DESIGN AND ANALYSIS OF SOME NEW CODES AND CRYPTO SCHEMES USING QUASIGROUPS

Thesis submitted in partial fulfillment for the award of degree

DOCTOR OF PHILOSOPHY

IN

MATHEMATICAL SCIENCES

BY

SATISH KUMAR

DEPARTMENT OF MATHEMATICAL SCIENCES
INDIAN INSTITUTE OF TECHNOLOGY
(BANARAS HINDU UNIVERSITY)
VARANASI – 221005
INDIA

Roll No. 18121501 April, 2024

Contents

Abbreviations & Notations

Abbreviations

MDS	Maximum Distance Separable
MAC	Message Authentication Codes
MPKC	Multivariate Public Key Cryptosystem
RS	Reed Solomon
ISBN	International Standard Book Number
EAN	European Article Number
SSN	Social Security Number
MQQ	Multivariate Quadratic Quasigroup
IND-CPA	Indistinguishability Against Chosen Plaintext Attack
IND-CCA	Indistinguishability Against Chosen Ciphertext Attack
NIST	National Institute of Standards and Technology
EUF-CMA	Existential Unforgeability Under Chosen Message Attack
USB	Universal Serial Bus
CDs	Compact Discs
RM code	Reed-Muller Code
CBC	Cipher Block Chaining
CFB	Ciphertext Feedback
OFB	Output Feedback
AES	Advanced Encryption Standard
ANF	Algebraic Normal Form
RFID	Radio-Frequency Identification
SHA	Secure Hash Function
NLPN	Non-Linear Pseudo Noise
BF	Block Frequency

LRO	Longest Run of Ones
BMR	Binary Matrix Rank
DFT	Discrete Fourier Transform
OTM	Overlapping Template Matching
NOTM	Non-overlapping Template Matching
MUS	Maurer's Universal Statistical
LC	Linear Complexity
AE	Approximate Entropy
CSF	Cumulative Sum Forward
CSB	Cumulative Sum Backward
RE	Random Excursions
REV	Random Excursion Variants

Notations

$x \parallel y$	the concatenation of the binary strings/vectors x and y
$d_H(x, y)$	the Hamming distance between x and y
$wt(x)$	the Hamming weight of x
$\mathbb{Z}$	set of integers
$\mathbb{Q}$	set of rational numbers
$\mathbb{R}$	set of real numbers
$\mathbb{F}_q$ or $\mathbb{GF}(q)$	finite field of order q
S_3	symmetric group on a set of 3 elements

Acknowledgments

At the completion of this doctoral dissertation, I would like to thank several individuals who in one way or another contributed and extended their valuable assistance in its preparation and completion.

First and above all, I express my greatest regards to the Almighty **Lord Mahadev and Maa Saraswati** for bestowing upon me the courage to face the complexities of life, providing me this opportunity and granting me the capability to proceed successfully.

It is my pleasure to express my profound gratitude and deep regards to my research supervisor **Dr. Ashok Ji Gupta** and co-supervisor **Dr. Indivar Gupta** for their constant support throughout my research work. Their insightful feedback and unwavering guidance have always motivated me to persevere in my efforts. I consider myself fortunate enough to get a chance of pursuing my doctoral program under their guidance. I would also like to thank Mr. Harshdeep Singh, SAG, DRDO, Delhi for many fruitful discussions that led to collaborative works. His willingness to help at various stages of this research work was invaluable. Additionally, I am grateful to Mr. Tapas, SAG, DRDO, Delhi for his valuable insights during the thesis writing.

I want to express my heartfelt thanks to several individuals at the Department of Mathematical Sciences, IIT (BHU) Varanasi. I am particularly grateful to Prof. (Retd.) B. M. Pandeya, for his constant encouragement and motivation throughout my research. I am also thankful to Prof. Sanjay Kumar Pandey, Head of the Department, for providing all the necessary facilities. I am grateful to the office staff of the Department of Mathematical Sciences for being so helpful and cooperative.

