STUDY OF QUASIGROUPS WITH CRYPTOGRAPHIC SIGNIFICANCE

Ph. D. THESIS

by

TAJENDER KUMAR

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE - 247 667 (INDIA)
DECEMBER, 2018

STUDY OF QUASIGROUPS WITH CRYPTOGRAPHIC SIGNIFICANCE

A THESIS

Submitted in partial fulfilment of the requirements for the award of the degree

of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

by

TAJENDER KUMAR

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE - 247 667 (INDIA)
DECEMBER, 2018

INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis entitled **"STUDY OF QUASIGROUPS WITH CRYPTOGRAPHIC SIGNIFICANCE"** in partial fulfilment of the requirements for the award of the Degree of Doctor of Philosophy and submitted in the Department of Mathematics of the Indian Institute of Technology Roorkee, Roorkee is an authentic record of my own work carried out during a period from January, 2013 to December, 2018 under the supervision of Prof. Sugata Gangopadhyay, Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, Roorkee.

The matter presented in this thesis has not been submitted by me for the award of any other degree of this or any other Institution.

(TAJENDER KUMAR)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

(Sugata Gangopadhyay)
Supervisor

The Ph.D. Viva-Voce Examination of **Mr. Tajender Kumar**, Research Scholar, has been held on March 29, 2019.

Chairman, SRC External Examiner

This is to certify that the student has made all the corrections in the thesis.

Signature of Supervisor Head of the Department

Dated: March 29, 2019

Dedicated

to

Mummy and Papa

Abstract

In this thesis, we study quasigroups with minimum number of associative triples. It is known the number of associative triples are connected to the security criteria of quasigroups based hash function. With the help of the permutations we implement the existing quasigroups and derive the counts on associative triples. We further evolve quasigroups with relatively small number of associative triples by using Genetic algorithm.

Drápel and Kepka [46] have shown that upper bound for associative triples of quasigroup Q isotopic to group $A(Q) \leq |Q|^3-4|Q|^2+6|Q|$, when $|Q| \geq 3$ and $A(Q) \leq |Q|^3-4|Q|^2+8|Q|$, when $|Q|$ is even, where $A(Q)$ is the set of associative triples of quasigroup Q. Grošek and Horák [64] state that best known upper bound for associative triples of any quasigroup Q is less than or equal to $2|Q|^2$. We set $a(Q)$ for minimum value of $A(Q)$, they also proved that for any quasigroup $a(Q) \geq 2|Q| - |I(Q)|$, where $I(Q)$ is the set of all idempotent elements of Q. Only Kotzig and Reischer [87] provided the infinite class of quasigroups with less than $|Q|^2$.

Gligoroski et al. [61] represented quasigroups as vectorial Boolean functions also called substitution boxes (S-boxes). In vectorial Boolean functions, each coordinate function is a Boolean function. First we evolve the balanced Boolean functions by Simulated annealing with best profile (n, d, nl, ac) [31]. Markovski and Mileva [104] generated huge quasigroups from small nonlinear bijections by extended Feistel functions. Snášel et al. [154] also evolved huge quasigroups by Genetic algorithm which are isotopic to modular subtraction quasigroups. For given a quasigroup Q along with three bijections (i.e., permutations) on Q, we can define the isotopic quasigroup. We proposed a new cost function and find the optimized permutations (i.e., isotopy) via Genetic algorithm which give the quasigroups with low number of associative triples.

Markovski and Mileva [104] defined the quasigroups via Feistel network and shown the

outcomes of Feistel network especially as relative to bijection from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. They indentified that Feistel network based quasigroup is highly non-associative with respective to the governing equations obtained from the associativity condition. We solve these equations for different kinds of permutations, i.e., linear permutations, quadratic permutations, APN (almost perfect nonlinear) permutations, differentially 4-uniform permutations and differentially δ-uniform permutations over $\mathbb{F}_2^n$ and derive the counts on associative triples. Further we identify the relation between the cryptographic characterstics, i.e., nonlinearity, differential uniformity and Strict Avalanche Criteria (SAC), of bijection mapping and Feistel network based quasigroup.

Kotzig and Reischer [87] proposed the construction of quasigroups by finite commutative ring, but not necessarily associative or unitary. We implement this construction by two different permutations over $\mathbb{F}_{2^n}$ and derive the counts on associative triples which is satisfy the best known upper bound. Further we also examine how the cryptographic characterstics, i.e., nonlinearity and differential uniformity, affect the quasigroups and using permutations.

Complete mapping permutations are used to construct quasigroups (equivalently, latin squares) which in turn show promise of being applied to design hash functions and block ciphers. Construction of complete mapping permutations by using Feistel structure has been proposed by Markovski and Mileva [104], they used the complete mapping permutations to construct huge quasigroups. Complete mapping permutations have been extensively studied in [8, 34, 93, 123, 162]. Stănică et al. [158] also used the complete mapping permutations to construct a new class of bent-negabent functions. We construct complete mapping permutations by using XS-circuits and give the total counts for particular order. We also construct $\mathcal{K}$-complete mapping permutation which can be used to define uniformly distributed sequences. We find a recursive constrictions that extend a complete mapping of dimension r to a complete mapping of dimension n, where $r \leq n$.

List of Publications

Journal

1. T. Kumar and S. Gangopadhyay, A Genetic Algorithm for Evolving Quasigroups with Minimum Associative triples, Soft Computing, communicated (21th Aug. 2018).

Conferences

1. T. Kumar and S. Gangopadhyay, Enhance the nonlinearity of optimizing Boolean function via permutations, In International Conference on Electrical, Electronics and Optimization Techniques (ICEEOT), IEEE, pp. 430–433, March 3 - 5, 2016.

2. T. Kumar and S. Gangopadhyay, The Cryptographic Properties of Feistel Network based Quasigroups, In International Conference on Emerging Technologies in Data Mining and Information Security, February 23 - 25, 2018, University of Engineering & Management (UEM), Kolkata, India.

Book Chapter

1. T. Kumar and S. Gangopadhyay, The Cryptographic Properties of Feistel Network based Quasigroups, Emerging Technologies in Data Mining and Information Security, Proceedings of IEMIS 2018, vol. 3, pp. 539–549, 2019.

