+5(3^2-1))}{2} = 33$$

$$\text{(c)}\, P = \frac{(2*4+2(3^2-1))}{2} = 12$$

The equation is used to calculate the Magic Sum (MS) (which includes the sum of all the rows, columns and diagonals numbers) in a magic square, as shown in equation (2.25):

$$MS = \frac{N^2(N^2+1)}{2} \qquad \ldots (2.25)$$

The MS for 3*3 = 45, MS for 4*4 = 136, MS for 5*5 = 325, MS for 8*8=2080 and so on; *MS* can also be calculated by multiplying the magic squares' MC * dimension [43] .

2.11 Magic Square Construction

Looking at magic squares and their hidden symmetries and amazing properties, it becomes difficult to believe that they can be constructed via several easy-to-remember approaches using simple rules. In fact, handbooks of "mental magic" often give these methods as "secret" ways to impress audiences. Several ways of magic squares construction have been developed through the ages. Based on these methods, magic squares can be categorized into 3 classes [44]:

2.11.1 Magic Squares of Odd Order

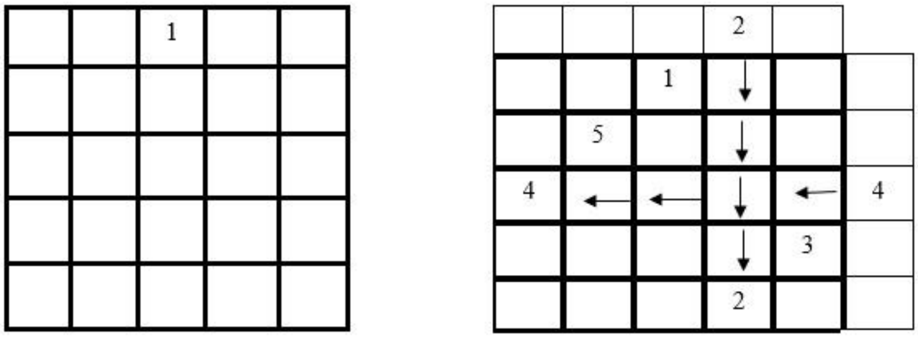
These are magic squares whose order *N* has the form 2*m* + 1, where *m* could be any positive integer 1, 2, 3, etc [45, 46].

- **De la Loubère's Method:**

Simon de la Loubère, a mathematician, in 1693, developed a method for the creation of any odd-order magic square. The method starts by positioning a 1 in the central upper cell. Let us construct a fifth-order magic square using this method.

Next, place 2 in an imaginary square diagonally upward to the right but outside the table. Here, we visually represent this box outside the table by temporarily adding another row and column to the square. Being that the 2 positioned outside the square,

it is brought to the bottom of the column. Next, position a 3 upward to the right of the 2, as illustrate in figure (2.5).



(a) De la Loubère's First Step (b) De la Loubère's Movements

Figure 2.5 Odd Order Magic Square (De la Loubère's Methods)

In the next step, place a 4 upward but to the right of the 3. Again, this 4 is outside the table, hence, it is placed at the opposite row end, with a 5 positioned upward to its right. It is not possible to place a 6 upward and to the right of the 5 since there is no space available; hence, 6 is positioned below the 5. We proceed until the 10 falls outside of the original square and continue the process. Notice that 16 falls outside the corner square and is written beneath the 15, as is the case when encountering an occupied square, as shown in figure (2.6).

	18	25	2	9	
17	24	1	8	15	17
23	5	7	14	16	23
4	6	13	20	22	4
10	12	19	21	3	10
11	18	25	2	9	

Figure 2.6 The Complete Square of De la Loubère's Method

➢ **In Summary:**

1. Start by placing 1 in the cell at the center of the top row.
2. Upon reaching any top edge, continue placing the integers in a diagonally upward position but to the right at the bottom of the next column.
3. Upon reaching the right-hand edge, continue placing the integers at the last cell but to the left of the next highest row.

4. Upon reaching an already filled cell, drop down one cell and continue.
5. Upon reaching the upper right corner cell, drop down one row.

By rotations and reflections, seven other magic squares can be constructed from this method. Once you have memorized this simple approach, you can amaze your friends by generating odd-order squares of a higher order. Additionally, you can start with a 1 in *any* cell and always generate a square that is magic in rows and columns but not necessarily diagonals.

You can also use de la Loubère's method to form imperfect magic squares that start with numbers other than 1. For example, the following square was created by starting with 3, and each succeeding integer was obtained by adding 2 to the preceding integer, as illustrate in figure (2.7):

17	3	13
7	11	15
9	19	5

Figure 2.7 De la Loubère's Square

Try this approach with other starting numbers and with other differences between succeeding integers.

- **Stairstep Method**

You may construct a magic square of odd order using the following easy recipe that involves a staircase like the assembly of cells. As an example, let's construct a

2 * 3 magic square. First, draw a "staircase" with consecutive integers along diagonals, as shown in figure (2.8):

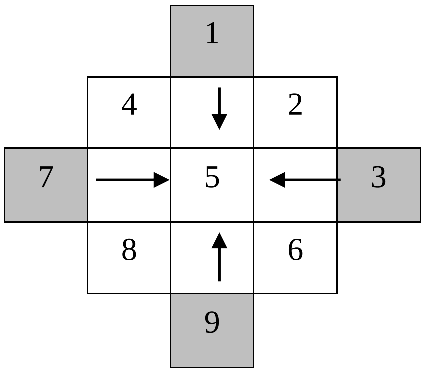


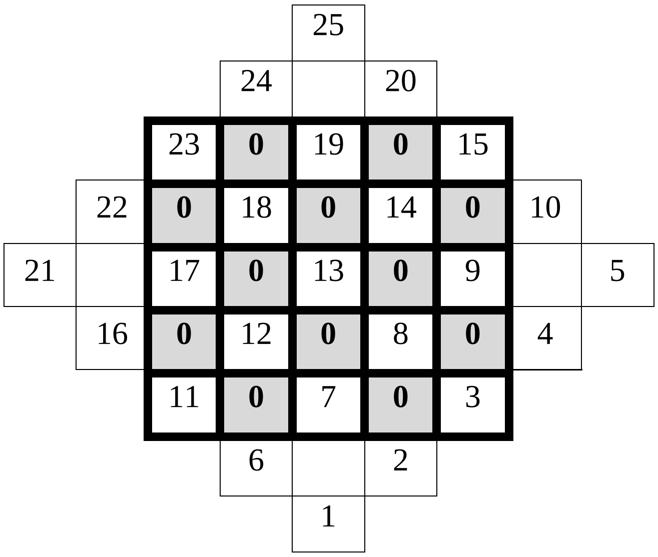
Figure 2.8 Stairstep Method

The cells containing the integers 1, 3, 7, and 9 are outside the central 3 * 3 array. To bring them into the array, slide each number to occupy the vacant cells furthest away from it along the same column or row. This movement will generate the following magic square, as illustrate in figure (2.9):

4	9	2
3	5	7
8	1	6

Figure 2.9 Third-Order Magic Square

Here is another example of the staircase method; this time, it is used to construct a 5 * 5 magic square, as shown in figures (2.10) and (2.11):



				25				
			24		20			
		23	**0**	19	**0**	15		
	22	**0**	18	**0**	14	**0**	10	
21		17	**0**	13	**0**	9		5
	16	**0**	12	**0**	8	**0**	4	
		11	**0**	7	**0**	3		
			6		2			
				1				

Figure 2.10 Staircase Before “infolding”

23	6	19	2	15
10	18	1	14	22
17	5	13	21	9
4	12	25	8	16
11	24	7	20	3

Figure 2.11 Final form of 5 * 5 Stair Step Magic Square

This time, let's start with the 1 on the bottom cell and proceed with numbering diagonally to the right. The dots represent empty cells to be filled in a manner similar to the previous 3 * 3 cell example.

2.11.2 Magic Squares of a Singly Even Order

Where *N* is of the form 2(2*m* + 1), such as 2, 6, 10, 14, 18, 22, etc. The order of a singly even square is only divisible by 2 and not by 4 [47].

- **Ralph Strachey's Method**

This method can be used for the construction of certain singly even order magic squares. As discussed, such magic squares have an order which is only divisible by 2 and not by 4. For instance, magic squares of order 6, 10, and 14 are considered singly even-order squares. Recall that singly even squares of order *N* are defined such that *N* = 4*x* +2 for positive integer values of *x*. In the following example, *N* = 6 an *x* = 1. The Strachey method is not quite as elegant as for odd squares in the sense that the method is largely empirical. Singly even magic squares are a big challenge to construct using simple rules. Let's describe the method generally before giving a specific example. Start by subdividing a square into four equal parts, *A*, *B*, *C*, and *D*, as shown in figure (2.12).

A	*C*
D	*B*

Figure 2.12 Strachey's Method

Eventually, square arrays will be inserted into *A*, *B*, *C*, and *D*; these four-square arrays will be of odd order *M* each with N ^{2}/ 4 cells. For our example case of N = 6, this means that each subsquare is of order M = 3, with nine cells. Here's a general description. Start by using de la Loubère's method to construct a magic square with integers 1 through M^2 where M = N / 2. Jam this magic square into *A*.

Construct and jam three other magic squares into *B*, *C*, and *D*. These additional magic squares go from $M^2 + 1$ through $2M^2$, $2M^2 + 1$ through $3M^2$, and $3M^2 + 1$ through $4M^2$. a large square filled with consecutive integers 1 through N^2 will be integrated.

If this N * N square was examined, the sum *R* of the integers in each row is the same. The sum *C* of the integers in each column is the same, but *R* does not equal *C*. The sums D_1 and D_2 of the integers in the main diagonals are different from the column sums or row sums. By swapping a small number (N^2 / 4 - N) of integers, the square can be converted into a magic square.

Look at an example to clarify this; let's choose x =1, which gives us a sixth-order square. Start by dividing a square into four equal squares *A*, *B*, *C*, and *D*. Using de la Loubère's method, the numbers 1 through 9 are used to construct the upper left square, as illustrate in figure (2.13):

8	1	6	26	19	24
3	5	7	21	23	25
4	9	2	22	27	20
35	28	33	17	10	15
30	32	34	12	14	16
31	36	29	13	18	11

Figure 2.13 Singly Even Strachey's Method

In square *B*, use the same approach to construct a magic square using numbers 10 through 18. In square *C*, the same approach is used to construct a magic square using numbers 19 through 27. In Square *D*, the same approach is used to construct a magic square using numbers 28 through 36. Look carefully, 6*6 magic square seems close to be obtained. Notice that at this point, all rows sum to the same number, 84. All columns sum to 111. The right main diagonal sums to 165. The left main diagonal sums to 57. this 6 * 6 square can be turned into a magic square by swapping just three pairs of numbers. To help you see the swaps, I’ve singly and doubly underlined pairs and put a pair in bold italic. Just by swapping the 8 and 35, the 4 and 31, and the 5 and 32 a perfect sixth-order magic square is obtained, as shown in figures (2.14) and (2.15).

8	1	6	26	19	24
3	5	7	21	23	25
4	9	2	22	27	20
35	28	33	17	10	15
30	32	34	12	14	16
31	36	29	13	18	11

Figure 2.14 Ralph Strachey’s Method Before Swapping

35	1	6	26	19	24
3	**32**	7	21	23	25
31	9	2	22	27	20
8	28	33	17	10	15
30	**5**	34	12	14	16
4	36	29	13	18	11

Figure 2.15 Ralph Strachey’s Method After Swapping

2.11.3 Magic Squares of a Doubly Even Order

These are magic squares whose order *N* is of the form 4*m*, such as 4, 8, 12, 16, 32, etc. The order of a doubly even magic square is divisible by both 2 and 4 [48].

- **Dürer’s Method:**

Albrecht Dürer’s 4 * 4 magic square was constructed in 1514 A.D. At that time, Dürer described a general method for constructing doubly even magic squares. First, draw imaginary main diagonals through every 4 * 4 sub-square of the square such as in the following square on the left. Then, position 1 in the upper left corner cell and proceed with the consecutive numbers horizontally to the right; however, only write the numbers down if the cells are crossed by diagonals. Repeat this procedure for each row but once the bottom right corner cell is reached, assume that that the number 1 falls within this square and reverse the step by proceeding to the left horizontally and filling the empty cells. The figure (2.16) shown squares are achieved for a fourth-order square before-and-after the described procedures:

1	2	3	**4**
5	6	7	8
9	10	11	12
13	14	15	**16**

(a) Before Diagonal Swaps

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

(b) After Diagonal Swaps

Figure 2.16 Doubly Even Durer's Method

In this example with a 4 * 4 square, we first write the consecutive numbers 1 through 16. Next, the main diagonals is examined and symmetrical swaps are made across the center of each highlighted diagonal. This means 1 swap with 16, 6 with 11, 13 with 4, and 10 with 7.

2.12 Some Significant Properties of Magic Squares

Some of the interesting features and properties considered are listed below during the construction of normal magic squares [49]:

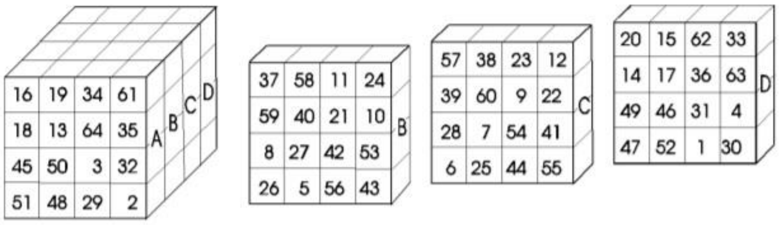
1. The magic nature of the squares is maintained by adding a certain number to each number in the squares.
2. The squares are kept magical by multiplying each number in the square by a certain number.
3. The squares are also kept magical by exchanging 2 rows or 2 columns from the center of square equidistantly.
4. An even order magic square is kept magical by interchanging its quadrants.
5. An odd order magic square is kept magical by rows and partial quadrants interchange.

6. The outstanding features of the square matrix make the square “magic” as it contains different positive integers from 1, 2, …, n^2 whose vector sum in all directions is constant.

2.13 Introduction to Magic cube

A magic cube of order n is a 3-D $n*n*n$ matrix (cubical table) $Q_n = [q\ (i, j, k);\ 1 \leq i, j, k \leq n]$ which contains the natural numbers 1, 2, 3, ... , n^3 in an order such that:

$\sum_{x=1}^{n} q(x,j,k) = \sum_{x=1}^{n} q(i,x,k) = \sum_{x=1}^{n} q(i,j,x) = \frac{n(n^3+1)}{2}$ For all $i, j, k = 1, 2, ..., n$, (Note: there is no need for the sums of elements on any diagonal in a magic cube). The triple of numbers $(i; j; k)$ is called the coordinates of the element $q\ (i; j; k)$. as shown in figure (2.17) below.



16	19	34	61
18	13	64	35
45	50	3	32
51	48	29	2

37	58	11	24
59	40	21	10
8	27	42	53
26	5	56	43

57	38	23	12
39	60	9	22
28	7	54	41
6	25	44	55

20	15	62	33
14	17	36	63
49	46	31	4
47	52	1	30

Figure 2.17 Magic Cube

A magic square of order 1 is the same as a magic cube of order 1. As there is no magic square of order 2, similarly, there is no magic cube of order 2 [50]. In a magic cube, the basic feature is that the sum of all numbers in the layers, each column/row, and main diagonal space is equal to the single number called the cubes’ magic constant, denoted by *M3*(*n*), as shown in equation (2.26).

$$M_3\,(n) = \frac{n(n^2\ +1)}{2} \qquad \dots (2.26)$$

As per M. Trenklers’ theorem, a magic cube can be derived by combining a magic square with 2 orthogonal Latin squares [51]. The magic square concept can be extended into the third dimension; doing this will give us a magic cube. The sum of the row, column and main diagonal lines in such cubes is always a constant. Figure (2.18) is an example of such cubes:

2	13	27
22	9	11
18	20	4

1st layer

16	21	5
3	14	25
23	7	12

2nd layer

24	8	10
17	19	6
1	15	26

3rd layer

Figure 2.18 Magic Cube of Order 3

Magic cubes consist of entries 1, ..., N^3 which are arranged in an analogous manner to those in magic squares. As illustrate in equation (2.27):

$$C_3 = \frac{N}{2}(N^3 + 1) \qquad \dots (2.27)$$

Each layer in a magic cube is a magic square. The magic cube is similar to the magic square from the perspective of construction probability which dramatically increases with the order [52] .

Another approach towards the construction of a magic cube is presented in figure (2.20) below. The starting element in the diagonal cube starts from one end of the cube (from the upper layer dimensions to the lower left corner). This represents the smallest normal magic cube of 3x3x3 dimensions consisting of sequential numbers from 1 - 27 which are arranged in 3 layers of 9 numbers. For this magic cube, the magic constant is equal 42, as shown in figure (2.19). These layers represent the face or dimension for the magic cube magically arranged from all directions.

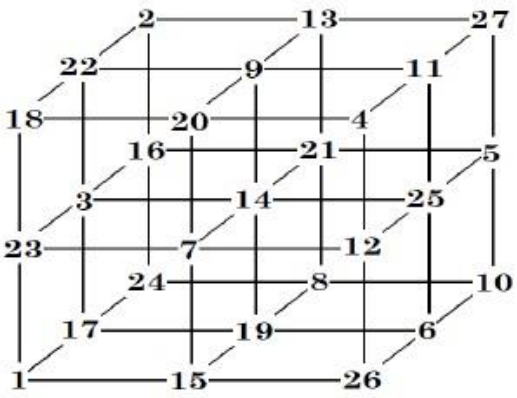


Figure 2.19 Magic Cube of Three Layers

There is more to magic cubes than just a game of numbers (as obtainable in chessboard or Rubik cube). The construction of magic cubes is mainly dependent on mathematical rules. They are rooted in several fields of mathematics, such as matrices, number theory, and combinatory [53].