I want to thank my seniors, Dr. Shiv Kumar, Mrs. Sonal and Dr. Varun Kumar of the Department of Mathematical Sciences, IIT (BHU), for their insightful discussions, unwavering support and guidance. Additionally, I want to thanks my fellow researchers at IIT (BHU) Mr. Kaushal Gupta, Mr. Pradeep Rai and Mr. Mukul Verma for their support. I would further like to pay my special thanks to my near and dear friends Mr. Ankit Prajapati, Mr. Arzoo Jamal and Mr. Prem

for always being there and bear with me in the good and bad times during my wonderful days in the campus. I am enormously thankful to my colleagues and all the research scholars of the department for maintaining friendly and positive work environments. Further, special thanks to my best friends Mr. Vishal Panchal and Mr. Sachin Mishra for their never ending support, encouragement, affection, and honest opinions, which provided me with all the strength to achieve my dreams.

I am indebted to my institute, Indian Institute of Technology (BHU), Varanasi for their financial support and all necessary resources throughout my research. I am also indebted to Scientific Analysis Group (SAG), Defence Research & Development Organization (DRDO), Delhi to provide the necessary resources for my research work.

I would like to dedicate this research work to my parents, Mr. Shashi Bhushan and Mrs. Pushpa Sinha for their love, patience and understanding. This accomplishment would not have been possible without their unconditional support and encouragement. With deepest respect, I remember the invaluable guidance for life I received from my Late grandfather Mr. Ram Avtar Kunwar and maternal grandfather, Late Ratneshwar Chaudhary. Special love to my younger brother Nitish Kumar.

This acknowledgment would be incomplete if the name of great visionary **Pt. Madan Mohan Malaviya** is not mentioned as who made this divine center of knowledge and I want to express my deepest regards to him.

Date: 26/04/2024
Place: Varanasi

(Satish Kumar)

Introduction

In modern era, communication and data sharing via noisy channels like internet are exceedingly common. Therefore, to ensure the confidentiality and integrity of data transmitted between two or more systems remains the paramount concern. Coding theory [81, 83, 110] is the study of mathematical techniques to construct different types of codes as their suitability for particular applications. Codes serve various purposes, such as data compression, error detection, error correction, data transmission, and data storage. Cryptography [69, 92, 119] is the study of mathematical techniques concerning information security including data integrity, data confidentiality, data authenticity and non-repudiation. Researchers worldwide design various cryptographic protocols and analyze their security.

In 1849, Euler [47] published a paper introducing a new theory on Latin squares with the property of being pairwise orthogonal, termed as mutually orthogonal Latin squares (MOLS). In subsequent years, Cayley [33] introduced the concept of group multiplication tables, and demonstrated that such tables could be viewed as a bordered Latin squares. In 1935, Moufang [95] first introduced the term *quasigroup* and later referred to the term *loop* as a quasigroup possessing an identity element. The versatility of quasigroups themselves, with their properties and existence of quasigroups of specific order enables their application in diverse theories encompassing coding theory, cryptography, telecommunications and beyond [11, 32, 33, 35, 116].

A quasigroup by definition, does not have the associative property, which is defining characteristic of a group. Hence, we can say every group is a quasigroup not the other way around. The properties such as closure and inversion of elements of quasigroups offers valuable functionality in the design of various cryptographic primitives. In Figure 1, various generalizations between groupoid and group are given. The associative structures like groups, rings, and finite fields have been widely employed in the development of diverse cryptographic primitives and codes. Similarly, Dénes and Keedwell [31–35] have done extensive research on the application of non-associative structures like quasigroup in designing the various cryptographic primitives. Latin squares, which serves as a fundamental combinatorial structure for quasigroups have found wide applications in coding theory and

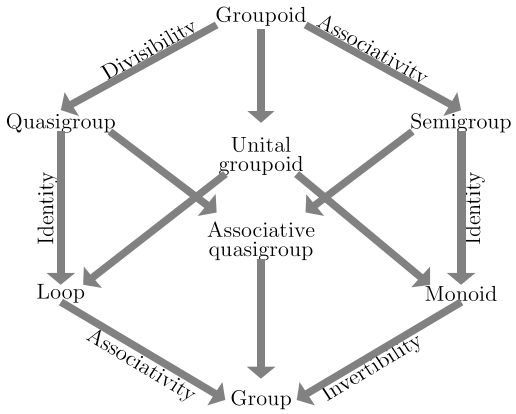

Figure 1: Algebraic structures between groupoid and group

cryptography [33–35]. This has spurred researchers worldwide to explore various aspects of Latin squares, including enumerating Latin subsquares [35], transversals of Latin squares, studying Latin squares which are pairwise orthogonal, namely mutually orthogonal Latin squares, etc. For an introductory understanding of the theory related to Latin squares and their applications, a reader may refer to [11, 33].