Acknowledgement

I would like to express my heartfelt gratitude and sincere thanks to my supervisor Prof. Sugata Gangopadhyay , Department of Computer Science and Engineering, Indian Institute of Technology Roorkee for his guidance, help and encouragement without which it would not have been possible for me to complete this work. It has been a great experience and joy to work with him. I consider myself extremely blessed to have worked under his scholarly guidance. His truly scientific intuition and broad vision inspired and enriched my growth as a student and researcher. The critical suggestions and valuable comments rendered by him during the discussions are deeply acknowledged. This work would have not been possible without his guidance, support and encouragement. Under his guidance I successfully overcome many difficulties and learned a lot. I humbly acknowledge a lifetime's gratitude to him.

I am thankful to Prof. N. Sukavanam, Head of the Department of Mathematics, IIT Roorkee, and Chairman, SRC; Prof. Kusum Deep, Chairman, DRC, for providing me with the basic facilities. I am also thankful to Dr. Sandip Banerjee, Internal Expert, Department of Mathematics, Dr. Sudeb Dasgupta, External Expert, Department of Electronics and Communication Engineering, for their support and helpful attitude during my Ph.D. program. I would also like to thank all the staff members in the department for creating the availing environment during the tenure of this work.

I would like to express sincerest thanks to my family who supported me throughout all the ups and downs in my life. I wish to thank my mother and aunties for their love, care and affection. I would also like to thank my sister Km. Lokesh and brother Yogeshwar for their love and affection. Very special thanks to my father Sh. Ram Daas for his constant support and love.

I am very blessed to have some great friends who made my stay pleasant and happier.

It's my good fortune to gratefully acknowledge the support of some special individuals who were always there beside me during the happy as well as hard moments to push me and motivate me. I am thankful to my childhood friends Arvind Thakur, Rajkumar, Dharmveer, Rajesh Bhaskar, Ajeet Singh and Manish Kumar who always motivated me. I am thankful to Sudhakar Yadav, Rohit Kumar, Rakesh Kumar Meena, Pankaj Kumar, Om Prakash Yadav, Mohan Tiwari, Ajay Kumar, Kiran Kumar Behera, Harshit Mahendra, Sudhir Kumar, Hari Raj and Sonia Rani for their cooperation, support and for making my stay at IIT Roorkee a memorable one. Very special thanks to my lab colleagues Bimal Mandal, Avinash Kumar, Nishant Sinha and Pratap Kumar Behera for providing their cooperation, support, healthy and progressive research environment.

I would like to thank all the reviewers of research papers for providing many valuable suggestions and criticism which had major influence to improve the quality of this work. I would like to acknowledge the contribution rendered by Ministry of Human Recourse Development (MHRD), by providing the necessary financial support in form of JRF/SRF to carry out this work.

Finally, I wish to acknowledge all those whose names have not figured above, but have helped me in any form during the entire period of my research work.

Roorkee

December 26, 2018 (Tajender Kumar)

List of Tables

Contents

Notations and Abbreviations

$\mathbb{Z}$: The set of integers.

$\mathbb{Q}$: The set of rational numbers.

$\mathbb{R}$: The set of real numbers.

S^* : The set of all elements of S except 0.

$|S|$: Cardinality of the set S.

$a(Q)$: The minimum number of associative triples in quasigroup Q.

$\mathbb{Z}_n$: The set of integers modulo n.

$\mathbb{F}_p$: Prime field of characteristic p.

$\mathbb{F}_p^n$: $\{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_p, 1 \leq i \leq n\}$, the vector space of dimension n over $\mathbb{F}_p$.

$\mathbb{F}_{p^n}$: Extension field of degree n over $\mathbb{F}_p$.

$\mathbb{F}_{p^n}^*$: The set of all nonzero elements of $\mathbb{F}_{p^n}$.

$\mathbb{F}_{p^n}[X]$: Polynomial ring over $\mathbb{F}_{p^n}$.

$\dim E$: The dimension of a vector space E.

Tr_l^n : Trace function from $\mathbb{F}_{p^n}$ to the subfield $\mathbb{F}_{p^l}$, $\mathrm{Tr}_l^n(x) = \sum_{i=0}^{k-1} x^{p^{il}}$, $x \in \mathbb{F}_{p^n}$ and $n = kl$.

$\mathcal{B}_n$: The set of all Boolean functions in n variables.

$\mathcal{B}_{n,m}$: The set of all vectorial Boolean functions in (n, m) variables.

$wt(f)$: Weight of a Boolean function f, total number of nonzero outputs of $f \in \mathcal{B}_n$.

$\deg(f)$: The algebraic degree of a Boolean function $f \in \mathcal{B}_n$.

ANF : Algebraic Normal Form.

APN : Almost Perfect Nonlinear.

AB : Almost Bent.

$GL(n, \mathbb{F}_p)$: The group of invertable $\mathbb{F}_p$-linear transformations acting on $\mathbb{F}_{p^n}$.

Chapter 1

Introduction

A quasigroup $(Q, *)$ is a set Q equipped with a closed binary operation $*$ on Q and when we choose any two elements from Q, the third element is determined by the equation $x * y = z$ uniquely. Hence the multiplication table of any quasigroup is equivalent to a Latin square. Many important results on quasigroups are discovered by Euler [51–53], Cayley [25, 26], Schröder [69] and Moufang [125]. These results made a strong relationship between the area of Algebra and Combinatorics. From the algebraic point of view quasigroups were intensively studied by Norton [127], Drápel [44, 46], Ježek and Kepka [71], Kotzig and Reischer [87] and recently by Grošek and Horák [64]. On further discussion on quasigroups we refer some books [76,148,151]. Therefore quasigroups inspired the people all throughout 20th and 21st centuray. We are interested in quasigroups from the cryptographic point of view.

Cryptographic primitives are based on the concept of Number theory, Group theory, Finite field theory and Boolean algebra and Boolean functions. All these mathematical structres are commutative and associative. Besides these quasigroups are non-associative. Non-associative mathematical structures also play a important role in cryptology [37, 39, 75, 112]. A science in which we study both parts cryptography and cryptanalysis is called cryptology.

• Cryptography: It is an art and science which deals the designing part of a cryptosystems in such a way when adversaries can't get any information.

• Cryptanalysis: It is an art and science which deals the breaking part of a cryptosystems in such a way when adversaries get the information without knowing the secret key.