2.14 The Construction of a Magic Cube

Magic cubes' construction is a challenging task that has over the years attracted much research interest in mathematical sciences. This is because there is no common method that works for both odd order and doubly even or singly cubes. However, the proposed method is suitable for all forms of magic cubes of any order as it basically relies on the technique of magic squares. This method allows for the construction of several magic cubes using sequential numbers or with constant differences between series of numbers. With this method, working for 6 squares will produce 1 magic cube while working for 12 squares will produce 2 magic cubes, etc. So, work with cubes involves the use of multiples of 6 numbers to generate several cubes based on the task requirements.

The basic notations for the construction of magic cubes are explained in the following examples:

1. Begin by building 6 separate magic squares of any order to correspond to the 6 sides of a cube as depicted in Figure (2.20).

2. Then, arrange the 6 cube surfaces as follows: position the 1st surface to face the 6th surface while the 2nd face the 5th. Finally, position the 3rd surface to face the 4th surface with the corresponding colors respectively.

21	0	15
6	12	18
9	24	3

1stsquare

48	27	42
33	39	45
36	51	30

2ndsquare

75	54	69
60	66	72
63	78	57

3rdsquare

102	81	96
87	93	99
90	105	84

4thsquare

129	108	123
114	120	126
117	132	111

5thsquare

156	135	150
141	147	153
144	159	138

6thsquare

Figure 2.20 Six Faces of Folding Magic Cube

Having constructed and colored the 6 sides/surfaces of the magic cube, compute the magic sum and magic constant concurrently for each square such that the sum of each of the similarly colored square pairs will produce the same result [16], as shown in figures (2.21) and (2.22).

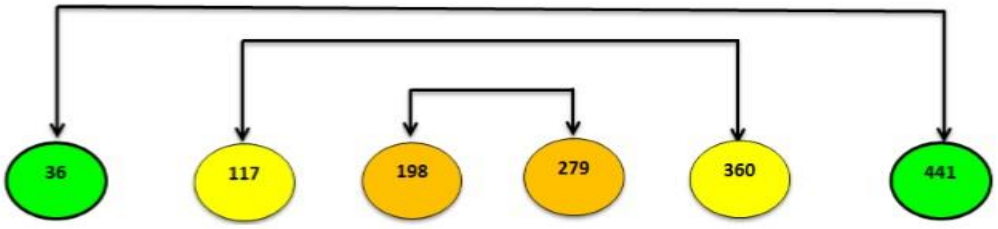


Figure 2.21 The Magic Constant of the Six Squares

36 + 441 = **477**, 117 + 360 = **477**, 198 + 279 = **477**

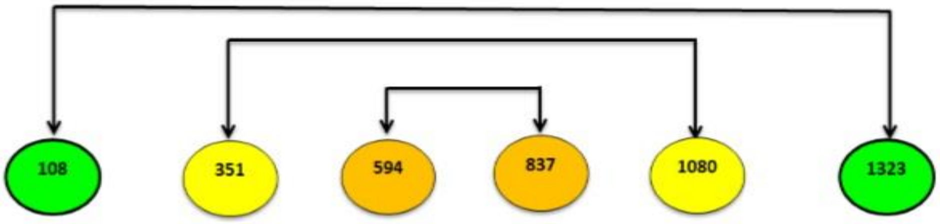


Figure 2.22 The Magic Sum of the Six Squares

108 + 1323 = **1431**, 351 + 1080 = **1431**, 594 + 837 = **1431**

The magic cube illustrated in Figure 2.20 is an order 3 cube with a starting value of 0 while the constant difference of 3 exists between each number pairs in the 1st square as in the following sequence (0, 3, 6, 9…24). The 2nd square begins and ends with the arrangement (27, 30, 33, 36…51) until the last or the 6th square of the cube which begins with the number 135 and ends with 159. A cube can be constructed from 11 distinct flat shapes which can be folded-up to generate the cube shapes. These shapes are presented in Figure (2.23):

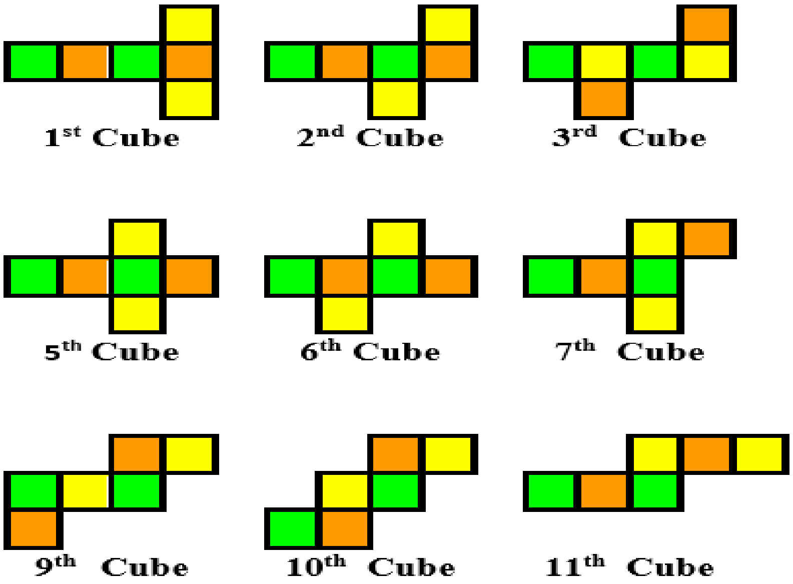


Figure 2.23 Eleven Distinct Shapes for the Magic Cubes

These shapes were colored with 3 distinct colors (green, yellow and Orange) with each opposing side similarly colored to achieve a folded cube with 6 sides/surfaces and the colors of each opposing side being the same. These colors were deployed to ensure that the arrangement of the magic square is maintained [16].

2.15 Applications of Magic Cube

Magic cube has delightful features that everyone appreciates; however, there is no specific application for magic cubes. Studies have recently combined magic squares with magic cubes in a bid to exploit their individual in several dimension and scopes [17], such as:

1. Cryptography.
2. Information security.
3. Remote access control.
4. Determinants and matrices field.
5. Applied mathematics.
6. Public/secret key sharing.
7. Number theory.
8. Coding and error correctness.

Chapter Three
Design and Implementation
Of the Proposed
Secret Sharing Algorithms

Chapter Three
Design and Implementation of the Proposed Secret Sharing Algorithms

3.1 Introduction

There are many different ways to develop secret sharing, but by combining them with the mathematical properties of magic cubes, the system has become stronger. The algorithms used to build magic cubes were previously used in secret key exchanges and encryption / decryption operations, but this is the first time that the properties of magic cubes have been used with secret sharing algorithms. The development of secret sharing algorithms depends on the methods of using the properties of magic cubes to share the secret among trusted participants. In this study, the proposed approach is combined with the secret of magic cubes and the approach of secret keys as an advanced approach to enhance safety requirements. This chapter presents four proposed algorithms as described in sections (3.2, 3.3, 3.4, and 3.5).

3.2 First Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange interpolation)

The main objective behind the adopted magic cube idea is to transfer the magic cube properties from the dealer to a group of trusted subscribers. The pivot element of one of the six magic squares is selected from the magic cube and sent within a polynomial (secret) to the participants. In addition, another selected element (The element of *G*) is sent to the subscribers to obtain the characteristics of the magic cube and then to reconstruct the original magic cube again. To describe the main notations for the mixing of magic cube with the Lagrange interpolation method of Shamir Scheme, the following must be explained:

The algorithm is beginning with build a magic cube of odd order in a manner as explain in chapter two (2.16). The pivot element is selected from the first magic square of the magic cube to use it as a secret value in the polynomial to compute the main points (x_i, y_i) and send them to the participants, as shown in equation (3.1):

$$F(x) = (pivot) + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \quad mod \quad prime \qquad \ldots (3.1)$$

Magic cube properties are sent to subscribers to be rebuilt again according to some parameters likewise (Start value, Difference value, Pivot element and the cube order). The new selected element (G) is chosen under special conditions after the magic cube is built by the dealer. This element must be smaller than the pivot element (Pivot > G) and greater than the cube's dimensions ($G > N$). When the Modular operation is taken between the pivot element and the numbers smaller than it, the output that will equal the dimensions (N) of the magic cube will be chosen accordingly, as shown in equation (3.2):

$$\text{Pivot Mod } G = N \qquad \ldots (3.2)$$

Also, the produce of dividing the (G) element on the dimensions of the magic cube will represent the difference (D) value according to the equation (3.3):

$$G / N = \text{Difference} \qquad \ldots (3.3)$$

After sending the points and (G) number to the participants. The Lagrange interpolation is used, as shown in equations (3.4, 3.5, 3.6, and 3.7) to reconstruct the secret again to obtain the pivot element (secret):

$$L_0 = \frac{x-x_1}{x_0-x_1} * \frac{x-x_2}{x_0-x_2} \qquad \ldots (3.4)$$

$$L_1 = \frac{x-x_0}{x_1-x_0} * \frac{x-x_2}{x_1-x_2} \qquad \ldots (3.5)$$

$$L_2 = \frac{x-x_0}{x_2-x_0} * \frac{x-x_1}{x_2-x_1} \qquad \ldots (3.6)$$

$$F(x) = \sum_{j=0}^{n} lj \cdot yj\ (x) \qquad \ldots (3.7)$$

After obtaining the pivot element, the equation (3.2) will be calculated to get the Dimensions (N) of the Magic cube and the equation (3.3) will also be calculated to obtain the difference (D) between the magic cube numbers. After obtaining (Pivot, Dimensions and Difference) of the magic cube, it is easy to obtain the starting number (A) of the magic cube by the equation (3.8) below:

$$\text{Start Number} = \frac{(\text{Pivot} * 2) - D*(N^2 - 1)}{2} \qquad \ldots (3.8)$$

Algorithm 3.1 First Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)

Input: pivot element, random coefficients (a_k), variable (x^k), modular reduction (prime number).
Output: secret (pivot).

1) Initialization of Algorithm

a- Select a magic cube with six magic squares of odd order exclusively.

2) Preprocessing Constructing Magic Cube (odd order)

a- The magic cube starts with a Start Number (A).

b- Choose the dimensions of the cube (N) and the amount of the difference between the cube numbers (D).

3) Transmitter Key Generation (KG)

a- Choose the Pivot element of the first magic square in the magic cube to be (secret) within the polynomial, equation (3.1).

b- Conclude Six points of polynomial.

c- Send points to six trusted subscribers.

d- Determine the Threshold value.

4) Generating (*G*) element

a- Select the element (G) with conditions (Pivot > G > N).

b- The selected G number should satisfy the condition of equations (3.2) and (3.3).

c- Send the (G) number to subscribers publicly.

5) Receiver Key Generation (KG)

a- Reconstruct the secret again by a specified number of subscribers (Threshold) to get the Pivot element via Lagrange Interpolation.

b- Equation (3.2).

c- Equation (3.3) where the resultant integer is taken and the remainder value is ignored.

d- After acquiring the properties of the magic cube (Pivot, D and N), the starting number (A) of the magic cube can be obtained through equation (3.8).

6) Reconstructing Magic Cube
a- Reconstructed the original magic cube through the characteristics obtained by the participants.

Example:

Assume that a folded magic cube of odd order (5*5) consisting of six magic squares, starting by the number 3 and with a constant difference between the sequential numbers is 4 as shown in figure (3.1).

67	95	3	31	59
91	19	27	55	63
15	23	51	79	87
39	47	75	83	11
43	71	99	7	35

1st Square

167	195	103	131	159
191	119	127	155	163
115	123	151	179	187
139	147	175	183	111
143	171	199	107	135

2nd Square

267	295	203	231	259
291	219	227	255	263
215	223	251	279	287
239	247	275	283	211
243	271	299	207	235

3rd Square

367	395	303	331	359
391	319	327	355	363
315	323	351	379	387
339	347	375	383	311
343	371	399	307	335

4th Square

467	495	403	431	459
491	419	427	455	463
415	423	451	479	487
439	447	475	483	411
443	471	499	407	435

5th Square

567	595	503	531	559
591	519	527	555	563
515	523	551	579	587
539	547	575	583	511
543	571	599	507	535

6th Square

Dimension = 5, Difference = 4, Start = 3

Figure 3.1 Odd Order Magic Cube with Six Dimensions

The Pivot element (51) of the first magic square is selected in the magic cube to be the secret within a polynomial. After that select the other coefficients randomly within the polynomial as stated in equation (3.1). The magic cube properties are represented in the Shamir's secret sharing scheme with the following important parameters:

Where n = participants, k = threshold, D = difference.

$n = 6$, $k = 3$, $p = 89$, $p > s$ and $p > n$.

$$F(x) = 51 + 14\,x + 6\,x^2 \quad \mod \ 89$$

As a result; six points of the polynomial are calculated and sent to six trusted subscribers (*n*) by the dealer as explained in Table (3.1).

Table 3.1 Generated Points of 1st Algorithm According to (*x*) And (*f* (*x*)) axes

(*x*)	***F* (*x*)**	**Points (*x*, *f* (*x*))**
1	71	(1, 71)
2	14	(2, 14)
3	58	(3, 58)
4	25	(4, 25)
5	4	(5, 4)
6	84	(6, 84)

Compute a suitable (*G*) number that fits to the pivot element and the dimensions (*D*) of the cube to be (*G* = 23). Pivot > *G*, *G* > Dimension (*N*).

$$51 > 23 > 5$$

Distribute the generated six points to six subscribers accompanied by the element (*G*). The selection of any three points (*k* = 3) to reconstruct the secret (Pivot) will be verified:

For Example: $D_0 = (2, 14)$, $D_1 = (4, 25)$, $D_2 = (6, 84)$

Compute the Lagrange interpolation through equations (3.4, 3.5, 3.6, and 3.7) :

$$\frac{1}{8}x^2 - \frac{5}{4}x + 3$$

$$-\frac{1}{4}x^2 + 2x - 3$$

$$\frac{1}{8}x^2 - \frac{3}{4}x + 1$$

Therefore, the original secret is (51).

After obtaining the Pivot element and (*G*) elements, it is possible to deduce the dimensions (*D*) of the original Magic Cube, as illustrate in equation (3.2):

$$51 \% 23 = 5.$$

By the same steps deduce the difference (D) between the numbers of the original Magic Cube according to the equation (3.3):

$$23 / 5 = 4.$$

After getting the following parameters (Pivot, Difference and Dimension), the starting number (A) can be obtained by equation (3.8):

$$\text{Start Number} = \frac{(51 * 2) - 4*(5^2 - 1)}{2} = 3$$

Finally, the six participants will have the ability to rebuild the original magic cube again as shown in Figure (3.2) below:

67	95	3	31	59
91	19	27	55	63
15	23	51	79	87
39	47	75	83	11
43	71	99	7	35

1st Square

167	195	103	131	159
191	119	127	155	163
115	123	151	179	187
139	147	175	183	111
143	171	199	107	135

2nd Square

267	295	203	231	259
291	219	227	255	263
215	223	251	279	287
239	247	275	283	211
243	271	299	207	235

3rd Square

367	395	303	331	359
391	319	327	355	363
315	323	351	379	387
339	347	375	383	311
343	371	399	307	335

4th Square

467	495	403	431	459
491	419	427	455	463
415	423	451	479	487
439	447	475	483	411
443	471	499	407	435

5th Square

567	595	503	531	559
591	519	527	555	563
515	523	551	579	587
539	547	575	583	511
543	571	599	507	535

6th Square

Figure 3.2 The Reconstruction of Original Odd Order Magic Cube

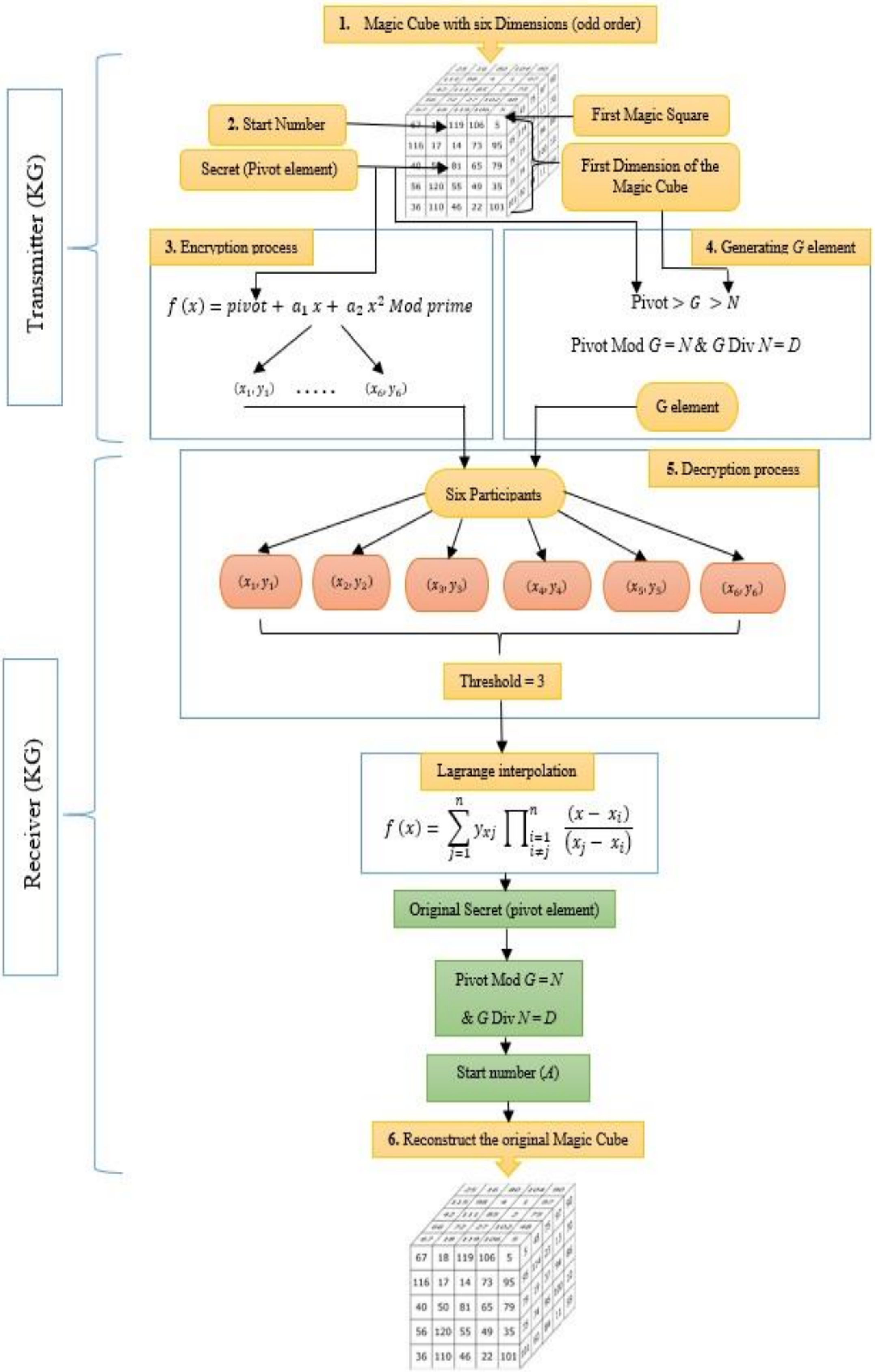


Figure 3.3 First Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)