In 2009, Markovski et al. proposed a secure hash function, named *NaSHA* [90], using quasigroups. The security of NaSHA relies upon various factors including the quasigroup string transformations, number of isotopies exists for a given quasigroups, number of quasigroups of particular order, etc. In the same year, Gligoroski et al [60] proposed another secure hash function *Edon-*$\mathcal{R}$, whose security relies on solving the system of quasigroup operations and finding the order of elements in a quasigroup. Later, various cryptographic schemes have been designed using quasigroups, which we discuss in subsequent part of the thesis.

Latin squares also find diverse practical applications, including the design of statistical experiments, construction of error-correcting telegraph codes, generation of magic squares, and messages encoding. The orthogonal properties of Latin squares and quasigroups render them suitable for application in coding theory [29, 33, 76]. In 2007, Gligoroski et al. [59] proposed an error-correcting code based on quasigroup transformations. To design such type of codes, they utilize an encryption scheme based on quasigroup transformation and produce non-linear and almost random codes. The authors compare their code with Reed-Muller (RM) code of rate 3/16 that can recover up to 7 errors in 32 bits, however the proposed non-linear code can correct even 5 errors in 16 bits which is much better than RM code.

Motivation/Objective of the Thesis

Quasigroups find wide applications in the design of various cryptographic primitives, including S-boxes [20], block ciphers [5, 87, 122], stream ciphers [88, 99, 131], hash functions [125], secret sharing schemes [56], message authentication codes [27] and in numerous other areas. For detailed survey on the application of quasigroups and Latin squares in cryptography and coding theory, readers are encouraged to refer [75, 116].

Consequently, the development of new efficient codes and cryptographic primitives based on quasigroups is a fascinating area of research. Driven by this motivation, we aim to develop new codes that are efficient than classical codes to detect burst errors resulting from noisy channels or any physical damage to information carriers (such as, USB and CDs). Similarly, the construction of MDS codes is also part of our research. In literature, numerous codes which can detect errors caused by noisy channels and MDS codes based on quasigroups exists. In this thesis, we construct the following two types of codes:

- First, we propose a new check block/character system using T-quasigroups to detect burst-type of errors. Subsequently, we analyze the error-detecting capabilities of the proposed check block system. Additionally, we will prove that the proposed check block system requires lesser number of field operations than Reed-Solomon code to detect single position error. Finally, we demonstrate its applicability in ISBN, SSN and bank routing number.

- Following that, we propose a class of 2-recursive and 3-recursive MDS codes over Q^2 by utilizing the strong orthogonality of quasigroups and extended invertibility of k-ary operations over Q, where Q is a finite commutative ring.

Quasigroup holds significant potential for applications in cryptography, spanning both symmetric and public-key cryptography. This research aims to develop cryptographic protocols leveraging the fundamental characteristics of quasigroups. Concurrently, we aim to enhance the efficiency and security of the proposed cryptographic protocols using the properties and structure of quasigroups.

- We propose a symmetric encryption scheme utilizing a chaining-like mode of operation. Unlike conventional chaining modes such as CBC or CFB, our scheme employs transformed initial vectors to encrypt subsequent blocks. We prove that the proposed scheme is IND-CPA secure and subsequently it achieves IND-CCA2 security after applying the unbalanced Feistel transformation.

Moreover, we analyze the computational complexity and entropy of the proposed encryption scheme. Simultaneously, compare the results with existing lightweight block ciphers based on quasigroups, such as INRU [122] and BCWST [21]. This comparison proves that the proposed scheme can be utilized in designing different lightweight cryptographic primitives.

- In literature, different public key cryptographic protocols has been proposed using quasigroups to achieve quantum security including MQQ-SIG [61], MQQ-ENC [62] etc. The security of MQQ-SIG [61] and MQQ-ENC [62] scheme relies on solving the system of multivariate polynomials over finite field. However, Faugére et al. proved in their work [48] that MQQ-SIG [61] and MQQ-ENC [62] schemes are vulnerable to polynomial-time key recovery attacks.