Thus cryptology plays an extensive role in the protection of information and data that is either in transit or in storage. Hence in order to maintain and increase the privacy, integrity, and protection of such information and computing systems against adversaries in an era of rapidly advancing technology with cyber warfare [4, 70] and numerous cyber security threats [15, 88, 165, 169] the theory and practice of cryptology must be thoroughly researched and developed via the scientific method and the mathematical method. The methods of cryptography have become increasingly complex with a rapidly expanding application domain. Modern cryptography is based heavily on the disciplines of mathematics, computer science and electrical engineering. The design of a cryptographic algorithm is based on assumptions of computational hardness, where the primary objective is to make such cryptographic systems computationally infeasible for an attacker. Although it is theoretically feasible to break such a cryptographic system, it must be practically infeasible to do so in any known workable situation or context; in this case, the system is considered to be computationally secure.

The computational security of a cryptographic system depends greatly on the underlying algebraic structures and operations that are used to build its algorithm and implementation. Finite groups and Galois fields [56, 96] are fundamental algebraic structures that are used to construct cryptographic systems. Therefore in order to assess the degree of protection, strength, and reliability that such a system offers, it is crucial to rigorously evaluate the underlying finite groups and Galois fields via the scientific method and the mathematical method.

Thus the structure of any finite group is encoded with a Cayley table (a corresponding latin square) and the structure of a Galois field is encoded with two Cayley tables (two corresponding latin squares), then many key properties of a given finite group or Galois field can be obtained by evaluating its representative latin square(s). This implies that latin squares are essential to cyber security because they can be directly utilized to evaluate the computational security of cryptographic systems.

1.1 Definitions and notations

Let $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{R}$ be the set of natural numbers, integers and real numbers, respectively. The cartesian product of sets $S_1, S_2, \ldots, S_n$ is the set of all ordered $n-$tuples $(a_1, a_2, \ldots, a_n)$,

where $a_i \in S_i$, and its set denoted by

$$S_1 \times S_2 \times \cdots \times S_n = \prod_{i=1}^{n} S_i.$$

If $S_1 = S_2 = \cdots = S_n = S$, this implies that $S \times S \times \cdots \times S = S^n = \{(a_1, a_2, \ldots, a_n) | a_i \in S_i, 1 \leq i \leq n\}$. A binary relation on a set Q is any subset of the set $Q \times Q$.

Definition 1.1.1. *Let Q be a set. A binary operation on Q is a function that assigns each ordered pair of elements of Q to an element of Q.*

Example 1.1.2. *Define $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $n * m = n + m$ for all $n, m \in \mathbb{Z}$. Then $*$ is an binary operation on $\mathbb{Z}$.*

Definition 1.1.3. *A binary groupiod $(Q, *)$ is a non-empty set Q together with a binary operation $*$.*

Example 1.1.4. *Let $Q = \{a, b, c\}$, then groupiod $(Q, *)$ is defined by Cayley table*

$*$	a	b	c
a	b	a	c
b	a	c	b
c	a	b	c

1.2 Quasigroup

A pair $(Q, *)$ is called a quasigroup if the operation $*$ is closed on Q and the equations:

$$a * x = b,$$

$$x * a = b.$$

have unique solution for every $a, b \in Q$.

Example 1.2.1. *The set of integers $\mathbb{Z}$ with subtraction forms a quasigroups.*

Example 1.2.2. *The set of all rational numbers $\mathbb{Q}^*$ or real numbers $\mathbb{R}^*$ forms a quasigroup with respect of division as the binary operations.*

Example 1.2.3. *More generally, the set of nonzero elements of any division algebra form a quasigroup.*

Moreover, we can also define the quasigroup with the help of modular subtraction.

Definition 1.2.4. *Suppose that n is any positive integer and a and b in $\mathbb{Z}$ is said to be congruent to b, written as $a \equiv b \ mod(n)$ if $n|(b-a)$.*

Definition 1.2.5. *Let $n(>0)$ and a be integers. The congruence class of a modulo n is the set of all integers which have the remainder equal to a when a divided by n. It is defined by*

$$[a]_n = \{x \in \mathbb{Z} | x \equiv a \ mod(n)\}.$$

The collection of all congruence classes modulo n is called the set of integers modulo n, denoted by $\mathbb{Z}_n$. The any element $[a]_n$ of $\mathbb{Z}_n$, we denoted by a.

Example 1.2.6. *Let $Q = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ and $* : Q \times Q \to Q$ be defined as:*

$$x * y = x - y \ mod \ (4).$$

Then $(Q, *)$ is a quasigroup, and the Cayley table of Q is given by

$*$	*0*	*1*	*2*	*3*
0	*0*	*3*	*2*	*1*
1	*1*	*0*	*3*	*2*
2	*2*	*1*	*0*	*3*
3	*3*	*2*	*1*	*0*

The Cayley table of the quasigroup given in Example 1.2.6. is equivalent to Latin square.

1.3 Latin square

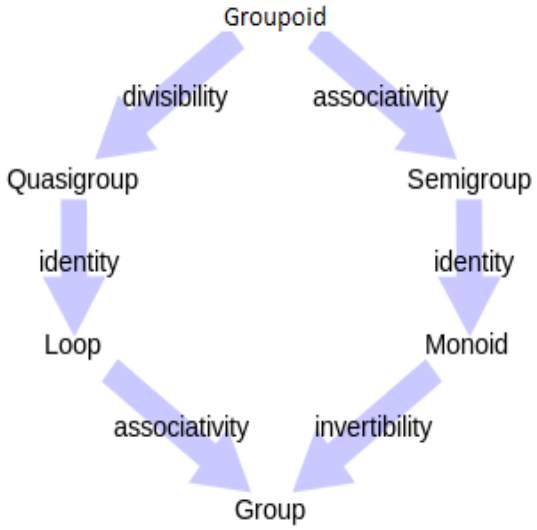
A latin rectangle of oreder $k \times n$ is a $k \times n$ matrix such that the entries in each row and each column are distinct. A latin square of order n is an $n \times n$ latin rectangle.

Definition 1.3.1. *A Latin square of order n is an $n \times n$ array filled with n different symbols, each ocurring exactly once in each row and exactly once in each column.*

Example 1.3.2. *The corresponding equivalent latin square for Example* 1.2.6 *is as follows*

0	*3*	*2*	*1*
1	*0*	*3*	*2*
2	*1*	*0*	*3*
3	*2*	*1*	*0*

Quasigroups differ from groups mainly in that they need not be associative. A quasigroup with an identity element is called a loop.



Proposition 1.3.3. *Let Q be a set and $*$ be a binary operation on Q. The following statements are equivalent:*

(i) *Q is an associative quasigroup.*

(ii) *Q is an associative loop.*

(iii) *Q is a group.*

Proof. We will prove this in the following direction $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.