3.3 Second Proposed Algorithm (Secret Sharing with Magic Cube using Hermite Interpolation)

This algorithm is a mixing of magic cube with secret sharing using Hermite interpolation, as:

The algorithm is beginning with build a magic cube of odd order in a manner as explain in chapter two (2.16). The pivot element is selected from the first magic square of the magic cube to use it as a secret value in the polynomial, as shown in equation (3.1) to compute the main points (x_i, y_i) and its derivatives (y'_i) and send them to the participants. Therefore, equation (3.1) becomes equation (3.9) after derivative:

$$F(x) = a_1 + 2.\, a_2\, x + \dots + k.\, a_k.\, x^{k-1} \quad \text{mod} \quad prime \qquad \dots (3.9)$$

Magic cube properties are sent to subscribers to be rebuilt again according to some parameters likewise (Start value, Difference value, Pivot element and the cube order). The new selected element (*G*) is chosen under special conditions after the magic cube is built by the dealer. This element must be smaller than the pivot element (Pivot > *G*) and greater than the cube's dimensions (*G* > *N*). When the Modular operation is taken between the pivot element and the numbers smaller than it, the output will equal the dimensions (*N*) of the magic cube, as shown in equation (3.2) will be chosen accordingly. Also, the output of dividing the (*G*) element on the dimensions of the magic cube will represent the difference (*D*) value according to equation (3.3). After sending the points and (*G*) number to the participants, the Hermite interpolation is used to reconstruct the secret again to obtain the pivot element (secret), as illustrate in equations (3.10, 3.11, and 3.12):

$$H_{2n+1}(x) = \sum_{j=0}^{n} f\left(x_j\right) H_{n,j}(x) + \sum_{j=0}^{n} f'\left(x_j\right) \hat{H}_{n,j}(x) \qquad \dots (3.10)$$

Where

$$H_{n,j}(x) = [1 - 2\left(x - x_j\right) \hat{L}_{n,j}\left(x_j\right)]\, L_{n,j}^{2}(x) \qquad \dots (3.11)$$

And

$$\hat{H}_{n,j}(x) = \left(x - x_j\right) L_{n,j}^{2}(x). \qquad \dots (3.12)$$

After obtaining the pivot element, will be calculated the (Pivot Mod *G*) to get the Dimensions (*N*) of the Magic cube, and (*G* Divide *N*) to obtain the difference (*D*) between the Magic cube numbers. After obtaining (Pivot, Dimensions and Difference) of the magic cube, it is easy to obtain the starting number (*A*) of the Magic cube by the equation regarding the equation (3.13) below:

$$\text{Start Number} = \frac{(\text{Pivot} * 2) - D*(N^2 - 1)}{2} \qquad \dots \ (3.13)$$

Algorithm 3. 2 Second Proposed Algorithm (Secret Sharing with Magic Cube using Hermite Interpolation)

Input: pivot element, random coefficients (a_k), variable (x^k), modular reduction (prime number).
Output: secret (pivot).

1) Initialization of Algorithm

a- Choose a magic cube with six magic squares of odd order exclusively.

2) Preprocessing Constructing Magic Cube (odd order)

a- The magic cube starts with a Start Number (*A*).

b- Choose the dimensions of the cube (*N*) and the amount of the difference between the cube numbers (*D*).

3) Transmitter Key Generation (KG)

a- Choose the Pivot element of the first magic square in the magic cube to be (secret) within the polynomial, as illustrate in equation (3.1), compute the polynomial derivative, as shown in equation (3.9).

b- Conclude Six points of (x_i, y_i) and (y'_i).

c- Send points and its derivatives to six trusted subscribers.

d- Determine the Threshold value.

4) Generating (G) element

a- Choose the element (*G*) with conditions (Pivot > *G* > *N*).

b- The selected *G* number should satisfy the condition of equations (3.2) and (3.3).

c- Send the (*G*) number to subscribers publicly.

5) Receiver Key Generation (KG)

a- Reconstruct the secret again by a specified number of subscribers (Threshold) to get the Pivot element via Hermite Interpolation.

b- Equation (3.2).

c- Equation (3.3) where the resultant integer is taken and the remainder value is ignored.

d- After acquiring the properties of the magic cube (Pivot, *D* and *N*), the starting number (*A*) of the magic cube can be obtained through equation (3.8).

6) Reconstructing Magic Cube

a- Reconstructed the original magic cube through the characteristics obtained by the participants.

Example:

Assume that a folded magic cube of odd order (5*5) consisting of six magic squares, starting by the number 5 and with a constant difference between the sequential numbers is 3 as shown in figure (3.4).

53	74	5	26	47
71	17	23	44	50
14	20	41	62	68
32	38	59	65	11
35	56	77	8	29

1st Square

128	149	80	101	122
146	92	98	119	125
89	95	116	137	143
107	113	134	140	86
110	131	152	83	104

2nd Square

203	224	155	176	197
221	167	173	194	200
164	170	191	212	218
182	188	209	215	161
185	206	227	158	179

3rd Square

278	299	230	251	272
296	242	248	269	275
239	245	266	287	293
257	263	284	290	236
260	281	302	233	254

4th Square

353	374	305	326	347
371	317	323	344	350
314	320	341	362	368
332	338	359	365	311
335	356	377	308	329

5th Square

428	449	380	401	422
446	392	398	419	425
389	395	416	437	443
407	413	434	440	386
410	431	452	383	404

6th Square

Dimension = 5, Difference = 3, Start = 5

Figure 3.4 The Odd Order Magic cube of 5*5 Dimension

The Pivot element (41) of the first magic square is selected in the magic cube to be the secret within a polynomial. After that select the other coefficients randomly within the polynomial to produce (y_i) as stated in equation (3.1). Additionally, compute the derivative of polynomial to deduce the (y'_i) as stated in equation (3.9). The magic cube properties are represented in the Hermite interpolation with the following important parameters:

Where n = participants, k = threshold, D = difference.

$n = 6$, $k = 3$, $p = 53$, $p > s$ and $p > n$.

$$F(x) = 41 + 9\,x + 11\,x^2 \quad mod \quad 53$$

And

$$f\,'(x) = 9 + 22\,x \qquad mod \qquad 53$$

As a result; six points (x_i,y_i) and (y'_i) of the polynomial are calculated and sent to six trusted subscribers (*n*) by the dealer as explained in Table (3.2).

Table 3.2 Generated Points of 2nd Algorithm According to (*x*) And (*f* (*x*)) axes

(*x*)	***f*(*x*)**	***f′*(*x*)**	**Points (*x*, *f* (*x*)), (*f′*(*x*))**
1	8	31	(1, 8), (31)
2	50	0	(2, 50), (0)
3	8	22	(3, 8), (22)
4	41	44	(4, 41), (44)
5	43	13	(5, 43), (13)
6	14	35	(6, 14), (35)

Compute a suitable (*G*) number that fits to the pivot element and the dimensions (*D*) of the cube to be (*G* = 18). Pivot > *G*, *G* > Dimension (*N*).

$$41 > 18 > 5$$

Distribute the generated six points to six subscribers accompanied by the element (*G*). The selection of any three points (*k* = 3) to reconstruct the secret (Pivot) will be verified:

For Example:

$$D_0 = (1, 8, 31), \quad D_1 = (2, 50, 0), \quad D_2 = (3, 8, 22)$$

Compute the Hermite interpolation:

First compute the Lagrange interpolation through equations (3.4, 3.5, and 3.6) and their derivatives, as shown in equation (3.9):

$$\frac{1}{2}x^2 - \frac{5}{2}x + 3, \qquad L'_{2,0}(x) = x - \frac{5}{2} = -1.5$$

$$-x^2 + 4x - 3, \qquad L'_{2,1}(x) = -2x + 4 = 0$$

And

$$\frac{1}{2}x^2 - \frac{3}{2}x + 1, \qquad L'_{2,2}(x) = x - \frac{3}{2} = 1.5$$

The polynomials $H_{2,j}$ through equation (3.11):

$$H_{2,0}(x) = [1 - 2(x-1)(-1.5)]\,(\frac{1}{2}x^2 - \frac{5}{2}x + 3)^2 = -18$$

$$H_{2,1}(x) = [1 - 2(x-2)(0)]\,(-x^2 + 4x - 3)^2 = 9$$

And

$$H_{2,2}(x) = [1 - 2(x-3)(1.5)]\,(\tfrac{1}{2}x^2 - \tfrac{3}{2}x + 1)^2 = 10$$

They $\widehat{H}_{2,j}$ are compute by equation (3.12):

$$\widehat{H}_{2,0}(x) = (x-1)(\tfrac{1}{2}x^2 - \tfrac{5}{2}x + 3)^2 = -9$$

$$\widehat{H}_{2,1}(x) = (x-2)(-x^2 + 4x - 3)^2 = -18$$

And

$$\widehat{H}_{2,2}(x) = (x-3)(\tfrac{1}{2}x^2 - \tfrac{3}{2}x + 1)^2 = -3$$

Finally, by using equation (3.10) produce:

$$H_5\,(x) = (-18*8) + (9*50) + (10*8) + (-9*31) + (-18*0) + (-3*22) = 41$$

Therefore, the original secret is (41).

After obtaining the Pivot element and (*G*) element, it is possible to deduce the dimensions (*N*) of the original Magic Cube, through equation (3.2):

$$41 \ \% \ 18 = 5.$$

By following the same steps, deduce the difference (*D*) between the numbers of the original Magic Cube according to the equation (3.3):

$$18 \,/\, 5 = 3.$$

After getting the following parameters (Pivot, Difference and Dimension), the starting number (*A*) can be obtained by equation (3.8):

$$\text{Start Number} = \frac{(41 * 2) - 3*(5^2 - 1)}{2} = 5$$

Finally, the six participants will have the ability to rebuild the original magic cube again as shown in Figure (3.5) below:

53	74	5	26	47
71	17	23	44	50
14	20	41	62	68
32	38	59	65	11
35	56	77	8	29

1st Square

128	149	80	101	122
146	92	98	119	125
89	95	116	137	143
107	113	134	140	86
110	131	152	83	104

2nd Square

203	224	155	176	197
221	167	173	194	200
164	170	191	212	218
182	188	209	215	161
185	206	227	158	179

3rd Square

278	299	230	251	272
296	242	248	269	275
239	245	266	287	293
257	263	284	290	236
260	281	302	233	254

4th Square

353	374	305	326	347
371	317	323	344	350
314	320	341	362	368
332	338	359	365	311
335	356	377	308	329

5th Square

428	449	380	401	422
446	392	398	419	425
389	395	416	437	443
407	413	434	440	386
410	431	452	383	404

6th Square

Figure 3.5 The Reconstruction of 5*5 Odd Order Magic Cube

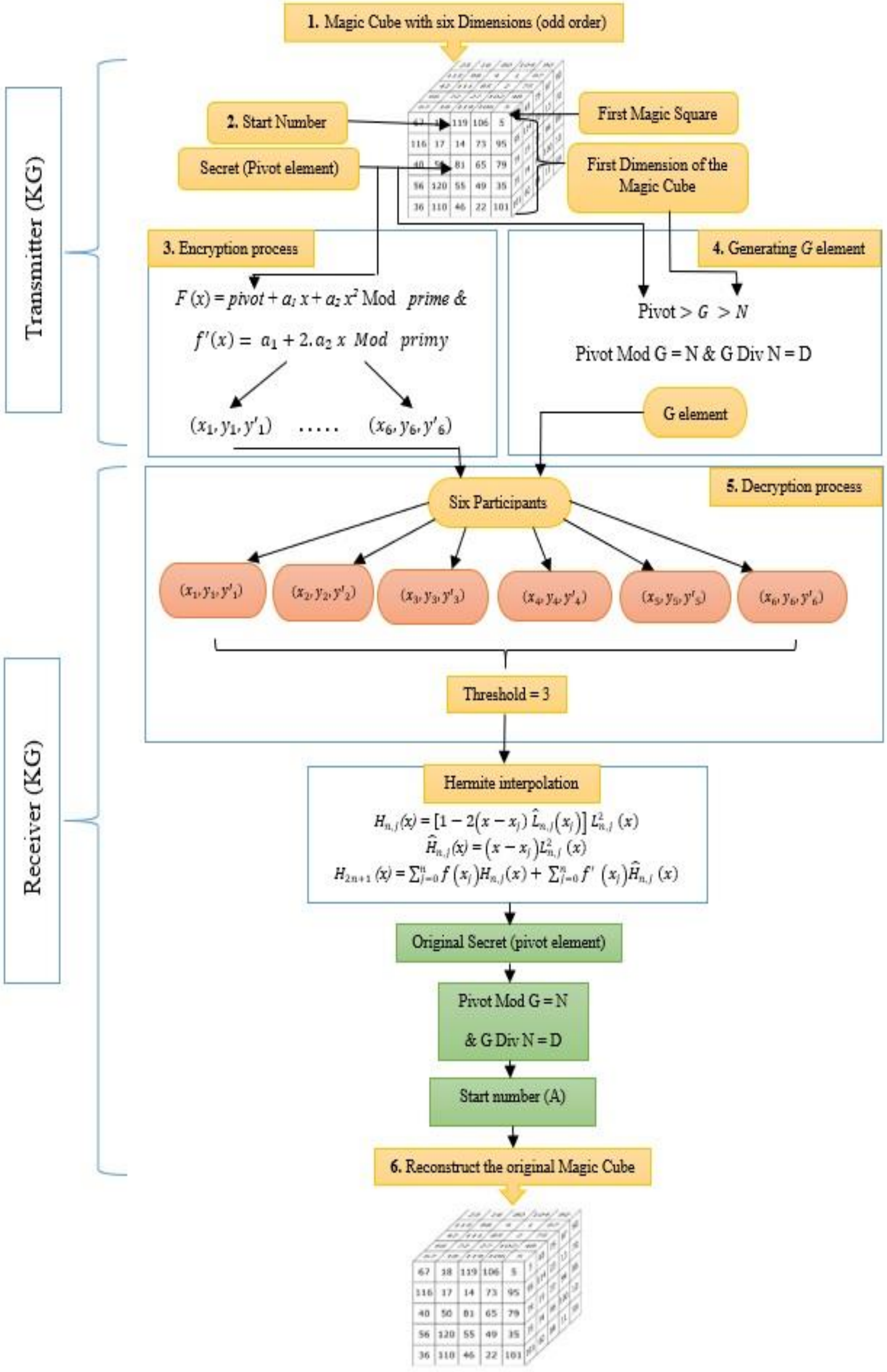

1. Magic Cube with six Dimensions (odd order)
Transmitter (KG)
2. Start Number
Secret (Pivot element)
First Magic Square
First Dimension of the Magic Cube
3. Encryption process
$F(x) = pivot + a_1 x + a_2 x^2$ Mod prime &
$f'(x) = a_1 + 2.a_2\,x$ Mod primy
(x_1, y_1, y'_1) ..... (x_6, y_6, y'_6)
4. Generating G element
Pivot > G > N
Pivot Mod G = N & G Div N = D
G element
Receiver (KG)
5. Decryption process
Six Participants
(x_1, y_1, y'_1)
(x_2, y_2, y'_2)
(x_3, y_3, y'_3)
(x_4, y_4, y'_4)
(x_5, y_5, y'_5)
(x_6, y_6, y'_6)
Threshold = 3
Hermite interpolation
$H_{n,j}(x) = [1 - 2(x - x_j)\,\hat{L}_{n,j}(x_j)]\,L^2_{n,j}(x)$
$\hat{H}_{n,j}(x) = (x - x_j)L^2_{n,j}(x)$
$H_{2n+1}(x) = \sum_{j=0}^{n} f(x_j)H_{n,j}(x) + \sum_{j=0}^{n} f'(x_j)\hat{H}_{n,j}(x)$
Original Secret (pivot element)
Pivot Mod G = N & G Div N = D
Start number (A)
6. Reconstruct the original Magic Cube
67 18 119 106 5
116 17 14 73 95
40 50 81 65 79
56 120 55 49 35
36 110 46 22 101

Figure 3.6 Second Proposed Algorithm (Secret Sharing with Magic Cube using Hermite Interpolation)

3.4 Third Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)

The main objective beyond the proposed method is to maintain the exchanging confidential information between the dealer and subscribers. The proposed method imposed that the share information must be strictly trusted and integrated. The transferred dimension to a group of trusted subscribers will move the characteristics of the original magic cube to all groups.