  This motivates us to design a quantum secure digital signature scheme which is more efficient and secure than MQQ-SIG scheme. Therefore, we propose a new signature scheme using MQQ motivated by the idea of Rainbow scheme for a single field equation. The proposed scheme exhibits resilience against Direct attack, Min-rank attack, High-rank attacks and Differential attack. Additionally, it is also secure against Existential unforgeability under chosen message attack. We prove that after applying the transformation proposed by Wang et al. [126] to the proposed scheme, it is infeasible to find an equivalent good key in polynomial time.

List of Tables

List of Figures

भारतीय प्रौद्योगिकी संस्थान
काशी हिन्दू विश्वविद्यालय

IIT INDIAN INSTITUTE OF TECHNOLOGY
BANARAS HINDU UNIVERSITY

CERTIFICATE

It is certified that the work contained in this thesis titled "**Design and Analysis of Some New Codes and Crypto Schemes Using Quasigroups**" by **Satish Kumar** has been carried out under my supervision and has not been submitted elsewhere for a degree.

It is further certified that the student has fulfilled all the requirements of Comprehensive Examination, Candidacy and SOTA for the award of Ph.D. degree.

Dr. Ashok Ji Gupta
(Supervisor)
Associate Professor
Department of Mathematical Sciences
Indian Institute of Technology
(Banaras Hindu University)
Varanasi, Uttar Pradesh – 221005
India

पर्यवेक्षक/Supervisor
गणितीय विज्ञान विभाग
Department of Mathematical Sciences
भारतीय प्रौद्योगिकी संस्थान
Indian Institute of Technology
(काशी हिन्दू विश्वविद्यालय)
(Banaras Hindu University)
वाराणसी/Varanasi-221005

Dr. Indivar Gupta
(Co-Supervisor)
Scientist 'F'
Scientific Analysis Group
DRDO, Metcalfe House
New Delhi–110054
India

DECLARATION BY THE CANDIDATE

I, **Satish Kumar**, certify that the work embodied in this thesis is my own bonafide work and carried out by me under the supervision of **Dr. Ashok Ji Gupta** from **January, 2019** to **April, 2024** at the **Department of Mathematical Sciences, Indian Institute of Technology (Banaras Hindu University), Varanasi**. The matter embodied in this thesis has not been submitted for the award of any other degree/diploma. I declare that I have faithfully acknowledged and given credits to the research workers wherever their works have been cited in my work in this thesis. I further declare that I have not willfully copied any other's work, paragraphs, text, data, results, etc., reported in journals, books, magazines, reports dissertations, theses, etc., or available at websites and have not included them in this thesis and have not cited as my own work.

Date: 26/04/2024
Place: Varanasi

Satish
(Satish Kumar)

CERTIFICATE BY THE SUPERVISOR

It is certified that the above statement made by the student is correct to the best of my/our knowledge.

Ashok

Dr. Ashok Ji Gupta
Associate Professor
Department of Mathematical Sciences
Indian Institute of Technology (BHU)
Varanasi, Uttar Pradesh – 221005
India

पर्यवेक्षक/Supervisor
गणितीय विज्ञान विभाग
Department of Mathematical Sciences
भारतीय प्रौद्योगिकी संस्थान
Indian Institute of Technology
(काशी हिन्दू विश्वविद्यालय)
(Banaras Hindu University)
वाराणसी/Varanasi-221005

26/04/2024

Head
Department of Mathematical Sciences
Indian Institute of Technology (BHU)
Varanasi, Uttar Pradesh – 221005
India

विभागाध्यक्ष/HEAD
गणितीय विज्ञान विभाग
Department of Mathematical Sciences
भारतीय प्रौद्योगिकी संस्थान
Indian Institute of Technology
(काशी हिन्दू विश्वविद्यालय)
(Banaras Hindu University)
वाराणसी/Varanasi-221005

COPYRIGHT TRANSFER CERTIFICATE

Title of the Thesis: Design and Analysis of Some New Codes and Crypto Schemes Using Quasigroups.

Name of the Student: Satish Kumar

COPYRIGHT TRANSFER

The undersigned hereby assigns to the Indian Institute of Technology (Banaras Hindu University), Varanasi all rights under copyright that may exist in and for the above thesis submitted for the award of the Ph.D. degree.

Date: 26/04/2024
Place: Varanasi

Satish

(Satish Kumar)

Note: However, the author may reproduce or authorize others to reproduce material extracted verbatim from the thesis or derivative of the thesis for author's personal use provided that the source and the Institute copyright notice are indicated.