$(i) \Rightarrow (ii)$. Let $x \in Q$, and $x_l, x_r \in Q$ such that $(x_l * x) * x_r = x_l * (x * x_r)$. This implies that $x_l * x = x = x * x_r$. So $x * x_r^2 = x * x_r = x$, which shows that $x_r^2 = x_r$. Let $a \in Q$ be such that $x_r * a = x$. Then $x_l * x_r * a = x_l * x = x = x_r * a$, so that $x_l * x_r = x_r = x_r^2$, or $x_l = x_r$. Set $e = x_r$. For any $y \in Q$, we have $e * y = e^2 * y$, so $y = e * y$. Similarly, $y * e = y * e^2$ implies $y = y * e$. This shows that e is an identity of Q.

$(ii) \Rightarrow (iii)$. First note that all of the group axioms are automatically satisfied in Q under $*$, except the existence of an (two-sided) inverse element, which we are going to verify presently. For every $x \in Q$ there are unique elements y and z such that $x * y = z * x = e$.

Then $y = e * y = (z * x) * y = z * (x * y) = z * e = z$. This shows that x is the inverse element for both y and z. Therefore G is a group under $*$.
$(iii) \Rightarrow (i)$. Every group is clearly a quasigroup and the binary operation is associative. ■

1.4 Associative triples in quasigroups

In quasi group $(Q, *)$, Let $A(Q)$ and $B(Q)$ be defined as

$$A(Q) = \{(x, y, z) \in Q^3 : \ (x * y) * z = x * (y * z)\},$$
$$B(Q) = Q^3 - A(Q).$$

Let $a(Q) = |A(Q)|$ and $b(Q) = |B(Q)|$. If Q is finite with $n = |Q|$ then

$$a(Q) + b(Q) = n^3.$$

There exist a unique left identity a_l and a unique right identity a_r $\forall$ $a \in Q$. Thus we get

$$a_l * a = a,$$
$$a * a_r = a.$$

Hence the triple (a_l, a, a_r) is associative for each $a \in Q$ and the lower bound for $a(Q)$ is $a(Q) \geq n$, we refer to [71]. Therefore $n \leq a(Q) \leq n^3$.

A quasigroup is said to be di-associative if exactly two of elements among x, y and z are distinct in $A(Q)$ and mono-associative when all three elements x, y and z are equal in $A(Q)$.
The following theorems are proven by Norton [127].

Theorem 1.4.1. [127, Theorem II] *Let $(Q, *)$ be a quasigroup for which both Q and $Q^2 = \{q * q : \forall q \in Q\}$ contain a "sufficient number" of elements, then Q is di-associative.*

Theorem 1.4.2. [127, Theorem III] *If a quasigroup $(Q, *)$ satisfy the constraint $x*(x*y) = (x * x) * y$ when $x \neq y \in Q$, then Q is mono-associative.*

For any quasigroup, we can say that

$$\text{Associativity (tri-associativity)} \implies \text{di-associativity} \implies \text{mono-associativity.}$$

Our target is to reduce the upper bound of $a(Q)$ and find out the exact number of $a(Q)$ for given quasigroup $(Q, *)$ of order n.

1.5 Boolean functions

Any function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function in n variables. The set of all n variables Boolean functions is denoted by $\mathcal{B}_n$ and its cardinality is 2^{2^n}. Boolean functions were extensively studied by more references. For Cusick and Stănică and Mesnager, we refer to their books [18, 20, 33, 111].

There are three standard representations of Boolean functions, namely truth-table representation, algebraic normal form (ANF) and trace representation. These are as follows:

Truth-table representation

Boolean function is also defined by truth table, i.e., $f(x_1, x_2, \ldots, x_n)$ over $\mathbb{F}_2^n$ is represented by a binary string of length 2^n,

$$[f(0, \ldots, 0, 0), f(0, \ldots, 0, 1), f(0, \ldots, 1, 0), \ldots, f(1, \ldots, 1, 1)].$$

Example 1.5.1. *Boolean function in* 3 *variables defined as in Table* 1.1 *in its truth table form as* $[f(0, \ldots, 0, 0), f(0, \ldots, 0, 1), f(0, \ldots, 1, 0), \ldots, f(1, \ldots, 1, 1)]$

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

Table 1.1: Truth-table of a Boolean function in 3 variables

Definition 1.5.2. *The Hamming weight of an n variables Boolean function f is the number of $1's$ in the truth table and it is denoted by $wt(f)$. For a Boolean function on $\mathbb{F}_2^n$, let $\Omega_f = \{x \in \mathbb{F}_2^n : f(x) = 1\}$ be the support of f.*

Definition 1.5.3. *The Hamming distance between two Boolean functions $f, g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$, denoted by $d(f, g)$, is defined as*

$$d(f, g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}| = wt(f \oplus g).$$

Example 1.5.4. *Suppose f and $g \in \mathcal{B}_3$ are Boolean functions with outputs $(1, 0, 1, 0, 0, 0, 0, 1)$ and $(0, 1, 1, 1, 0, 0, 1, 0)$ respectively. Then*

$$wt(f) = 3, \quad wt(g) = 4 \quad \text{and} \quad d(f, g) = 5.$$

Algebraic normal form

Any Boolean function $f \in \mathcal{B}_n$ can be uniquely expressed as a polynomial in $\mathbb{F}_2[x_1, x_2, \ldots, x_n]/\langle x_1^2 + x_1, \ldots, x_n^2 + x_n \rangle$. This form is called Algebraic normal form (ANF) of f, defined as:

$$f(x_1, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_a(\prod_{i=1}^{n} x_i^{a_i}), \tag{1.5.1}$$

where $\mu_a \in \mathbb{F}_2$. Each term of the form $\prod_{i=1}^{m} x_i^{a_i}$ is called a monomial.

Definition 1.5.5. *The algebraic degree of Boolean function $f \in \mathcal{B}_n$ is defined by number of variables in the highest order monomial with nonzero coefficient in its (ANF), denoted by $deg(f)$.*

$$deg(f) = \max_{a\in\mathbb{F}_2}\{wt(a) : \mu_a \neq 0\}.$$

The degree of a monomial $\prod_{i=1}^{m} x_i^{a_i}$ is $wt(a)$.

Definition 1.5.6. *A linear Boolean function is denoted by*

$$L_w(x) = w_1x_1 \oplus w_2x_2 \cdots \oplus w_nx_n,$$

where $w \in \mathbb{F}_2^n$ and w_ix_i denotes the bitwise and operation of the i-th bit of w and x, $\oplus$ denotes bitwise xor operation where addition is over $\mathbb{F}_2^n$.