The proposed method can be described to explain each part for the dealer and subscribers' side. A magic cube is chosen with *n* dimensions that are considered secret where (secret = a_0 = order) under the polynomial equation. This selected magic cube consists of six magical squares with any ($n*n$) dimension (odd, doubly and singly even order). When selecting the dimensions (N) of the magic cube, the factorial is computed for the dimension (Fact (N)) to deduce the magic cube starting value (A), as shown in equation (3.14) bellow:

$$\text{Factorial } (N) = A \qquad \dots (3.14)$$

Thereafter, the power for the dimension (Power (N)) is computed to obtain the magic cube and the difference (D) value between the numbers of the magic cube, as shown in equation (3.15):

$$\text{Power } (N) = D \qquad \dots (3.15)$$

After concluding the basic properties of Magic Cube (N, A and D) which will be compatible with the required confidential information provided by dealer and subscribers, the dimensions (N) of the magic cube will be the (secret) within the polynomial to get points (x_i , y_i) and then send them to the participants as shown in equation (3.22).

$$F(x) = (\text{order}) + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1} \quad \text{mod} \quad prime \qquad \dots (3.16)$$

When points are received by subscribers, Lagrange interpolation is used to reconstruct the secret (order) as stated in the mathematical equations (3.4, 3.5, 3.6, and 3.7).

When the participants get the secret (dimensions) of the original magic cube, they will calculate the factorial value for the cube-dimension (N) to get the start element (A), and then calculate the power for the cube-dimension to get the Difference (D) between the numbers of the magic cube. All participants will have the dimension value and difference value for the magic cube and consequently they will be able to conclude the start value easily as shown in equation (3.8).

The participants can reconstruct the original magic cube and compute the pivot element easily, as shown in equation (3.17). The pivot element (*P*) can also be deduced if the magic cube is (odd order). Thus, the magic constant (*MC*) and the magic sum (*MS*) of the magic cube can be calculated according the following mathematical equations (3.18) and (3.19):

$$\text{Pivot } (P) = \frac{(2*A) + D*(N^2 - 1)}{2} \qquad \ldots (3.17)$$

$$\text{Magic Constant } (MC) = N*(\frac{(2*A) + D*(N^2 - 1)}{2}) \qquad \ldots (3.18)$$

$$\text{Magic SUM } (MS) = \text{Magic Constant } (MC)* \text{ Order } (N) \qquad \ldots (3.19)$$

The proposed method increased the computational complexities for the reconstruction process. The introduced algorithm requires additional effective parameters of magic cube to rebuild the secret properly. The proposed approach involves various mathematical comprehensions that require more mathematical computational effort. These extra simple operations include the folded magic cube reconstruction, factorial operation, and power computation in addition to secret reassembling. figure (3.9) below shows the main stages for the proposed algorithm.

Algorithm 3.3 Third Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)

Input: order, random coefficients (a_k), variable (x^k), modular reduction (prime number).
Output: secret (order).

1) Initialization of Algorithm

a- Choose a specific dimension for the magic cube (odd, singly or Doubly even order).

b- Apply the Factorial to the dimensions (*N*) of the magic cube to obtain the starting number (*A*).

c- Apply the power to the dimensions (*N*) of the magic cube to get the difference (*D*) between the numbers of the magic cube.

2) Preprocessing Constructing Magic Cube (odd, singly or doubly even order)

a- Build the magic cube by starting number (*A*), magic cube dimensions (*N*), and

the difference (D) between the magic cube numbers.
3) Transmitter Key Generation (KG)
a- Choose the magic cube order to be (secret) within the polynomial, as shown in equation (3.16). b- Conclude six points of polynomial. c- Send points to six trusted subscribers. d- Determine the Threshold value.
4) Receiver Key Generation (KG)
a- Reconstruct the secret again by a specified number of subscribers (Threshold) to get the original magic cube order (N) via Lagrange Interpolation. b- Cube dimensions (N) are the secret, (secret = a_0 = order). c- Compute equation (3.14) of the magic cube. d- Compute equation (3.15) of the magic cube.
5) Reconstructing Magic Cube
b- Reconstruct the original magic cube through the characteristics obtained by the participants. c- Calculate the magic constant (MC) of the magic cube by equation (3.18). d- Calculate the magic sum (MS) of the magic cube by equation (3.19). e- Calculate the pivot element of (odd order) magic cube by equation (3.17).

Example:

Assume that there is a magic cube of (doubly even order) that consists of six magical square arrays. The factorial mathematical operation is taken for magic cube dimension (N) to get the starting number (A) in magic cube construction. Additionally, the power mathematical operation is computed for the dimension (N) value in order to determine the difference (D) values between the numbers of the magic cube, as illustrated in Figure (3.7). The main parameters can be determined as follows:

The cube dimension with fourth order of $n*n$ = 4*4*4*4*4*4.

Factorial (4) = 24, the start number (A) of the magic cube is = 24

Power (4) = 16, the difference (D) between the numbers of the magic cube is = 16.

264	**40**	**56**	**206**
88	**184**	**168**	**136**
152	**120**	**104**	**200**
72	**232**	**248**	**24**

1st Square

520	**296**	**312**	**472**
344	**440**	**424**	**392**
408	**376**	**360**	**456**
328	**488**	**504**	**280**

2nd Square

776	**552**	**568**	**728**
600	**696**	**680**	**648**
664	**632**	**616**	**712**
584	**744**	**760**	**536**

3rd Square

1032	**808**	**824**	**984**
856	**952**	**936**	**904**
920	**888**	**872**	**968**
840	**1000**	**1016**	**792**

4th Square

1288	**1064**	**1080**	**1240**
1112	**1208**	**1192**	**1160**
1176	**1144**	**1128**	**1224**
1096	**1256**	**1272**	**1048**

5th Square

1544	**1320**	**1336**	**1496**
1368	**1464**	**1448**	**1416**
1432	**1400**	**1384**	**1480**
1352	**1512**	**1528**	**1304**

6th Square

Dimension = 4, Difference = 16, Start number = 24

Figure 3.7 Doubly Even Magic Cube

Select the magic cube of fourth order to be the (secret) within the polynomial, and then select the other parameters randomly within the polynomial, as shown in equation (3.16). The magic cube properties are represented in the Shamir's secret sharing scheme:

Where n = participants, k = threshold, d = difference.

$n = 6$, $k = 3$, $p = 19$, $p > s$ and $p > n$.

$$F(x) = 4 + 9\text{ x} + 13\text{ x}^2 \quad \text{mod} \quad 19$$

Six points of the polynomial are computed, concluded and sent to six trusted subscribers (n) by the dealer, as illustrated in table (3.3) bellow.

Table 3.3 Generated Points of 3rd Algorithm According to (x) And (f (x)) axes

(*x*)	***F* (*x*)**	**Points (*x*, *f* (*x*))**
1	7	(1, 7)
2	17	(2, 17)
3	15	(3, 15)
4	1	(4, 1)
5	13	(5, 13)
6	13	(6, 13)

The dealer will determine the allowed threshold computation that the participants will need for reconstructing the secret properly. The dealer will distribute the six polynomial points among six subscribers. According to the threshold idea, any three of the six participants ($k = 3$) will be able to reconstruct the secret (order):

To prove that, choose three polynomial points as follows:

$$D_0 = (1, 7),\ D_1 = (2, 17),\ D_2 = (3, 15)$$

Compute the Lagrange interpolation using equations (3.4, 3.5, 3.6, and 3,7):

$$\frac{1}{2}x^2 - \frac{5}{2}x + 3$$

$$-\ x^2 + 4x - 3$$

$$\frac{1}{2}x^2 - \frac{3}{2}x + 1$$

Therefore, the original secret is (4).

After obtaining the (order = 4), it is possible to compute the factorial and the power to (4) using equations (3.14) and (3.15):

The order of the magic cube is = 4

Factorial (4) = 24, the start number (A) of the magic cube is = 24.

Power (4) = 16, the difference (D) between the numbers of the magic cube is = 16.

The conclusion of order, difference and start number of the original magic cube, the magic constant (MC) and the magic sum (MS) can be obtained by using equations (3.18) and (3.19).

The six participants can reconstruct the original (Doubly even order) magic cube, as illustrated in Figure (3.8).

264	40	56	206
88	184	168	136
152	120	104	200
72	232	248	24

1st Square

520	296	312	472
344	440	424	392
408	376	360	456
328	488	504	280

2nd Square

776	552	568	728
600	696	680	648
664	632	616	712
584	744	760	536

3rd Square

1032	808	824	984
856	952	936	904
920	888	872	968
840	1000	1016	792

4th Square

1288	1064	1080	1240
1112	1208	1192	1160
1176	1144	1128	1224
1096	1256	1272	1048

5th Square

1544	1320	1336	1496
1368	1464	1448	1416
1432	1400	1384	1480
1352	1512	1528	1304

6th Square

Figure 3.8 The Reconstructed Magic Cube

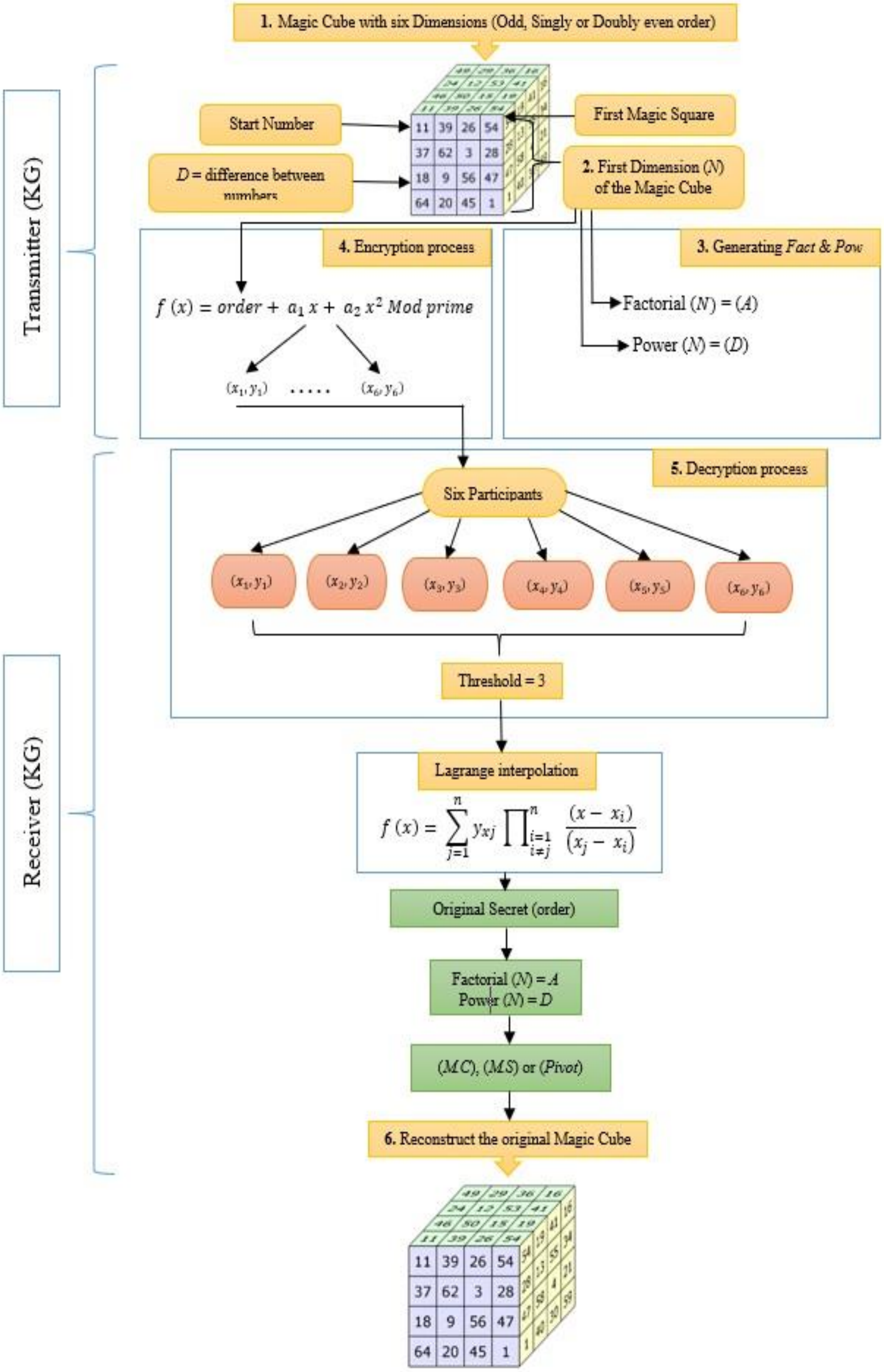


Figure 3.9 Third Proposed Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)

3.5 Fourth Proposed Algorithm (Secret Sharing with Magic Cube using Newton Divided Difference Interpolation)

A magic cube is chosen with *n* dimensions that are considered secret where (secret = a_0 = order) under the polynomial equation. This selected magic cube consists of six magical squares with any (*n*n*) dimension (odd, doubly and singly even order). When selecting the dimensions (*N*) of the magic cube, the factorial is computed for the dimension (Fact (*N*)) to deduce the magic cube starting value (*A*), as shown un equation (3.14).

Thereafter, the power for the dimension (Power (*N*)) is computed to obtain the magic cube and the difference (*D*) value between the numbers of the magic cube, as illustrate in equation (3.15).

After concluding the basic properties of Magic Cube (*N*, *A* and *D*) which will be compatible with the required confidential information provided by dealer and subscribers, the dimensions (*N*) of the magic cube will be the (secret) within the polynomial to get points (x_i , y_i) and then send them to the participants as shown in equation (3.16).

When points are received by subscribers, Newton's Divided Difference Interpolation Formula is used to reconstruct the secret (order) as stated in the following mathematical equations (3.20, 3.21, 3,22, and 3,23):

$$x_0 \quad f(x_0)$$

$$\frac{f(x_1) - f(x_0)}{x_1 - x_0} \qquad \dots (3.20)$$

$$x_1 \quad f(x_1) \qquad \frac{\frac{f(x_2) - f(x_1)}{x_2 - x_1} - \frac{f(x_1) - f(x_0)}{x_1 - x_0}}{x_2 - x_1} \qquad \dots (3.21)$$

$$\frac{f(x_2) - f(x_1)}{x_2 - x_1} \qquad \dots (3.22)$$

$$x_2 \quad f(x_2) \qquad \vdots$$

$$\vdots$$

$$\vdots \qquad \vdots$$

$$\vdots$$

$x_n \quad f(x_n)$

$$f(x) = f[x_0] + (x - x_0)\ f[x_0,x_1] + (x - x_0)\ (x - x_1)\ f[x_0,x_1,x_2] + \dots + (x - x_0)(x - x_1)\dots(x - x_{k-1}) f[x_0,x_1,\dots,x_{k-1}] \qquad \dots(3.23)$$

When the participants get the secret (dimensions) of the original magic cube, they will calculate the factorial value for the cube-dimension (*N*) to get the start element (*A*), and then calculate the power for the cube-dimension to get the Difference (*D*) between the numbers of the magic cube. All participants will have the dimension value and difference value for the magic cube and consequently they will be able to conclude the start value easily as shown in equation (3.8).

The participants can reconstruct the original magic cube and compute the pivot element easily. The pivot element (*P*) can also be deduced if the magic cube is (odd order). Thus, the magic constant (*MC*) and the magic sum (*MS*) of the magic cube can be calculated according to the mathematical equations (3.13, 3.18, and 3,19). The proposed method increased the computational complexities for the reconstruction process. The introduced algorithm requires additional effective parameters of magic cube to rebuild the secret properly. The proposed approach involves various mathematical comprehensions that require more mathematical computational effort. These extra simple operations include the folded magic cube reconstruction, factorial operation, and power computation in addition to secret reassembling. Figure (3.13) below shows the main stages for the proposed algorithm.

Algorithm 3.4 Fourth Proposed Algorithm (Secret Sharing with Magic Cube using Newton Divided Difference Interpolation)

Input: order, random coefficients (a_k), variable (x^k), modular reduction (prime number).

Output: secret (order).

1) Initialization of Algorithm

a- Choose a specific dimension for the magic cube (odd, singly or Doubly even order).

b- Apply the Factorial to the dimensions (*N*) of the magic cube to obtain the starting number (*A*).

c- Apply the power to the dimensions (*N*) of the magic cube to get the difference (*D*) between the numbers of the magic cube.

2) Preprocessing Constructing Magic Cube (odd, singly or doubly even order)

a- Build the magic cube by starting number (*A*), magic cube dimensions (*N*), and the difference (*D*) between the magic cube numbers.

3) Transmitter Key Generation (KG)

b- Choose the magic cube order to be (secret) within the polynomial, as illustrate in equation (3.16).

c- Conclude six points of polynomial.

d- Send points to six trusted subscribers.

e- Determine the Threshold value.

4) Receiver Key Generation (KG)

a- Reconstruct the secret again by a specified number of subscribers (Threshold) to get the original magic cube order (*N*) via Newton's Divided Difference Interpolation Formula.

b- Cube dimensions (*N*) are the secret, (secret = a_0 = order).

c- Compute equation (3.14) of the magic cube.

d- Compute equation (3.15) of the magic cube.