Definition 1.5.7. *The affine functions are defined by the set of linear functions and their complements:*

$$A_{w,c}(x) = L_w(x) + c, \text{ where } c \in \mathbb{F}_2.$$

The set of all afine functions $\mathcal{A}_n$ is define by

$$\mathcal{A}_n = \{A_{w,c}(x) : w \in \mathbb{F}_2^n, c \in \mathbb{F}_2\}.$$

For two vectors $u,\ v \in \mathbb{F}_2^n$, the canonical dot product is defined as:

$$u \cdot v = \sum_{i=1}^{n} u_i v_i.$$

Thus we get the set of all 2^n linear functions, i.e., $A_{w,0} = L_w$, when w varies all over $\mathbb{F}_2^n$.

Example 1.5.8. *The algebraic normal form (ANF) of f given in Table 1.1 is*

$$f(x_1, x_2, x_3) = x_3x_2 + x_3x_1 + x_3 + x_2.$$

Thus the degree of f is 2.

We denote the extention field of degree n over $\mathbb{F}_2$ by $\mathbb{F}_{2^n}$ and the unit group therein by $\mathbb{F}_{2^n}^*$. Let $p(x)$ be a primitive polynomial of degree n then $\mathbb{F}_{2^n}$ is defined as

$$\mathbb{F}_{2^n} = \mathbb{F}_2[x]/\langle p(x)\rangle = \{c_0 + c_1x + \cdots + c_{n-1}x^{n-1} : c_i \in \mathbb{F}_2, i = 0, 1, \ldots, n-1\}.$$

$\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ both are n dimension vector spaces over $\mathbb{F}_2$. Let $B = \{b_1, b_2, \ldots, b_n\}$ be an $\mathbb{F}_2$ a basis of $\mathbb{F}_{2^n}$. Then any element $a \in \mathbb{F}_{2^n}$ can be written as

$$a = x_1b_1 + x_2b_2 + \cdots + x_nb_n$$

where $x_i \in \mathbb{F}_2$, $i = 1, 2, \ldots, n$. Using the following mapping one can check that $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ are vector isomorphism over $\mathbb{F}_2$:

$$x = (x_1, x_2, \ldots, x_n) \longrightarrow x_1b_1 + x_2b_2 + \cdots + x_nb_n$$

where $\{b_1, b_2, \ldots, b_n\}$ is an $\mathbb{F}_2$ basis of $\mathbb{F}_{2^n}$. With respect to the basis defined as above, the n-tuple vector $(x_1, x_2, \ldots, x_n)$ is called the coordinates of $x \in \mathbb{F}_{2^n}$.

Example 1.5.9. *Let α be a root of primitive polynomial $x^3 + x + 1 = 0$, then the one to one correspondance between $\mathbb{F}_2^3$ and $\mathbb{F}_{2^3}$ is given by*

$\mathbb{F}_{2^3}$	$\mathbb{F}_2^3$
0	(0, 0, 0)
1	(0, 0, 1)
α	(0, 1, 0)
α^2	(1, 0, 0)
$\alpha^3 = \alpha + 1$	(0, 1, 1)
$\alpha^4 = \alpha^2 + \alpha$	(1, 1, 0)
$\alpha^5 = \alpha^2 + \alpha + 1$	(1, 1, 1)
$\alpha^6 = \alpha^2 + 1$	(1, 0, 1)

Table 1.2: Correspondance between finite fields and vector spaces

Definition 1.5.10. *The* trace *function $tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by*

$$tr_1^n(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}, \ \textit{for all } x \in \mathbb{F}_{2^n}.$$

Given any $x, y \in \mathbb{F}_{2^n}$, $tr_1^n(xy)$ is an inner product of x and y. For any $w \in \mathbb{F}_{2^n}$, $L_w \in \mathcal{B}_n$ denotes the linear function defined by $L_w(x) = tr_1^n(wx)$ for all $x \in \mathbb{F}_{2^n}$.

A Boolean function $f \in \mathcal{B}_n$ is said to be a monomial Boolean function if there exits $\lambda \in \mathbb{F}_{2^n}$ and a positive integer d such that $f(x) = tr_1^n(\lambda x^d)$ for all $x \in \mathbb{F}_{2^n}$. The positive integer d is said to be the exponent defining the function f, whereas $deg(f) = wt(d)$.

Walsh-Hadamard transform

The discrete Fourier transform of Boolean function is called Walsh-Hadamard transform, Walsh transform or Walsh spectrum. Walsh-Hadamard transform are involved for determining the many cryptographic properties of Boolean functions.

Definition 1.5.11. *The Walsh transform of a Boolean function f on $\mathbb{F}_2^n$ is the mapping $W_f : \mathbb{F}_2^n \longrightarrow \mathbb{R}$, defined as*

$$W_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + L_w(x)}$$

It expresses a Boolean function in terms of its cross correlation to all linear functions. We denote the maximum absolute value by

$$WH_{max}(f) = \max_{w \in \mathbb{F}_2^n} \mid W_f(w) \mid . \tag{1.5.2}$$

The multiset $[W_f(w) : w \in \mathbb{F}_2^n]$ *is said to be the Walsh spectrum of* f*. The absolute value of the Walsh spectrum of* f *is at most* 2^n*. It is also related to the nonlinearity of* f*.*

It is also defined over the finite field $\mathbb{F}_{2^n}$ as

$$W_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+tr_1^n(wx)} \quad \text{for all} \quad w \in \mathbb{F}_{2^n}. \tag{1.5.3}$$

Proposition 1.5.12. [33, Corollary 2.19] *Any Boolean function* $f \in \mathcal{B}_n$ *satisfies the following identity*

$$\sum_{w \in \mathbb{F}_2^n} W_f^2(w) = 2^{2n}. \tag{1.5.4}$$

This identity is called Parseval's identity. It can be shown that $\max\{|W_f(w)| : w \in \mathbb{F}_2^n\} \geq 2^{n/2}$.

1.5.1 Cryptographic characteristics of Boolean functions

There are following cryptographic significance of Boolean functions.

Algebraic Degree

The algebraic degree of Boolean function gives the linear complexity of the pseudo-random generator. To resist the Berlekamp-Messey attack [18, 105, 110] and Rønjom-Helleseth attack [141] of a cryptosystem it is needed that Boolean function used in pseudo-random generators posses optimal algebraic degree. From the algebraic normal form of a Boolean function we know that the maximum algebraic degree of a Boolean function in n variables is at most n.