5) Reconstructing Magic Cube

a- Reconstruct the original magic cube through the characteristics obtained by the participants.

b- Calculate the magic constant (*MC*) of the magic cube through equation (3.18).

c- Calculate the magic sum (*MS*) of the magic cube through equation (3.19).

d- Calculate the pivot element of (odd order) magic cubes through equation (3.17).

Example:

Assume that there is a magic cube of (singly even order) that consists of six magical square arrays. The factorial mathematical operation is taken for magic cube dimension (*N*) to get the starting number (*A*) in magic cube construction. Additionally, the Power mathematical operation is computed for the dimension (*N*) value in order to determine the difference (*D*) values between the numbers of the magic cube, as illustrated in Figure (3.10). The main parameters can be determined as follows:

The cube dimension with fourth order of $n*n$ = 6*6*6*6*6*6.

Factorial (6) = 720, the start number (*A*) of the magic cube is = 720.

Power (6) = 36, the difference (*D*) between the numbers of the magic cube is = 36

1944	720	900	1620	1368	1548
792	1836	936	1440	1512	1584
1800	1008	756	1476	1656	1404
972	1692	1872	1296	1044	1224
1764	864	1908	1116	1188	1260
828	1980	1728	1152	1332	1080

1st square

3240	2016	2196	2916	2664	2844
2088	3132	2232	2736	2808	2880
3096	2304	2052	2772	2952	2700
2268	2988	3168	2592	2340	2520
3060	2160	3204	2412	2484	2556
2124	3276	3024	2448	2628	2376

2nd square

4536	3312	3492	4212	3960	4140
3384	4428	3528	4032	4104	4176
4392	3600	3348	4068	4248	3996
3564	4284	4464	3888	3636	3816
4356	3456	4500	3708	3780	3852
3420	4572	4320	3744	3924	3672

3rd square

5832	4608	4788	5508	5256	5436
4680	5724	4824	5328	5400	5472
5688	4896	4644	5364	5544	5292
4860	5580	5760	5184	4932	5112
5652	4752	5796	5004	5076	5148
4716	5868	5616	5040	5220	4968

4th Square

7128	5904	6084	6804	6552	6732
5976	7020	6120	6624	6696	6768
6984	6192	5940	6660	6840	6588
6156	6876	7056	6480	6228	6408
6948	6048	7092	6300	6372	6444
6012	7164	6912	6336	6516	6264

5th Square

8424	7200	7380	8100	7848	8028
7272	8316	7416	7920	7992	8064
8280	7488	7236	7956	8136	7884
7452	8172	8352	7776	7524	7704
8244	7344	8388	7596	7668	7740
7308	8460	8208	7632	7812	7560

6th Square

Dimension = 6, Difference = 36, Start number = 720

Figure 3.10 Singly Even Magic cube

Select the magic cube of sixth order to be the (secret) within the polynomial, and then select the other parameters randomly within the polynomial, as shown in equation (3.16). The magic cube properties are represented in the Newton's Divided Difference Interpolation Formula:

Where *n* = participants, *k* = threshold, *d* = difference.

$n = 6$, $k = 3$, $p = 11$, $p > s$ and $p > n$.

$$F(x) = 6 + 8\,x + 5\,x^2 \quad \text{mod} \quad 11$$

Six points of the polynomial are computed, concluded and sent to six trusted subscribers (*n*) by the dealer, as illustrated in table (3.4).

Table 3.4 Generated Points of 4th Algorithm According to (*x*) And (*f* (*x*)) axes

(*x*)	***F* (*x*)**	**Points (*x*, *f* (*x*))**
1	8	(1, 8)
2	9	(2, 9)
3	9	(3, 9)
4	8	(4, 8)
5	6	(5, 6)
6	3	(6, 3)

The dealer will determine the allowed threshold computation that the participants will need for reconstructing the secret properly. The dealer will distribute the six polynomial points among six subscribers. According to the threshold idea, any three of the six participants (k = 3) will be able to reconstruct the secret (order):

To prove that, choose three polynomial points as follows:

$$D_0 = (2, 9), \quad D_1 = (4, 8), \quad D_2 = (6, 3)$$

Compute the Newton's Divided Difference Interpolation using equations (3.20, 3.21, 3.22, and 3.23):

$$\frac{8-9}{4-2} = -\,0.5$$

$$\frac{-\,0.5+2.5}{6-2} = -\,0.5$$

$$\frac{3-8}{6-4} = -\,2.5$$

Finally,

$$f(x) = [9] + (x - 2)\,[-\,0.5] + (x - 2)\,(x - 4)\,[-\,0.5] = 6$$

Therefore, the original secret is (6).

After obtaining the (order = 6), it is possible to compute the factorial and the power to (6):

The order of the magic cube is = 6

Factorial (6) = 720, the start number (*A*) of the magic cube is = 720.

Power (6) = 36, the difference (*D*) between the numbers of the magic cube is = 36.

The conclusion of order, Difference and Start number of the original magic cube, the magic constant (*MC*) and the magic sum (*MS*) can be obtained by using equations (3.18) and (3.19).

The six participants can reconstruct the original (Singly even order) magic cube, as illustrated in Figure (3.11).

1944	720	900	1620	1368	1548
792	1836	936	1440	1512	1584
1800	1008	756	1476	1656	1404
972	1692	1872	1296	1044	1224
1764	864	1908	1116	1188	1260
828	1980	1728	1152	1332	1080

1st square

3240	2016	2196	2916	2664	2844
2088	3132	2232	2736	2808	2880
3096	2304	2052	2772	2952	2700
2268	2988	3168	2592	2340	2520
3060	2160	3204	2412	2484	2556
2124	3276	3024	2448	2628	2376

2nd square

4536	3312	3492	4212	3960	4140
3384	4428	3528	4032	4104	4176
4392	3600	3348	4068	4248	3996
3564	4284	4464	3888	3636	3816
4356	3456	4500	3708	3780	3852
3420	4572	4320	3744	3924	3672

3rd square

5832	4608	4788	5508	5256	5436
4680	5724	4824	5328	5400	5472
5688	4896	4644	5364	5544	5292
4860	5580	5760	5184	4932	5112
5652	4752	5796	5004	5076	5148
4716	5868	5616	5040	5220	4968

4th Square

7128	5904	6084	6804	6552	6732
5976	7020	6120	6624	6696	6768
6984	6192	5940	6660	6840	6588
6156	6876	7056	6480	6228	6408
6948	6048	7092	6300	6372	6444
6012	7164	6912	6336	6516	6264

5th Square

8424	7200	7380	8100	7848	8028
7272	8316	7416	7920	7992	8064
8280	7488	7236	7956	8136	7884
7452	8172	8352	7776	7524	7704
8244	7344	8388	7596	7668	7740
7308	8460	8208	7632	7812	7560

6th Square

Figure 3.11 The Reconstructed Singly Even Magic Cube

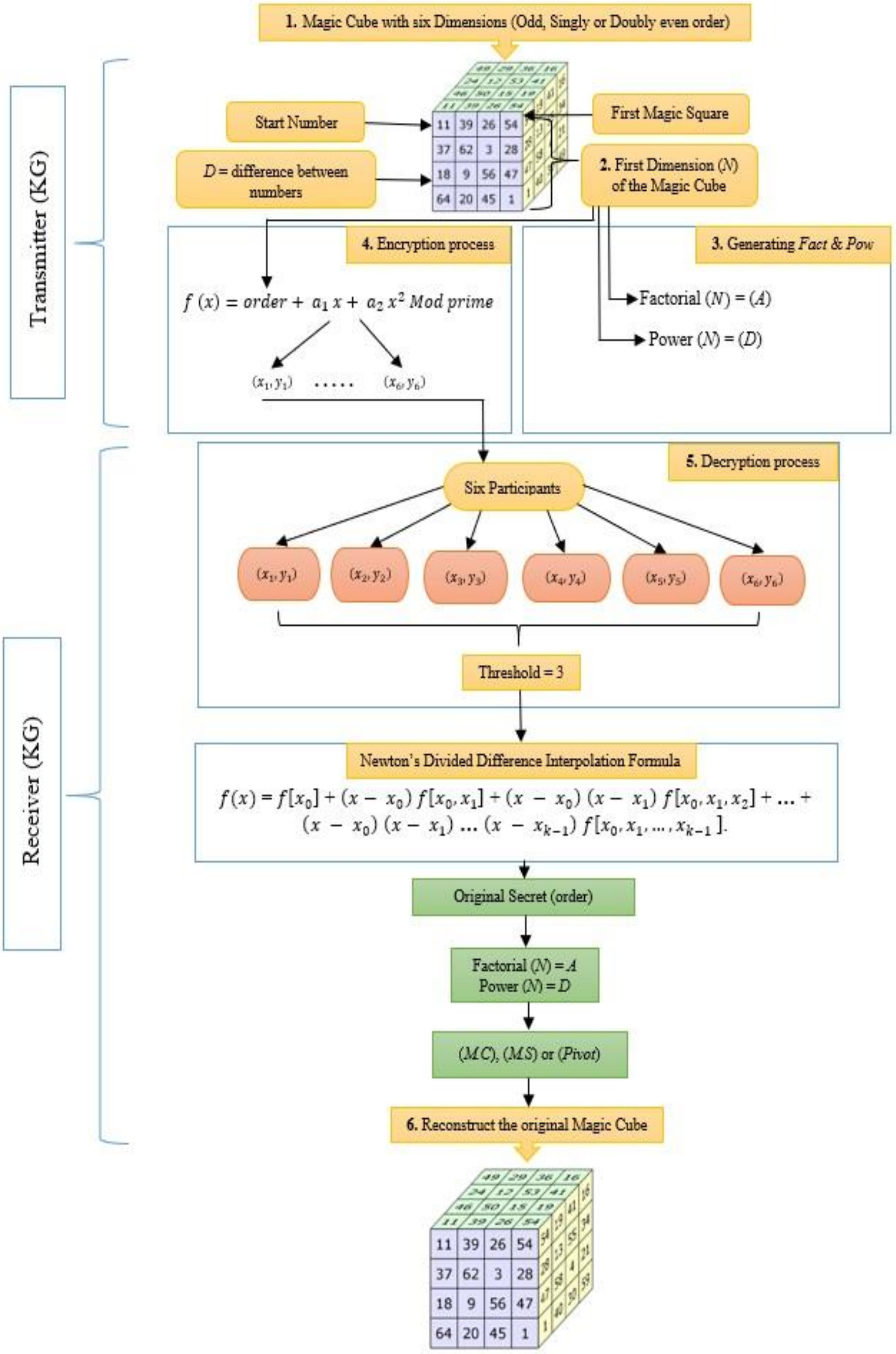


Figure 3.12 Fourth Proposed Algorithm (Secret Sharing with Magic Cube using Newton Divided Difference Interpolation)

In the four proposed algorithms three types of magic cubes were used. Three mathematical methods of numerical analysis were used to protect the secret keys. Below is a table (3.5) showing the characteristics of the four proposed algorithms.

Table 3.5. Comparison among the Proposed Algorithms According to (Secret Sharing and Magic Cube Properties)

M.C Type	Construction Type	Smallest Possible Order	Dimension	*M.C* Order	Secret Sharing Points	Secret Sharing Threshold	Numerical Analysis Method
Odd	Math	3-Order	Folding 6-D	5	6-points	K = 3	Lagrange Interpolation
Odd	Math	3-Order	Folding 6-D	5	6-points	K = 3	Hermite Interpolation
Doubly Even	Math	4-Order	Folding 6-D	4	6-points	K = 3	Lagrange Interpolation
Singly Even	Math	6-Order	Folding 6-D	6	6-points	K = 3	Divided Difference Interpolation

According to above table the second algorithm has many qualities which makes it the best algorithm to be suggested in this chapter. These qualities are the Hermite interpolation method has great complexities to protect confidential information. In addition to the derivative used in this method where the stages of complexity and calculations necessary to rebuild the secret keys by users. As will as the complexity added by (G element) in the algorithm which in case of loss or stolen of this element no one can benefit from stealing it as long as the secret key is unknown to the cryptanalyst.

Chapter Four

Results and Analysis

Chapter Four

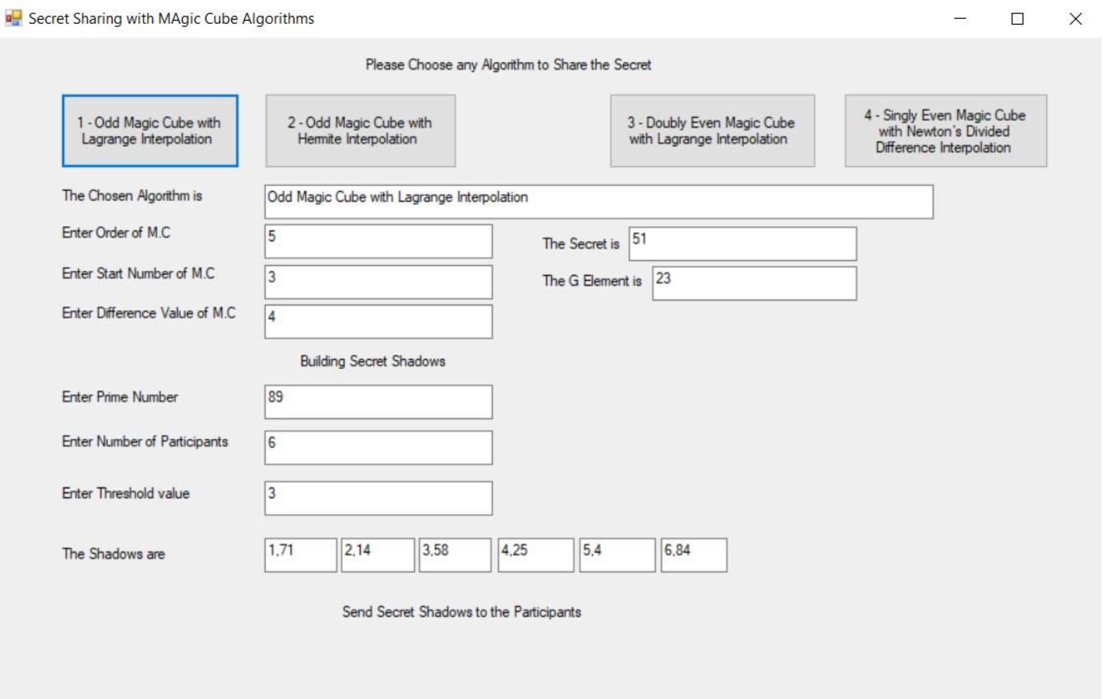
Results and Analysis

4.1 Introduction

The implemented secret sharing algorithms rely on the interaction between the secret sharing algorithm and the unique properties possessed by magic cubes and the mathematical processes among them. The main idea of the implemented algorithms was based on increasing the complexity of the properties provided by magic cube properties to preserve confidential information and to resist any risks related to harmful attacks and security aspects. The design of the implemented algorithms is based on providing a high degree of security for the secret keys between the dealer and the trusted subscribers. Therefore, in this chapter the analysis of confidentiality, advantages, limitations and applications of the implemented algorithms will be examined.

4.2 Graphical User Interface (GUI)

This study is designed by simple graphical interfaces that allow the user to choose one of the implemented algorithms and use them in the process of managing secret keys. In addition, the user is given the freedom to choose one of the mathematical numerical analysis methods (Lagrange, Hermite, Divided difference) for the purpose of sharing the secret. The dimensions of the magic cube, which is built by the user if it is (odd, singly or double even), which contains all the confidential and sensitive information, can also be chosen easily. The secret sharing algorithms implemented in this study designed by Microsoft Visual Studio 2017 (C sharp language) include a graphic environment in order to make it easier for the user to select and use the appropriate algorithm, as illustrate in figures (4.1, and 4.2). Computer specification used in programming algorithms (processor core (TM) i7-77HQ CPU @ 2.80 GHz, Ram 16.0 GB, 64 bit-Operating system, HD 1TB, windows10, and 4GB VGA). This design includes all the necessary mathematical operations in addition to the methods of creating magic cubes in all their dimensions, as well as all numerical analysis methods that have been used.