Balancedness

A Boolean function $f \in \mathcal{B}_n$ is said to be balanced if the truth-table of f has equal number of 1's and 0's, i.e., $wt(f) = 2^{n-1}$. There are many balanced functions in $\mathcal{B}_n$. Boolean functions

used in a cryptosystem must be balanced otherwise a cryptosystem is unable to prevent the distinguishing attacks [20] as the attacker gain some statistical information between plaintext and ciphertext of a stream cipher. If a Boolean function is balanced then the algebraic degree is at most $n-1$. It is to be noted that any nonconstant affine function is balanced.

Example 1.5.13. *Suppose $f, g \in \mathcal{B}_3$ are Boolean functions with outputs $(1,0,1,0,0,0,0,1)$ and $(0,1,1,1,0,0,1,0)$ respectively. Here g is balanced and f is not balanced.*

Crosscorrelation and Autocorrelation

Let $f, g \in \mathcal{B}_3$. Then the crosscorrelation between f and g at $w \in \mathbb{F}_2^n$, $\mathcal{C}_{f,g}(w)$ is defined as

$$\mathcal{C}_{f,g}(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x+w)}.$$

Two Boolean functions f and g in n variables are called uncorrelated of order r, $0 \leq r \leq n$ if $\mathcal{C}_{f,g}(w) = 0$, for all $w \in \mathbb{F}_2^n$ with $0 \leq wt(w) \leq r$. If for all $w \in \mathbb{F}_2^n$, $\mathcal{C}_{f,g}(w) = 0$ then f and g are perfectly uncorrelated, we refer to [33, 111, 145].

Example 1.5.14. *Suppose f and $g \in \mathcal{B}_3$ are Boolean functions with outputs $(1,0,1,0,0,0,0,1)$ and $(0,1,1,1,0,0,1,0)$ respectively. Then the crosscorelation value of f and g is $\mathcal{C}_{f,g}(w) = 6$.*

The autocorrelation of $f \in \mathcal{B}_n$ at $w \in \mathbb{F}_2^n, \mathcal{C}_f(w)$, is defined as

$$\mathcal{C}_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+w)}.$$

It is obvious that if $w = 0$ then $\mathcal{C}_f(w)$ is equal to 2^n.

Nonlinearity

The nonlinearity $nl(f)$ of a Boolean function $f \in \mathcal{B}_n$ is its minimum distance to any affine function. Nonlinearity of an n variables Boolean function f represents the dissimilarity between f and the set of n variables affine functions, $\mathcal{A}_n$, that of f bears closest bitwise similarity which is measured by hamming distance between f and $\mathcal{A}_n$. To resist the affine approximation attacks [41] this value is as large as possible nonlinearity and Walsh spectrum of f is related as follows:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{w \in \mathbb{F}_2^n} |W_f(w)|. \tag{1.5.5}$$

Using Parseval's identity, we can conclude the upper bound of nonlinearity. The nonlinearity of an Boolean function is at most $2^{n-1} - 2^{\frac{n}{2}-1}$. Rothaus [142] introduced the idea of nonlinearity and Matsui [106] discovered the relationship between nonlinearity and explicit attack on stream ciphers. For a detailed study we refere to [12, 18, 20, 72, 74, 85, 142, 144].

Bent functions

Boolean functions used as cryptographic premitives must resist affine approximation, which is achieved by having high nonlinearity. The bent functions defined on n variables have the maximum nonlinearity, i.e., they offer maximum resistance to affine approximation.

Definition 1.5.15. *A Boolean function $f \in \mathcal{B}_n$ is said to be a bent if*

$$W_f(w) = \pm 2^{\frac{n}{2}} \quad \textit{for all} \quad w \in \mathbb{F}_2^n.$$

From Equation (1.5.5), $f \in \mathcal{B}_n$ is said to be bent if and only if its nonlinearity is maximum, i.e.,

$$nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Example 1.5.16. *Suppose $f \in \mathcal{B}_4$ are Boolean functions with ANF $f(x_1, x_2, x_3, x_4) = 1 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$. Then f is a bent function as $|W_f(w)| = 4$ for all $w \in \mathbb{F}_2^n$ and $nl(f) = 6$.*

Similarly Almost bent functions and semi-bent function can be defined as follows, we refer to [23] [58] [63].

- Almost bent Functions (AB): If n is odd

$$W_f(w) \in \{0, \pm 2^{\frac{n+1}{2}}\} \quad \text{for all} \quad w \in \mathbb{F}_2^n.$$

Example 1.5.17. *Suppose $f \in \mathcal{B}_3$ is Boolean functions with outputs $(0, 1, 1, 0, 1, 0, 1, 0)$. Then f is a almost bent function because its Walsh-hadamard spectrum is $(0, 4, 0, -4, 0, -4, 0, -4)$.*

- Semi-bent Functions:

  If n is even

  $$W_f(w) \in \{0, \pm 2^{\frac{n+2}{2}}\} \quad \text{for all} \quad w \in \mathbb{F}_2^n.$$

  If n is odd

  $$W_f(w) \in \{0, \pm 2^{\frac{n+1}{2}}\} \quad \text{for all} \quad w \in \mathbb{F}_2^n.$$

Example 1.5.18. *Suppose $f \in \mathcal{B}_4$ are Boolean functions with outputs $(0,1,1,0,1,0,1,0,0,1,1,0,1,0,1,0)$. Then f is a semi bent function because its Walsh-hadamard spectrum is $(0,8,0,-8,0,-8,0,-8,0,0,0,0,0,0,0,0)$.*

1.5.2 Vectorial Boolean functions

Let $f_0, f_1, ..., f_{m-1} \in \mathcal{B}_n$ and a Boolean mapping $\mathcal{F} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ is defined as:

$$\mathcal{F}(x) = (f_0(x), f_1(x), ..., f_{m-1}(x)),$$

is called a vectorial Boolean function and $f_0, f_1, ..., f_{m-1}$ are called coordinate functions, where $f_k : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ and $f_k \in \mathcal{B}_n,\ k = 0, 1, \ldots, m-1$. The set of (n, m) variables vectorial Boolean functions is denoted by $\mathcal{B}_{n,m}$ and its cardinality is 2^{m2^n}.

Walsh-Hadamard transform of vectorial Boolean function

Besides the coordinates, all linear combinations of the coordinates are involved for determining the cryptographic properties of a vectorial Boolean function, in the sense of the following definition.