Secret Sharing with MAgic Cube Algorithms
Please Choose any Algorithm to Share the Secret
1 - Odd Magic Cube with Lagrange Interpolation
2 - Odd Magic Cube with Hermite Interpolation
3 - Doubly Even Magic Cube with Lagrange Interpolation
4 - Singly Even Magic Cube with Newton's Divided Difference Interpolation
Building Secret Shadows
Send Secret Shadows to the Participants

The Chosen Algorithm is: Odd Magic Cube with Lagrange Interpolation

Enter Order of M.C: 5

Enter Start Number of M.C: 3

Enter Difference Value of M.C: 4

The Secret is: 51

The G Element is: 23

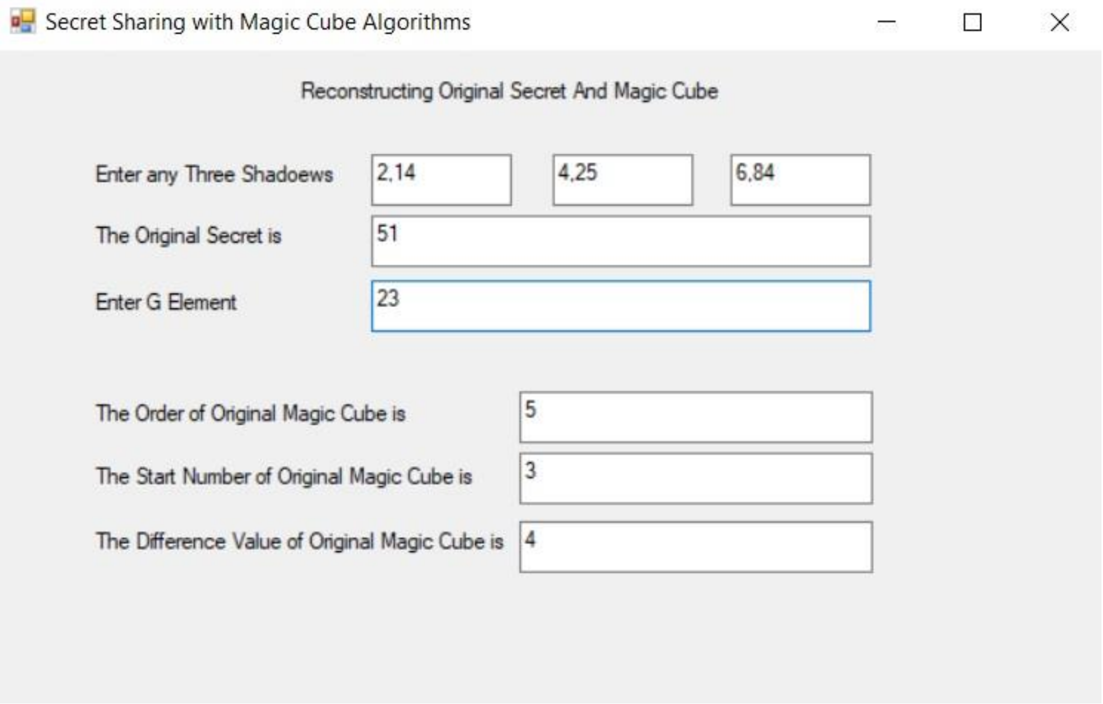
Enter Prime Number: 89

Enter Number of Participants: 6

Enter Threshold value: 3

The Shadows are: 1,71 | 2,14 | 3,58 | 4,25 | 5,4 | 6,84

Figure 4.1. Secret Sharing with Magic Cube algorithms (Building the Secret Keys)


Secret Sharing with Magic Cube Algorithms
Reconstructing Original Secret And Magic Cube

Enter any Three Shadoews: 2,14 | 4,25 | 6,84

The Original Secret is: 51

Enter G Element: 23

The Order of Original Magic Cube is: 5

The Start Number of Original Magic Cube is: 3

The Difference Value of Original Magic Cube is: 4

Figure 4.2. Secret Sharing with Magic Cube algorithms (Rebuilding the Secret Keys)

4.3 The Analysis of Interpolation Methods

Each method of numerical analysis has a set of characteristics that distinguishes it from other methods. Therefore, Lagrange interpolation requires very large computation operations and its use can be risky. Lagrange interpolation greatly increases the problem of finding coefficients so it only takes (linear time) to find these coefficients. This is good for Lagrange interpolation if they need the same set of points in frequently manner, but this process does not benefit in the case of repeated the calculations more than once. In other words, Lagrange interpolation is much better when many information sets have to be made on the same data points. Often, Lagrange interpolation is a theoretical tool used to prove theorems, because it is ineffective when adding a new point (which requires calculating the boundary many times again, from zero) and is also numerically unstable.

In contrast to the Lagrange Interpolation, Newton divided difference formula is much more efficient because it does not require very large calculations, the coefficients can be obtained at a reasonable rate square time and the evaluations are more stable. The fact that there is no need to re-calculate the evaluations for many of the interpolation, made Newton divided difference formula more efficient than the Lagrange Interpolation. In the sense that if new point is added to the calculations, it is not required to return the calculation from zero, but calculate the new point only, so it is stable numerically and effectively from the point of calculation.

Newton divided difference formula does not require a long-time calculation or prior knowledge of the number of points in the solution so it is more efficient and useful than Lagrange Interpolation.

Returning to Hermite interpolation, it possesses characteristics no less than its counterparts (Lagrange and Newton divided difference) because it possesses a double computational complexity that exists in both previous ways because it contains (derivative of polynomial and points), so it strengthens exists in its derivatives. Without an existing derivative result, no solutions can be made to arithmetic operations so the process of reconstructing the secret is twice as complicated as the previous two methods. Hermite interpolation provides double protection for confidential information and has the highest accuracy in analysis and arithmetic complexity over Lagrange interpolation.

All the previously methods are using the same number of (coefficients) and it deal with points (equal and unequal) dimension. Through the characteristics mentioned above, the user is shown the most efficient way suitable to his work from the three-interpolation mentioned to be used in the applications of share sharing. Through the characteristics mentioned for each of the previous three numerical analysis methods which uses the same number of (coefficients) and it deal with points (equal and unequal) dimension.

4.4 Security Analysis for the Implemented Secret Sharing Algorithms

The implemented algorithms are based on finding suitable and useful solutions to mathematical problems facing the secret sharing algorithms to maintaining confidential information. Therefore, all algorithms are designed to provide a level of safety and high efficiency. This part of the study will include the analytical aspects of the security of implemented secret sharing algorithms.

4.4.1 The Security Analysis of The First Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)

The introduced method is the result of merging two completely different mathematical foundations. The proposed method is adopted to apply high degree of confidentiality for trusting the information sharing and managing. Basically, the building of $N*N$ magic cube depends on an odd order of folded magic square with six dimensions. The magic cube construction requires several impact parameters such as (Dimension, Pivot element, Difference Value and the Start Value). These parameters have a vital role in the reconstruction process of the magic cube secret scheme.

The efficiency of the implemented system depends on how to transfer the properties of the magic cubes by sharing the secret (pivot element) among a group of trusted subscribers. The reliability and the efficiency of the implemented method faded away the security concerns about distribution the secret on untrusted server. The mixture of magic cube mathematical base and the Lagrange interpolation mathematical problem introduces high mathematical complexity.

The strength of the mathematical complexity will prevent the attacker or intruder from revealing any information about the polynomial equation or magic cube parameters. Thus, since the attacker will need sufficient information for reconstructing the magic cube or rebuilding the secret, he tries to disclose the magic cube parameters throughout the leakage information from the interpolation equation. The attacker will need to know at least three parameters from four unknown parameters in order to recover the secret. This means the implemented method gives another security layer for the secret scheme which is ultimately strong and secret. However, it is easy to alter all the parts (or even *k*) without modifying the secret and without discovering any information about the secret. The replacement or alteration process is occurred through the selection of a new Lagrange interpolation polynomial *f* (*x*) and a new set of participants (shares).

Therefore, in the event of loss or theft part of this confidential information, it will be impossible to retrieve the secret key. Put differently, if the shares are less than (*k*-threshold), it will be very hard to rebuild the secret key and to reconstruct the original magic cube. The magic cube comprehension provides an additional security layer that requires high estimation probability and high guessing strategy with a large search space. Since the attacker has to predicate the correct dimension and the first value (starting number) for the building magic cube, he or the cryptanalyst also will need the amount of consecutive difference value between the numbers. The process of merging magic cubes with (secret sharing) provides more reliability and efficiency.

The submitted method is perfectly secure and gives a robust idea to distribute the properties of the magic cube to a group of trusted subscribers. Finally, the participants will try to get the secret (pivot element) from the Lagrange interpolation equation then reconstruct magic cube properly. The implemented method doesn’t give any leakage information for the pivot element or secret coefficients. Thus; it can resist any attempts to predict the secret or computing the polynomial coefficients of degree (*k*-1).

4.4.2 The Security Analysis of The Second Algorithm (Secret Sharing with Magic Cube using Hermite Interpolation)

The implemented algorithm is produced by mixing mathematical properties of the secret sharing with the mathematical properties of magic cubes. This algorithm was implemented for the purpose of providing the highest degree of protection for confidential information transmitted over internet networks. A magic cube (odd order) composed of $N*N$ was built. The mathematical properties of magic cubes play a major role in the process of protecting sensitive information through impact parameters required to construct any magic cube (start number, difference value, dimension, pivot element).

The efficiency of this algorithm depends on how the mathematical properties of the magic cubes are transferred by the secret sharing. The (Pivot Element) plays an important role in this process, because it will be considered a secret and embedded in the polynomial and transferred to a group of trusted participants.

The use of Hermite Interpolation in the process of the secret sharing with the mathematical properties of Magic Cubes has been added dramatically mathematical complexity to the algorithm. Hermite interpolation made the derivative of the polynomial and then sends all points with their derivatives to subscribers through confidential communication channels. After the trusted participants have obtained the points and their derivatives, the original secret (pivot element) is reconstructed to obtain the mathematical properties of the original magic cube to rebuild it.

The mathematical complexity provided by the derivative may be complex relative to the trusted participants during the reconstruction of the original secret, but this complexity will provide significant protection for confidential information against any risk by adversaries and unauthorized subscribers. Integrating the mathematical complexity provided by Hermite interpolation with the mathematical properties of Magic Cube will be a major obstacle to any cryptanalyst trying to predict secret key parts. In addition, the opponent must get all the magic cube's parameters (start number, difference value, dimension, pivot element) so that he can rebuild it to get the secret information.

4.4.3 The Security Analysis of The Third Algorithm (Secret Sharing with Magic Cube using Lagrange Interpolation)

In the implemented study, a high degree of confidentiality has been applied to protect information by integrating two different algorithms of magic cube reconstruction algorithm and secret sharing algorithm. The process of building magic cubes depends on complex techniques, and these techniques give a powerful magic cube construction against any malicious activity. This study is based on how to transfer the properties of magic cubes to a group of trusted participants during the secret sharing process. The confidentiality of information is an important part that is offered by complex mathematical relationships in magic cubes. The magic cube characteristics give additional secure layer against the active attacks.

This complexity relies on hiding the dimension cube via the interpolation polynomial equation. This notation prevents the intruder from knowing the dimensions of the magic cube, the starting number or even the amount of difference value among the magic cube numbers. The process of integrating magic cubes with a sharing secret provides great challenge in key management protocols. Furthermore; the preservation of confidential information by distributing the properties of the magic cube to a group of trusted subscribers acts a real difficulty. The implemented algorithm produced several secure layers of computational complexity that require high potential analysis.

It embedded the magic cube construction in the secret value to facilitate the reconstruction process of the magic cube dimensions on the part of participants. Thus, the implemented system resists any attempts by cryptanalyst to predict the magic cube dimensions, the starting number, or the difference value between the elements or any parameter. In this respect, the intruder tries to get some leakage information to deduce the secret value and consequently discovers the dimension of magic cube. In this sense, the factorial and power computation increase the protection stages, because it will increase the difference between the numbers, and make it difficult to predict the difference between the elements of the magic cube. However, there are many previous studies that have been published by researchers on magic cubes but they have not achieved the desired goals.

4.4.4 The Security Analysis of The Fourth Algorithm (Secret Sharing with Magic Cube using Newton Divided Difference Interpolation)

In the implemented algorithm, the maximum protection of sensitive information has been applied by the integration of two different mathematical systems, one of which is the other, the secret and magic cubes. The construction of the magic cube is done through methods and techniques that give it strength and mathematical complexity in the face of any possible danger to which the information is exposed. The focus of this algorithm is how to transfer the properties of the magic cubes to a group of trusted subscribers by secret mode. The process of transition is done by making the (Dimension) of the magic cube the secret in the polynomial and then sending the points to the subscribers.

After the participants get the points, the Newton Divided Difference Interpolation formula are used for the purpose of rebuilding the original secret (Dimension) and then can be obtained all magic cube parameters for the purpose of rebuilding the original magic cube. Also, the factorial and power provided the algorithm with a high degree of complexity, due to the inability of the opponent to predict the value of the starting number or the amount of difference between the elements of the magic cube.

Thus, the obvious focus of the method of this research is the process of integrating magic cubes (with any order) along with the sharing of the secret key to provide a compact mathematical system, which contains multi security layers and high computational complexity. As a result, the attacker will be unable to compute the secret value even if part of secret information lost or theft according to the threshold (*k*-1). This means that there are no sufficient data to rebuild the secret key and to get the original magic cube.

The algorithms implemented in this study are based on the security of the Shamir's secret sharing scheme and the second-degree boundary polynomials in addition to numerical analysis methods with the mathematical properties of the magic cubes. The table (4.1) below showing an analysis of the strength and complexity of the implemented algorithms.

Table 4.1 A Comparison of the Strength and Complexity Analysis of the Implemented Algorithms with Shamir's model

Property	1st proposed algorithm	2nd proposed algorithm	3rd proposed algorithm	4th proposed algorithm	Shamir' s secret sharing
The dealer distributes the secret shadow	privately	privately	privately	privately	privately
Prevent (*t*-1) or viewer participants from recovering the secret	Based threshold	Based threshold	Based threshold	Based threshold	Based threshold

Resist the conspiracy attack	Point independency	Point independency	Point independency	Point independency	Point independency
Secure channel is needed	Threshold*shadow = secret	Threshold*shadow = secret	Threshold*shadow = secret	Threshold*shadow = secret	Threshold*shadow = secret
Prevent the participants from revealing each other's secret Shadow after the recovery phase	No. of point > eq. (order +1)	No. of point > eq. (order +1)	No. of point > eq. (order +1)	No. of point > eq. (order +1)	No. of point > eq. (order +1)
Resist revelation of the secret shadow of the participants from the public information	No correlation between secret & shadows	No correlation between secret & shadows	No correlation between secret & shadows	No correlation between secret & shadows	No correlation between secret & shadows
Resist the cheating action from the participants	Pivot element	Pivot element	Order value	Order value	Constant value of equation
Shadows are not reusable when participants join/leave the group	Unique shadow	Unique shadow	Unique shadow	Unique shadow	Unique shadow
The shadow is not reusable when shared secrets are reconstructed	One – time shadow	One – time shadow	One – time shadow	One – time shadow	One – time shadow
The dealer does not know the shadow of each participant	Secret-random distribution	Secret-random distribution	Secret-random distribution	Secret-random distribution	Secret-random distribution
Security is based on different numerical analysis interpolation	Lagrange	Hermite	Lagrange	Divided difference	Lagrange

4.5 Investigation and Analysis about Prime Number Affect

The strength and complexity of secret sharing scheme lies in the size of finite field arithmetic. The size of $p \in$ P, ($p > S$) and ($p > n$) is used. The prime number must be very large, greater than the number of subscribers (n) and a_i. The calculation of points should be (x, $f(x)$ mod p) instead of (x, $f(x)$). So, each participant will receive one point and will be aware of the prime number (publicly), therefore, the prime number should not be small to be predicted and discovered by opponents.

Assuming that the secret and the coefficients are as follows:

(S = 1234, a_1 = 166, a_2 = 94) Where ($a_0 = S$).

The Polynomial that will produce points are:

$f(x) = 1234 + 166\,x + 94\,x^2$

Six points will be produced from this Polynomial:

$B_{x\text{-}1} = (x, f(x))$, B_0 = (1, 1494), B_1 = (2, 1942), B_2 = (3, 2578), B_3 = (4, 3402), B_4 = (5, 4414), B_5 = (6, 5614).

It is possible to choose any three points randomly to reconstruct the secret:

(x_0, y_0) = (2, 1942), (x_1, y_1) = (4, 3402), (x_2, y_2) = (5, 4414).

Lagrange interpolation will be calculated:

$$\ell_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x - 4}{2 - 4} \cdot \frac{x - 5}{2 - 5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\ell_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 2}{4 - 2} \cdot \frac{x - 5}{4 - 5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\ell_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 2}{5 - 2} \cdot \frac{x - 4}{5 - 4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore,

$$
\begin{aligned}
f(x) &= \sum_{j=0}^{2} y_j \cdot \ell_j(x) \\
&= y_0\ell_0 + y_1\ell_1 + y_2\ell_2 \\
&= 1942\left(\frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}\right) + 3402\left(-\frac{1}{2}x^2 + \frac{7}{2}x - 5\right) + 4414\left(\frac{1}{3}x^2 - 2x + \frac{8}{3}\right) \\
&= 1234 + 166x + 94x^2
\end{aligned}
$$

The secret is the constant part of the Polynomial which equals 1234.

The problem (Cryptoanalysis):

when using only integer numbers in the polynomial, it will be dangerous to the secret because it is possible to be revealed easily.

If one of the opponents managed to steal two points out of a total of six, and remaining one point to reveal the original secret, note that k = 3, n = 6, $f(x) = S + a_1 x + a_{k-1} x^{k-1}$, $a_0 = S$, $a_i \in$ N. He needs to know more information about the secret so he will do the following:

i. Fills the $f(x)$ formula with S and the value of k: $f(x) = S + a_1 x + \ldots + a_{3-1} x^{3-1}$ ➔ $f(x) = S + a_1 x + a_2 x^2$.

ii. Fills (i) with values of D_0's x and $f(x)$: $1494 = S + a_1 1 + a_2 1^2$ ➔ $1494 = S + a_1 + a_2$.

iii. Fills (i) with the values of D_1's x and $f(x)$: $1942 = S + a_1 2 + a_2 2^2$ ➔ $1942 = S + 2 a_1 + 4 a_2$.

iv. Does (iii)-(ii): $(1942 – 1494) = (S – S) + (2 a_1 – a_1) + (4 a_2 – a_2)$ ➔ $448 = a_1 + 3a_2$ and rewrites this as $a_1 = 448 – 3a_2$.

v. Know that $a_2 \in \mathbb{N}$ so she starts replacing a_2 in (iv) with 0, 1, 2, 3, … to find all possible values for a_1:

- $a_2 = 0$ ➔ $a_1 = 448 – 3 * 0 = 448$
- $a_2 = 1$ ➔ $a_1 = 448 – 3 * 1 = 445$
- $a_2 = 2$ ➔ $a_1 = 448 – 3 * 2 = 442$

-
-
-
- $a_2 = 148$ ➔ $a_1 = 448 – 3 * 148 = 4$
- $a_2 = 149$ ➔ $a_1 = 448 – 3 * 149 = 1$

After $a_2 = 149$, the opponent will stop here because he knows if he continues to solve, he will get negative values for a_1 (This is impossible because $a_1 \in$ N) the opponent will now conclude that $a_2 \in [0, …., 149]$.

vi. Replaces a_1 by (iv) in (ii): $1494 = S + (448 – 3a_2) + a_2$ ➔ $S = 1046 + 2a_2$.

vii. Replaces in (vi) a_2 by the values found in (v) so she gets $S \in [1046 + 2 * 0, 1046 + 2 + 1, ………, 1046 + 2 *149]$.

Which will lead to information: the secret (S) $\in$ [1046, 1048, ……, 1344], he now owns 150 numbers only to guess the secret instead of the finite numbers.

The solution to this problem is to use a prime number to complicate the process of detecting the secret or predicting it by the opponents and also it must be sufficiently large.i.e, larger than the number of participants and a_i in the polynomial.

Assuming that the prime number = 1613 was chosen in the same polynomial, the points would be as follows: $B_0 = (1, 1494)$, $B_1 = (2, 329)$, $B_2 = (3, 965)$, $B_3 = (4, 176)$, $B_4 = (5, 1188)$, $B_5 = (6, 775)$.

If the opponent has two points $B_0 = (1,1494)$, $B_1 = (2, 329)$, k = 3, n = 6, $f(x) = S + a_1 x + a_{k-1} x^{k-1} \bmod p$, $a_0 = S$, $a_i \in$ N.

He needs to know more information about the secret so he will do the following:

i. Fills the $f(x)$ formula with S and the value of k and P: $f(x) = S + a_1 x + … + a_{3-1} x^{3-1} \bmod 1613$ ➔ $f(x) = S + a_1 x + a_2 x^2 – 1613m_x$: $m_x \in \mathbb{N}$

ii. Fills (i) with values of D_0's x and $f(x)$: $1494 = S + a_1 1 + a_2 1^2 – 1613m_1$ ➔ $1494 = S + a_1 + a_2$

iii. Fills (i) with the values of D_1's x and $f(x)$: $1942 = S + a_1\ 2 + a_2\ 2^2 - 1613m_2$ ➔ $1942 = S + 2\ a_1 + 4\ a_2 - 1613m_1$

iv. Does (iii)-(ii): $(1942 - 1494) = (S - S) + (2\ a_1 - a_1) + (4\ a_2 - a_2) + (1613m_1 - 1613m_2)$ ➔ $448 = a_1 + 3a_2 + 1613(m_1 - m_2)$ and rewrites this as $a_1 = 448 - 3a_2 - 1613(m_1 - m_2)$

v. Know that $a_2 \in \mathbb{N}$ so she starts replacing a_2 in (iv) with 0, 1, 2, 3, … to find all possible values for a_1:

- $a_2 = 0$ ➔ $a_1 = 448 - 3 * 0 - 1613(m_1 - m_2) = 448 - 1613(m_1 - m_2)$
- $a_2 = 1$ ➔ $a_1 = 448 - 3 * 1 - 1613(m_1 - m_2) = 445 - 1613(m_1 - m_2)$
- $a_2 = 2$ ➔ $a_1 = 448 - 3 * 2 - 1613(m_1 - m_2) = 442 - 1613(m_1 - m_2)$
- .
  .

In this case the opponent cannot be stopped because the $(m_1 - m_2)$ can be any number, even if it is negative it is $(m_2 > m_1)$, there are an infinite value for a_1. Because the number is prime, the opponent cannot get any information about the secret.

4.6 The Comparison of Implemented Algorithms According to Prime Number usage

In the implemented algorithms, the prime numbers were chosen in varying sizes. This choice was made clear. The more important the prime number is, the results are greater and make it more difficult to predict or know any information about the secret. A comparison was made between all the implemented algorithms in terms of mathematical computation foe the key space. Each time three values of (X_i) for each algorithm were compared with other algorithms and observed the results. In the first comparison, three values were selected for the x = (1, 2, 3) of all the algorithms and the results were compared with each other in terms of complexity, as illustrated in figure (4.3):

Table 4.2 Selected Values Where the (x = 1, 2, 3)

1st Algorithm		2nd Algorithm		3rd Algorithm			4th Algorithm	
x	**y**	**x**	**y**	**x**	**y**	**y'**	**x**	**y**
1	71	1	7	1	8	31	1	8
2	14	2	17	2	50	0	2	9
3	58	3	15	3	8	22	3	9

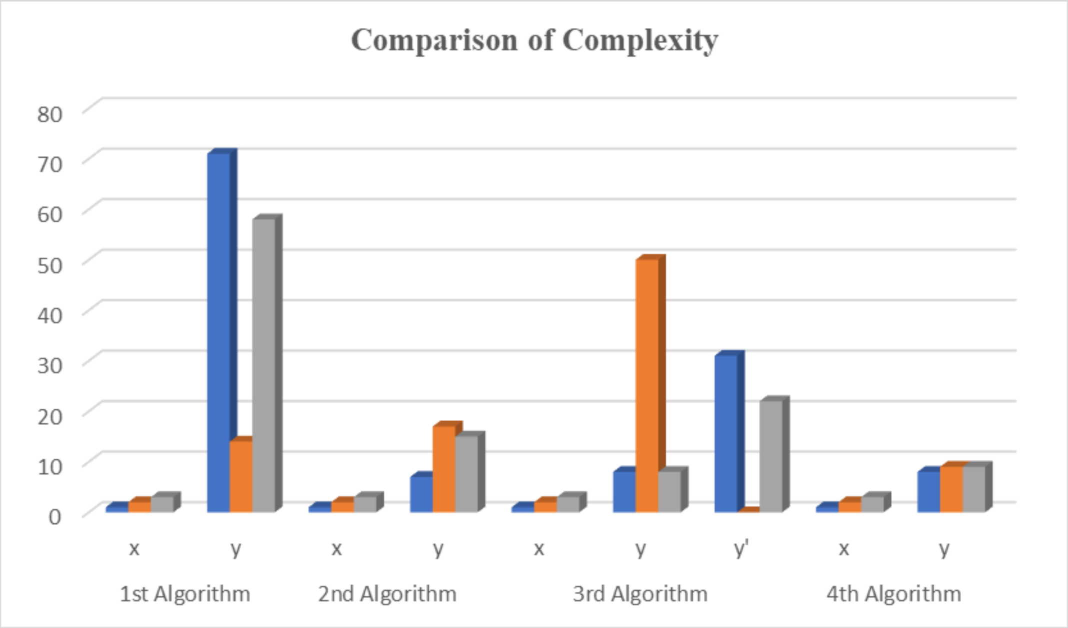


Figure 4.3. Comparison of Key Space for (x) Values Mod Prime

In the second comparison, three values were selected for the x = (4, 5, 6) of all the algorithms and the results were compared with each other in terms of complexity, as illustrated in figure (4.4):

Table 4.3 Selected Values Where the (x = 4, 5, 6)

1st Algorithm		2nd Algorithm		3rd Algorithm			4th Algorithm	
x	**y**	**x**	**y**	**x**	**y**	**y'**	**x**	**y**
4	25	4	1	4	41	44	4	8
5	4	5	13	5	43	13	5	6
6	84	6	13	6	14	35	6	3

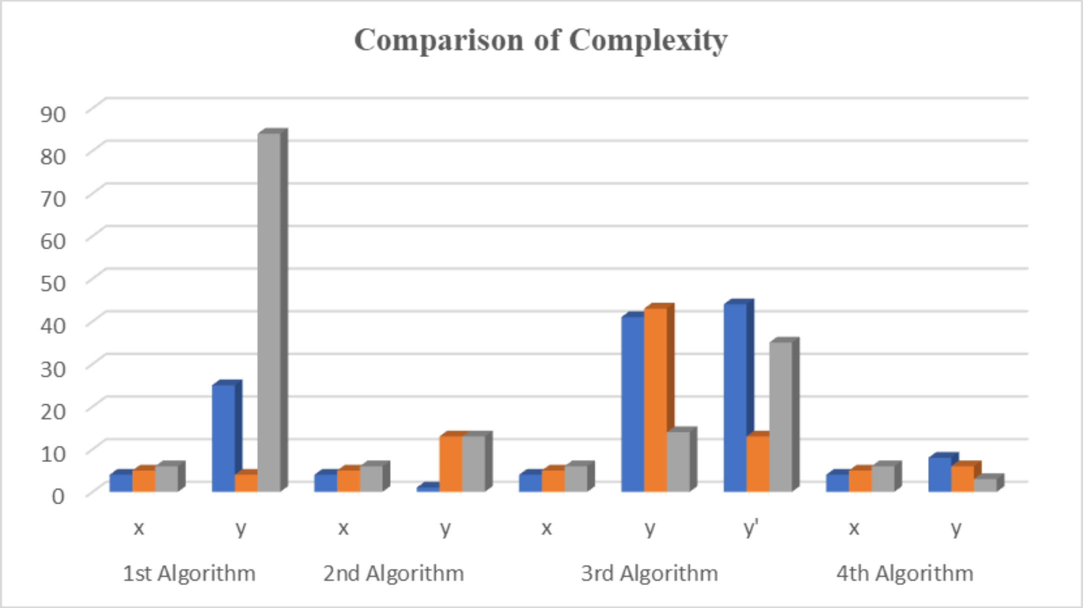


Figure 4.4. Comparison of Key Space for (x) Values Mod Prime

In the third comparison, three values were selected for the x = (2, 4, 6) of all the algorithms and the results were compared with each other in terms of complexity, as illustrated in figure (4.5):

Table 4.4 Selected Values Where the (x = 2, 4, 6)

1st Algorithm		2nd Algorithm		3rd Algorithm			4th Algorithm	
x	**y**	**x**	**y**	**x**	**y**	**y'**	**x**	**y**
2	14	2	17	2	50	0	2	9
4	25	4	1	4	41	44	4	8
6	84	6	13	6	14	35	6	3

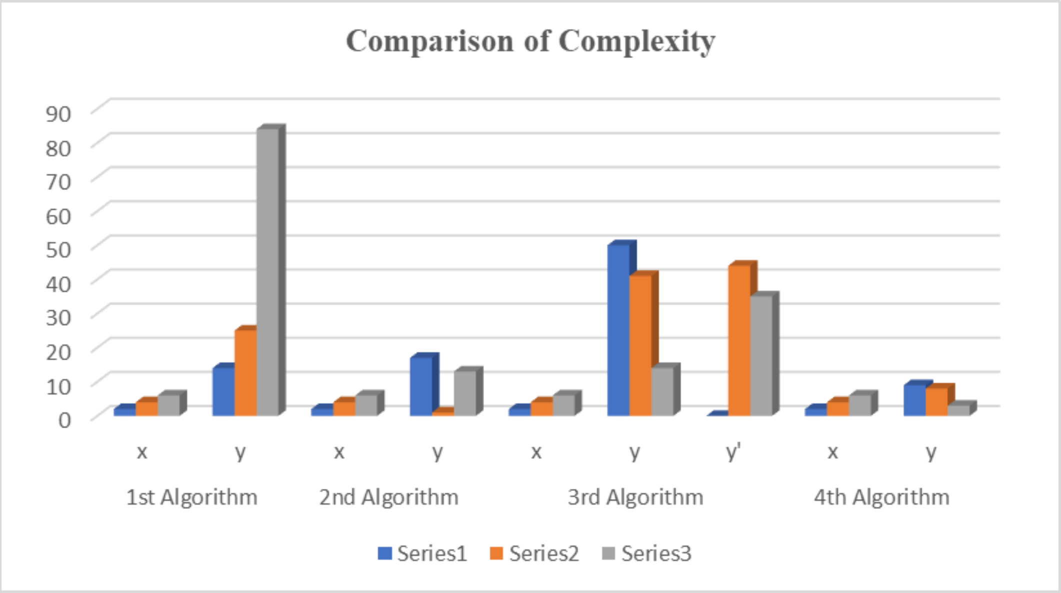


Figure 4.5. Comparison of Key Space for (x) Values Mod Prime

In the first algorithm a prime number is used that is larger than the prime numbers used in other algorithms. In all comparisons, it is clear that the graph of the first algorithm is higher than all other algorithms due to the size of the prime number used. Therefore, the larger the size of the prime number, the more complicated the calculations in the algorithm, which increases the stages of protection of confidential information. Mathematical complexities used to rebuild secret keys also increase.

4.7 Comparison of Elapsed Times to Reconstruct the Implemented Algorithms

In addition to calculating the complexity of each of the implemented algorithms, the time taken to rebuild the secret was calculated by the subscribers. In each process, three values of (X_i) for each algorithm were compared with the other algorithms and the time taken for each was recorded in second. In each comparison three different points were selected for the four implemented algorithms as shown in the tables (4.5, 4.6, 4.7, and 4,8):

Table 4.5 Elapsed Time According to (x) Values

1st Algorithm		2nd Algorithm		3rd Algorithm		4th Algorithm	
X	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**
1	00:00:05.4212005	1	00:00:06.6172480	1	00:00:06.7423327	1	00:00:06.8210514
2		2		2		2	
3		3		3		3	

Table 4.6 Elapsed Time According to (x) Values

1st Algorithm		2nd Algorithm		3rd Algorithm		4th Algorithm	
X	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**
4	00:00:04.1776682	4	00:00:05.8433516	4	00:00:08.2397311	4	00:00:08.4262575
5		5		5		5	
6		6		6		6	

Table 4.7 Elapsed Time According to (x) Values

1st Algorithm		2nd Algorithm		3rd Algorithm		4th Algorithm	
X	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**
2	00:00:04.7798393	2	00:00:05.2166433	2	00:00:08.4472697	2	00:00:08.2021446
4		4		4		4	
6		6		6		6	

Table 4.8 Elapsed Time According to (x) Values

1st Algorithm		2nd Algorithm		3rd Algorithm		4th Algorithm	
X	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**	**X**	**Elapsed Time in Second**
1	00:00:05.6760810	1	00:00:06.2275102	1	00:00:08.7820440	1	00:00:10.6471402
3		3		3		3	
5		5		5		5	

Concerning to the above comparison, the time taken to rebuild the original secret was calculated by the trusted users of the implemented algorithms and the time was fixed for each algorithm.

4.8 Pros and Cons of the Implemented Secret Sharing Algorithms

There are several advantages and disadvantages of any algorithm being developed or algorithms being implemented because there is no perfect work in all aspects of the design. The implemented algorithms have many advantages and limitations, which can be mentioned as follows:

4.8.1 The Pros of the Implemented Algorithms

1. Maintains the parts of the password even in case of loss or theft of one of the points (shadows) sent by the dealer to the trusted subscribers.
2. Perfect secret sharing algorithm, that means all shares do not contain any information about the original secret.
3. If the number of subscribers is smaller than (*t*-1), the participants cannot rebuild the password. This process preserves and protects the confidentiality even if it falls into the hands of subscribers who are not eligible to retrieve it and are less than the value of the threshold.
4. Ideal secret sharing algorithm, which means all parts of the secret must be equal in size, and the size of the (shadow) should not be greater than the secret size. This process keeps the transmission of the parts of the password correctly between the dealer and the trusted subscribers.
5. Fraud prevention by both parties (dealer or subscribers) is prohibited in the secret key management process, through which fraud can be detected and exceeded to maintain confidentiality.
6. The use of a very large prime number increases the complexity of calculations and the opponent cannot predict the parts of the secret or restore the original secret.
7. Any (shadow) can be replaced without having to change the original (secret) when changing one of the trusted participants or addition one participant to the group.

4.8.2 The Cons of the Implemented Algorithms

1. If there are stolen transactions for more than a one shadow of the shareholders sent to trusted subscribers or frauds that occur by the dealer or by subscribers, it

will affect the process of rebuilding the original password again. Because it will reconstruct incorrect secret.

2. If the parts of the password are not equal in size or larger than the size of the original password, they cannot be sent to the subscribers. Therefore, all parts of the secret must be equal in size before sending them because this will affect the process of rebuilding the original secret by the participants.
3. After every process of sending the secret from the dealer to the subscribers, there must be an update on the original secret. Therefore, the password cannot be reused more than once so that it can be detected by the adversaries.
4. The time taken to build the password by the dealer is quite different from the time taken by trusted subscribers to rebuild the original password. Due to the lack of synchronization of the pool of participants during the reconstruction, which may expose the secret to security risks and can be discovered. It is therefore very important that all trusted participant's share pool at the same time to protect the confidentiality of the liabilities.
5. All confidential (shareholders) must be sent through secret channels exclusively to all trusted subscribers in order to avoid loss or theft by the opponents.
6. If the size of the secret parts is too small, it presents the secret to the risk of theft or disclosure by the adversaries. Because the small parts of the secret lead to the speed of predicting the original secret by the opponent.
7. The large size of the secret leads to the need for a prime number larger than it, which leads to the need for larger storage space.

4.9 Applications of the Implemented Secret Sharing Algorithms

The implemented algorithms can be used in many aspects and many contributions such as:

1. It can be used in banks to keep financial transactions confidential.
2. It can be used in laboratory fields to keep confidential information by qualified biologists only to protect them from falling into the hands of unqualified persons.
3. It can be used in war fields, where it can protect the secret codes for launching warplanes.

4. It can be used to keep confidential sensitive personal information in mobile and personal Computer devices.
5. It can be used in encryption\decryption operations for complex layers of protection and maintenance of confidential information such as (business transactions).
6. Easy to apply to electronic devices because they do not need devices with high capabilities and specifications.
7. Through which it can transfer a large number of sensitive information that resides within the cells of the magic cube and completely confidential to any trusted party.
8. They have the ability to protect the secret codes of websites because they provide more complex layers to protect the secret from the risk of the opponent.
9. Radar Management Systems.