Definition 1.5.19. *Let $\mathcal{F}$ be a vectorial Boolean function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$. The Boolean components of $\mathcal{F}$ are the n variables Boolean functions*

$$\mathcal{F}_\lambda : x \to \lambda \cdot \mathcal{F}(x),$$

for any $\lambda \in \mathbb{F}_2^m$. The component corresponding to $\lambda = 0$ is called the zero (or trivial) component.

Definition 1.5.20. *The nonlinearity $nl(\mathcal{F})$ of an (n, m) variables vectorial Boolean function is the minimum nonlinearity of all the component functions $x \in \mathbb{F}_2^n \mapsto \lambda \cdot \mathcal{F}(x), \lambda \in$*

$\mathbb{F}_2^m, \lambda \neq 0$.

The Walsh transform of a vectorial Boolean function $\mathcal{F} \in \mathcal{B}_{n,m}$ is the mapping $W_{\mathcal{F}} : \mathbb{F}_2^n \times \mathbb{F}_2^m \longrightarrow \mathbb{Z}$, defined as:

$$W_{\mathcal{F}}(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a.x+b.\mathcal{F}(x)}.$$

Moreover, the linearity [16] of $\mathcal{F}$ is

$$\mathcal{L}(\mathcal{F}) = \max_{b \in (\mathbb{F}_2^n)^*} \mathcal{L}(\mathcal{F}_b) = \max_{a \in \mathbb{F}_2^n, b \in (\mathbb{F}_2^n)^*} \mid W_{\mathcal{F}}(a,b) \mid,$$

and the nonlinearity [19] of $\mathcal{F}$ is

$$nl(\mathcal{F}) = 2^{n-1} - \frac{1}{2}(\mathcal{L}(\mathcal{F})),$$

or

$$nl(\mathcal{F}) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n, b \in (\mathbb{F}_2^n)^*} \mid W_{\mathcal{F}}(a,b) \mid .$$

The vectorial Boolean functions also defined over finite fields. Let $\mathcal{F}$ be a vectorial Boolean function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$. Then the above definitions are transform as follows:

Definition 1.5.21. *Let $\mathcal{F}$ be an vectorial Boolean function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$. The Boolean components of $\mathcal{F}$ are the n variables Boolean functions*

$$\mathcal{F}_\lambda : x \to tr_1^m(\lambda \mathcal{F}(x)),$$

for any $\lambda \in \mathbb{F}_{2^m}$. The component corresponding to $\lambda = 0$ is called the zero (or trivial) component.

Definition 1.5.22. *The nonlinearity $nl(\mathcal{F})$ of an (n,m) variables vectorial Boolean function is the minimum nonlinearity of all the component functions $x \in \mathbb{F}_{2^n} \mapsto tr_1^m(\lambda \mathcal{F}(x)), \lambda \in \mathbb{F}_{2^m}, \lambda \neq 0$.*

In the bivariate case, where $f : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$, insted of Equation (1.5.3) we have

$$W_f(u,v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x,y)+tr_1^n(ux)+tr_1^n(vx)} \quad \text{for all} \quad (u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}.$$

Differential uniformity

The derivative of the vectorial Boolean function $\mathcal{F} \in \mathcal{B}_{n,m}$ in the direction of $a \in \mathbb{F}_2^n$ is defined as

$$D_{\mathcal{F}}(a) = \mathcal{F}(x+a) + \mathcal{F}(x).$$

Definition 1.5.23. [129, Differential uniformity] *Let $\mathcal{F}$ be a vectorial Boolean function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. The derivative of $\mathcal{F}$ for differences pair (a,b) in $\mathbb{F}_2^n$ is defined as:*

$$D_{\mathcal{F}}(a \to b) = \{x \in \mathbb{F}_2^n | \mathcal{F}(x \oplus a) \oplus \mathcal{F}(x) = b\}.$$

The cardinality of the $D_{\mathcal{F}}(a \to b)$ is correspond to the entry at (a,b) in the difference table of $\mathcal{F}$. It is denoted by $\delta_{\mathcal{F}}(a,b)$.

In addition, the diffrential uniformity of $\mathcal{F}$ is given by

$$\delta(\mathcal{F}) = \max_{a \neq 0, b} \delta_{\mathcal{F}}(a,b).$$

Therefore the differential uniformity of a vectorial Boolean function is always even or $\delta(\mathcal{F}) \geq 2$.

Condition for Differential uniformity:

The differential uniformity is achieved based on the value of m and n. The vectorial Boolean function $\mathcal{F} : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ has

Case-1 [128, Theorem 3.2]: for $n > m$ the minimum differential uniformity 2^{n-m} is reached if and only if $2m \leq n$ and n is even. For $n/2 < m < n$ the minimum differential uniformity is unknown.

Case-2 [131, Section 3]: for $n \leq m$ the minimum differential uniformity is 2. A function which reaches this bound is called almost perfect nonlinear (APN).

Case-3 [130, Section 3]: for $n < m$ the minimum differential uniformity is 2 and can be reached by simple modification of APN function.

Example 1.5.24. *Suppose $\mathcal{F} \in \mathcal{B}_{3,3}$ is vectorial Boolean function with $\mathcal{F}(x_1,x_2,x_3) = (x_1x_3 + x_2x_3 + x_2, x_1 + x_2 + x_1x_3, x_1 + x_2 + x_3 + x_1x_2)$. Then differential uniformity of $\mathcal{F}$ is 2 so it is APN.*

	(0,0,0)	(0,0,1)	(0,1,0)	(0,1,1)	(1,0,0)	(1,0,1)	(1,1,0)	(1,1,1)
(0,0,0)	-	-	-	-	-	-	-	-
(0,0,1)	-	$\{(0,0,0),(0,0,1)\}$	-	$\{(1,1,0),(1,1,1)\}$	-	$\{(0,1,0),(0,1,1)\}$	-	$\{(1,0,0),(1,0,1)\}$
(0,1,0)	-	-	$\{(1,0,1),(1,1,1)\}$	$\{(0,0,1),(0,1,1)\}$	-	-	$\{(1,0,0),(1,1,0)\}$	$\{(0,0,0),(0,1,0)\}$
(0,1,1)	-	$\{(1,0,1),(1,1,0)\}$	$\{(0,0,0),(0,1,1)\}$	-	-	$\{(1,0,0),(1,1,1)\}$	$\{(0,0,1),(0,1,0)\}$	-
(1,0,0)	-	-	$\{(0,1,0),(1,1,0)\}$	$\{(0,0,0),(1,0,0)\}$	$\{(0,1,1),(1,1,1)\}$	$\{(0,0,1),(1,0,1)\}$	-	-
(1,0,1)	-	$\{(0,1,0),(1,1,1)\}$	$\{(0,0,1),(1,0,0)\}$	-	$\{(0,0,0),(1,0,1)\}$	-	-	$\{(0,1,1),(1,1,0)\}$
(1,1,0)	-	-	-	-	$\{(0,1,0),(1,0,0)\}$	$\{(0,0,0),(1,1,0)\}$	$\{(0,1,1),(1,0,1)\}$	$\{(0,0,1),(1,1,1)\}$
(1,1,1)	-	$\{(0,1,1),(1,0,0)\}$	-	$\{(0,1,0),(1,0,1)\}$	$\{(0,0,1),(1,1,0)\}$	-	$\{(0,0,0),(1,1,1)\}$	-