Chapter Five

Conclusions and Suggestions for Future Works

Chapter Five

Conclusions and Suggestions for Future Works

5.1 Introduction

The results of experiments for the development of the techniques of (*SS*) based on the mathematical characteristics of the (*MCs*) were explained in detail in the previous chapter. The impact of mathematical techniques on magic cubes was demonstrated in the process of managing the secret keys and in increasing the complexity of the process of reconstructing the secret when moving from the dealer to the trusted participants. This chapter is intended to provide conclusions about the performance of development sharing a secret algorithm. In addition, make some suggestions for future work.

5.2 Conclusions

The important conclusions of this work can be summarized by a set of points:

1. The first implemented algorithm combined the (odd order) magic cube and (Lagrange) mathematical base to give a secure secret sharing method.
2. The first and second algorithms depended basically on sending the pivot element as a secret to all participants. Since the pivot play avital role in reconstruction the secret with sufficient information.
3. The submitted method gives a multi security layers in sharing the secret key with high level of security. Since, the implemented method requires high guessing mathematical operations as well as high search space probability.
4. A new numerical analysis method was implemented in the second algorithm that based on the Hermite interpolation. This algorithm adds a great deal of complexity to the protection of the secret keys because it does not rely solely on Lagrange interpolation, but relies on the derivative of the polynomial in the conclusion of the shares before sending them to subscribers by the dealer.
5. The Hermite interpolation allowed the subscribers to reconstruct the secret through the derivative results and the selected points. Because the derivative results will represent an additional secure layer.

6. The clue of magic cube diminution-order(N) gave conditional rules in reconstruction the secret and consequently increased the computational complexity for the key management scheme.
7. The factorial and power mathematical operations have been adapted in algorithms third and fourth to increase the complexity layers in construction and reconstruction the secret.
8. The use of magic cubes characteristics has increased the complexity of the security of the secret keys transferred between the dealer and the trusted subscribers compared with the Shamir secret sharing scheme, which relies solely on the protection provided by Lagrange Interpolation polynomial.
9. The mathematical properties of magic cube was not affect on the time taken to transfer the secret key from the dealer to the participants compared with Shamir's secret sharing scheme.
10. The fourth implemented algorithm has adopted a Newton’s divided difference interpolation formula that includes a new interpolation method for secret sharing based on magic cube mathematical notation. The Newton divided difference produce a new direction in secret key management.
11. Finally, the Hermite algorithm can be considered the best algorithm among the proposed algorithms. Because it has many good features that enable it to manage the secret securely as a result of its own a derivative mathematical property.

5.3 Suggestions for Future Works

The contributions of this thesis can be extended in different directions as in the following suggestions:

1. Developing new methods of sharing a secret with the magic cubes using new different methods of numerical analysis mathematical basis.
2. Propose new methods for multi-secret sharing techniques through the use of mathematical properties for a magic cube.
3. Suggest secure reconstruction of secret approach in multi-magic cubes with equal dimensions.

4. Implementation the algorithms in a real cases or scenario such as cloud computing, financial transferring money and ad hoc network.
5. Use implemented algorithms in encryption/decryption processes.

References

References

[1] S. D. Patil and P. K. Ithape, "Verifiable Image Secret Sharing with Cheater Identification," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2018, pp. 1238-1241: IEEE.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the national computer conference*, 1979, vol. 48, no. 313.

[3] A. J. C. o. t. A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[4] K. Shima and H. Doi, "({1, 3}, n) Hierarchical Secret Sharing Scheme Based on XOR Operations for a Small Number of Indispensable Participants," in *2016 11th Asia Joint Conference on Information Security (AsiaJCIS)*, 2016, pp. 108-114: IEEE.

[5] C. A. Pickover and S. S. C. A. Pickover, *The Zen of Magic Squares, Circles, and Stars: An Exhibition of Surprising Structures Across Dimensions*. Princeton University Press, 2002.

[6] I. J. I. J. o. s. Tomba and r. Publications, "On the Techniques for Constructing Even-order Magic Squares using Basic Latin Squares," International Journal of scientific and research Publications, vol. 2, no. 9, 2012.

[7] O. A. Dawood, A. M. Rahma, and A. Mohssen J. Abdul Hossen, "*Symmetric Ciphers and Asymmetric Ciphers Based on Magic Cube with 6-D,"* LAP Lambert Academic Publishing, no.148, 2016.

[8] H. A. Vyas, "Secret Sharing: Secure Password Sharing Technique," in *2015 Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 731-735: IEEE.

[9] S. N. Pundkar and N. Shekokar, "Cloud computing security in multi-clouds using Shamir's secret sharing scheme," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016, pp. 392-395: IEEE.

[10] K. Muthukumar and M. Nandhini, "Modified secret sharing algorithm for secured medical data sharing in cloud environment," in *2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM)*, 2016, pp. 67-71: IEEE.

[11] N. Kaneko and K. Iwamura, "Improvement of Communication Traffic and Security of Proactive Secret Sharing Schemes and Combination Proactive Secret Sharing Scheme with an Asymmetric Secret Sharing Scheme," in *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2017, pp. 13-18: IEEE.

[12] A. Kheiri and E. J. T. C. J. Özcan, "Constructing constrained-version of magic squares using selection hyper-heuristics," The Computer Journal, vol. 57, no. 3, pp. 469-479, 2013.

[13] A. Farhan and F. Awad, "*Color Image Encryption With a Key Generated by Using Magi Square*," Journal of Engineering and Applied Sciences, vol. 13, pp. 2038-2041, 2018.

[14] S. Jamel, T. Herawan, and M. M. Deris, "A cryptographic algorithm based on hybrid cubes," in *International Conference on Computational Science and Its Applications*, 2010, pp. 175-187: Springer.

[15] X. Feng, X. Tian, and S. Xia, "An improved image scrambling algorithm based on magic cube rotation and chaotic sequences," in *2011 4th International Congress on Image and Signal Processing*, 2011, vol. 2, pp. 1021-1024: IEEE.

[16] A. M. S. J. I. J. o. C. S. Rahma and I. Security, "New Variant of Public Key Based on Diffie-Hellman with Magic Cube of Six-Dimensions," International Journal of Computer Science and Information Security (IJCSIS), vol. 13, no. 10, 2015.

[17] O. A. Dawood, A. M. S. Rahma, A. M. J. A. J. I. J. o. I. S. Hossen, and Applications, "Generalized Method for Constructing Magic Cube by Folded Magic Squares," International Journal of Intelligent Systems and Applications, vol. 8, no. 1, p. 1, 2016.

[18] E. Dawson, D. J. C. Donovan, and Security, "The breadth of Shamir's secret-sharing scheme," Computers & Security, vol. 13, no. 1, pp. 69-78, 1994: Elsevier.

[19] R. L. Rivest, A. Shamir, and Y. Tauman, "How to share a secret," in *Communications of the ACM*, 1979: Citeseer.

[20] F. Oriol and P. Carles, "Ideal Hierarchical Secret Sharing Schemes," IEEE transactions on information theory, vol.58, no.5, pp. 3273-3286, 2012.

[21] J. Shao, Z. J. A. M. Cao, and Computation, "A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme," Applied Mathematics and Computation, vol. 168, no. 1, pp. 135-140, 2005: Elsevier.

[22] C. Ignacio, C. Ronald, M. Diego, P. Ola Carles, and X. Chaoping, "On secret sharing with nonlinear product reconstruction," SIAM Journal on Discrete Mathematics, vol.29, no.2, pp. 1114--1131, 2013.

[23] D. Johnson, "Secret sharing schemes and noncommutative polynomial interpolation," 2018.

[24] S. Rubinstein-Salzedo, "Cæsar Ciphers," in *Cryptography*: Springer, pp. 5-8, 2018,

[25] S. J. a. p. a. Narani, "Social secret sharing for resource management in cloud," arXiv preprint arXiv:1302.1185, 2013.

[26] A. Beimel, "Secret-sharing schemes: a survey," in *International Conference on Coding and Cryptology,* 2011, pp. 11-46: Springer.

[27] C. L. Corniaux and H. Ghodosi, "An entropy-based demonstration of the security of Shamir's secret sharing scheme," in *2014 International Conference on Information Science, Electronics and Electrical Engineering*, 2014, vol. 1, pp. 46-48: IEEE.

[28] K. M. J. C. Martin, P. o. t. R. F. A. o. B. f. S. Cryptography II, and t. Arts, "Challenging the adversary model in secret sharing schemes," pp. 45-63, 2008: Citeseer.

[29] M. Nojoumian and D. R. Stinson, "Social secret sharing in cloud computing using a new trust function," in *2012 Tenth Annual International Conference on Privacy, Security and Trust*, 2012, pp. 161-167: IEEE.

[30] M. Tompa and H. J. j. o. C. Woll, "How to share a secret with cheaters," journal of Cryptology, vol. 1, no. 3, pp. 133-138, 1989: Springer.

[31] D. G. Tieng and E. Nocon, "Some Attacks on Shamir's Secret Sharing Scheme by Inside Adversaries," DLSU Research Congress, vol,4, 2016.

[32] I. Karim, S. Sumpeno, and M. H. Purnomo, "Synthesis of virtual character poses using Lagrange polynomial interpolation," in *2015 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, 2015, pp. 273-278: IEEE.

[33] K. A. J. I. J. o. C. S. Hussien and N. Security, "The lagrange interpolation polynomial for neural network learning," International Journal of Computer Science and Network Security, vol. 11, no. 3, pp. 255-261, 2011.

[34] 足立智子, "Multi secret sharing scheme based on Hermitian interpolation (New contact points of algebraic systems, logics, languages, and computer sciences)," 2015.

[35] T. Adachi, C. J. J. o. A. M. Okazaki, and Physics, "A multi-secret sharing scheme with many keys based on Hermite interpolation," Journal of Applied Mathematics and Physics, vol. 2, no. 13, p. 1196, 2014.

[36] B. Das, D. J. I. J. o. M. T. Chakrabarty, and Technology, "Lagranges Interpolation Formula: Representation of Numerical Data by a Polynomial Curve," International Journal of Mathematics Trend and Technology, pp. 23-31, 2016.

[37] J. J. U. o. S. M. Lambers, Fall, "Fixed-point Iteration," University of Southern Mississippi, Fall, 2009.

[38] S. A. Al-Najjar, A. Nuha, F. J. E. AAl-Heety, and T. Journal, "Computation of Odd Magic Square Using a New Approach with Some Properties," Engineering and Technology Journal, vol. 30, no. 7, pp. 1203-1210, 2012.

[39] X. J. S. a. m. v. GUOCE, math. CO, "Constructing All Magic Squares of Order Three," September arXiv: math/0409468v1, math. CO, vol. 24, 2004.

[40] S. J. I. J. o. D. I. Al-Ashhab and W. Communications, "Special magic squares of order six and eight," International Journal of Digital Information and Wireless Communications (IJDIWC), vol. 1, no. 4, pp. 769-781, 2012.

[41] R. P. J. I. J. o. P. Nordgren and A. Mathematics, "New constructions for special magic squares," International Journal of Pure and Applied Mathematics, vol. 78, no. 2, pp. 133-154, 2012.

[42] I. Tomba and N. Shibiraj, "Improved Technique for Constructing Doubly-even Magic Squares using Basic Latin Squares," 2013: Citeseer.

[43] W. W. R. Ball, *Mathematical recreations and problems of past and present times*. Macmillan and Company, 1892.

[44] C. Prasartkaew and S. Choomchuay, "Parity check matrix construction via Magic Square Based Algorithm," in *2012 International Symposium on Communications and Information Technologies (ISCIT)*, 2012, pp. 54-59: IEEE.

[45] M. K. J. a. p. a. Nasution, "Algebraic on magic square of odd order n," arXiv preprint arXiv:1207.5117, 2012.

[46] V. F. Rickey, "Dürer’s Magic Square, Cardano’s Rings, Prince Rupert’s Cube, and Other Neat Things," 2008: Citeseer.

[47] P. J. D. o. P. Loly, The University of Manitoba, "Franklin Squares'a Chapter in the Scientific Studies of Magical Squares," Departement of Pyhsic, The University of Manitoba, 2006.

[48] T. Irom and S. Ningthoujam, "Successful Implementation of the Hill and Magic Square Ciphers: A New Direction," International Journal of Advanced Computer Technology (IJACT), vol.2, no.3, 2019.

[49] R. P. J. L. A. Nordgren and i. Applications, "On properties of special magic square matrices," Linear Algebra and its Applications, vol. 437, no. 8, pp. 2009-2025, 2012.

[50] M. J. T. M. G. Trenkler, "Magic cubes," The Mathematical Gazette, vol. 82, no. 493, pp. 56-61, 1998: Cambridge University Press.

[51] D. Rajavel and S. Shantharajah, "Cubical key generation and encryption algorithm based on hybrid cube's rotation," in *International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012),* 2012, pp. 183-187: IEEE.

[52] A. Rogers and P. Loly, "The Inertial Properties of Magic Squares and Cubes," 2004: Citeseer.

[53] F. Swetz, *Legacy of the Luoshu: The 4,000 Year Search for the Meaning of the Magic Square of Order Three*. AK Peters/CRC Press, 2008.

الخلاصة

تعتبر حماية البيانات السرية والحساسة التي تتم مشاركتها عبر الانترنت من اهم المشاكل التي تواجه مستخدمي شبكة الانترنت. على الرغم من التقدم التكنلوجي وظهور الكثير من الحلول لحماية البيانات السرية لا يزال التحدي الرئيسي هو مشاركة البيانات خلال بيئة مفتوحة. ان طرق مشاركة السر تلعب دوراً كبيراً في استراتيجية ادارة المفاتيح للبيانات الحساسه و مفاتيح التشفير فيما يخص التوليد, المبادلة و الادارة بطريقة امنة. ان صفة المشاركة السرية الذي تم بناءه قد تم تأسيسه على مباديء رياضية مثبتة والتي تسمح للموزع بتوزيع المفاتيح السرية بين العديد من المشتركين بأمان. في هذه الاطروحه تم اقتراح 4 خوارزميات حسابية جديدة والتي هي مبنية بالكامل على مباديء المكعبات السحرية والخلفية الرياضية لـ (Lagrange Interpolation). اعتمدت الخوازمية الاولى على توليد نظام طوي للمكعب السحري الفردي والذي يستغل العنصر المحوري للمربع السحري الاول في المكعب ليكون السر ومن ثم يتم تضمنيه في معادلة متعددة الحدود. سيدعم العنصر المحوري في نقل خصائص المكعب السحري للمشتركين ليتمكن من اعادة بناء المكعب السحري الاصلي مرة اخرى. الطريقة الرياضية (Hermite Interpolation) تم استخدامها في الخوارزمية الثانية والتي تعتبر اكثر تعقيدا من طريقة (Lagrange Interpolation). وذلك لانها تعتمد على مشتقات متعددة الحدود ومشتقة (Lagrange Interpolation) في عملية بناء واعادة بناء السر من قبل الموزع والمشتركين. تفترض الخوارزمية الثالثة بان البعد (N) للمكعب السحري هو المفتاح السري والذي سوف يتم تضمينه في معادلة متعددة الحدود وارسالة الى المشتركين الموثوقين . سيتمكن المشتركين من الحصول على السر(ابعاد المكعب) بعد استخدام (Lagrange Interpolation). تتطلب الخوارزمية العثور على رقم قيمة البداية لبناء المكعب وقيمة الفرق بين عناصر المكعب السحري ليتم اعادة بنائه مرة اخرى. يمكن للخوارزمية الثالثة العمل مع انواع مختلفة للمكعبات السحرية ذات(الترتيب فردي

, نظام مفرد او زوجي). الخوارزمية الرابعة المقترحة هي الطريقة الحسابية للتحليل العددي (Newton's Divided Difference Interpolation). تم تطبيق معادلة (Newton) على خوارزمية متعددة الحدود الثانية واظهرت نتائج جيدة مقارنة بما سبق في عملية حماية المفاتيح السرية. ان عملية دمج مشاركة السر مع الخصائص الحسابية للمكعبات السحرية اظهرت مرونة كبيرة في التعامل مع مختلف طرق التحليل العددي. ان طرق المشاركة السرية المقترحة تم اختبارها وقياسها وفقا لبعض المقاييس المهمة مثل الوقت المنقضي وعامل التعقيد الحسابي. ان الاختبارات المنفذة اعطت نتائج معقولة ومقبولة لحساب السر. كل طرق التحليل العددي المستعملة قدمت نتائج جيدة خلال عملية مشاركة السر واعطت الحماية الضرورية للمعلومات الحساسة. الطرق المقترحة ولدت نتائج مميزة ووضعت المستخدمين امام خيارات عديدة لاختيار الطريقة المناسبة لنقل معلوماتهم السرية والحساسة للمشتركين الموثوقين لحمايتها من السرقة, الخسارة أو خطر المهاجم (محلل الشفرات). تم برمجة الطرق المقترحه من خلال برنامج فيجوال استوديو 2016 بلغة برمجة سي شارب تحت نظام وندوز 10 نسخة 64 بت باستخدام معالج (TM) core i7-77HQ CPU @ 2.80 GHz , Ram 16.0 GB , HD 1TB , 4GB VGA.

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة الأنبار

كليّة علوم الحاسوب وتكنلوجيا المعلومات

قسم علوم الحاسبات

إدارة مفاتيح المشاركة السرية بالإعتماد على المكعب السحري

رسالة مقدمة الى
قسم علوم الحاسبات – كلية علوم الحاسوب وتكنولوجيا المعلومات
جامعة الانبار
وهي جزء من متطلبات نيل درجة الماجستير في علوم الحاسبات

مقدمة من قبل الطالب

رافد صيهود عبد العزيز

بإشراف

أ.د. علي مكي صغير		م.د. عمر عبد الرحمن داود

1441هـ		2019 م