Table 1.3: The Difference Distribution Table of given $\mathcal{F}$

In finite field case, the above $\mathcal{F}$ is equal to $\mathcal{F}(x) = x^5$ on $\mathbb{F}_{2^3}$.

Completeness [83, Definition 2] For any positive integer n, $c_1^{(n)}, c_2^{(n)}, ..., c_n^{(n)} \in \mathbb{F}_2^n$ are defined as:

$$c_1^{(n)} = [0, 0, ..., 1]$$

$$c_2^{(n)} = [0, ..., 1, 0]$$

$$\vdots$$

$$c_n^{(n)} = [1, 0, ..., 0].$$

A function from $\mathcal{F}$: $\mathbb{F}_2^n \to \mathbb{F}_2^m$ is complete if and only if

$$\sum_{x \in \mathbb{F}_2^n} \mathcal{F}(x) \oplus \mathcal{F}(x \oplus c_i^{(n)}) > (0, 0, ..., 0),$$

for all i $(1 \leq i \leq n)$, where both the greater-than and the summation are componentwise over $\mathbb{F}_2^m$.

Avalanche effect [83, Definition 3] A function from $\mathcal{F}$: $\mathbb{F}_2^n \to \mathbb{F}_2^m$ shows the avalanche effect if and only if

$$\sum_{x \in \mathbb{F}_2^n} wt(\mathcal{F}(x) \oplus \mathcal{F}(x \oplus c_i^{(n)})) = m2^{n-1},$$

for all i $(1 \leq i \leq n)$, where $wt()$ denotes the Hamming weight function.

Strict Avalanche Criteria

If a function $\mathcal{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ satisfies the following equations:

$$\sum_{x \in \mathbb{F}_2^n} \mathcal{F}(x) \oplus \mathcal{F}(x \oplus c_i^{(n)}) = (2^{n-1}, 2^{n-1}, ..., 2^{n-1})$$

for all i $(1 \leq i \leq n)$. We say that $\mathcal{F}$ satisfies SAC ([83], Definition 4) or $\mathcal{F}$ is said to be a strong S-box. When a single bit of the input vector is complemented then each output bit should be changed with 50%. Therefore a strong S-box is complete and shows the avalanche effect.

Example 1.5.25. *Suppose $f \in \mathcal{B}_3$ is Boolean function with output $(1, 1, 1, 0, 0, 1, 1, 1)$. Then f satisfies SAC*

Input	Output	$c^{(1)}$	Output	$c^{(2)}$	Output	$c^{(3)}$	Output
(0, 0, 0)	1	(0, 0, 1)	1	(0, 1, 0)	1	(1, 0, 0)	0
(0, 0, 1)	1	(0, 0, 0)	1	(0, 1, 1)	0	(1, 0, 1)	1
(0, 1, 0)	1	(0, 1, 1)	0	(0, 0, 0)	1	(1, 1, 0)	1
(0, 1, 1)	0	(0, 1, 0)	1	(0, 0, 1)	1	(1, 1, 1)	1
(1, 0, 0)	0	(1, 0, 1)	1	(1, 1, 0)	1	(0, 0, 0)	1
(1, 0, 1)	1	(1, 0, 0)	0	(1, 1, 1)	1	(0, 0, 1)	1
(1, 1, 0)	1	(1, 1, 1)	1	(1, 0, 0)	0	(0, 1, 0)	1
(1, 1, 1)	1	(1, 1, 0)	1	(1, 0, 1)	1	(0, 1, 1)	0

Table 1.4: 3 variables Boolean function which satisfies SAC

If all coordinate functions of $\mathcal{F} \in \mathcal{B}_{n,m}$ satisfy the SAC then $\mathcal{F}$ satisfies SAC or $\mathcal{F}$ is said to be a strong S-box.

1.6 Quasigroups as vectorial Boolean functions

For any quasigroup $(Q, *)$ of order $|Q| = 2^d$, we can define a bijective mapping from the set of quasigroup to the set of binary strings of length d. Let α be a bijective mapping and it is defined as:

$$\alpha : Q \to \mathbb{F}_2^d$$
$$q_1 \mapsto (x_1, x_2, ..., x_d).$$

Then

$$*_\alpha : \mathbb{F}_2^d \times \mathbb{F}_2^d \to \mathbb{F}_2^d$$
$$(\alpha(q_1), \alpha(q_2)) \mapsto \alpha(q_1 * q_2).$$

Let $\alpha(q_1 * q_2) = (x_1, x_2, ..., x_d) *_\alpha (x_{d+1}, x_{d+2}, ..., x_{2d}) = (z_1, z_2, ..., z_d)$. Here we see that each z_i is presented as $2d-$ary Boolean function $f_i(x_1, x_2, ..., x_{2d})$, where $f_i : \mathbb{F}_2^d \to \mathbb{F}_2$ is determined by $*$.

Lemma 1.6.1. [54, Lemma 1] *For any quasigroup $(Q, *)$ of order $|Q| = 2^d$, let $\alpha : Q \to \mathbb{F}_2^d$ be any bijective mapping. Then there exist an unique vectorial Boolean function $*_\alpha$ and $2d$-ary Boolean functions $f_1, f_2, ..., f_d$ uniquely determined by d. For all a, b and c in Q, we have:*

$$\begin{aligned} a * b =& c \\ \Downarrow& \\ (x_1, x_2, ..., x_d) *_\alpha (x_{d+1}, x_{d+2}, ..., x_{2d}) =& (f_1(x_1, x_2, ..., x_{2d}), f_2(x_1, x_2, ..., x_{2d}), \ldots, \\ & f_d(x_1, x_2, ..., x_{2d})). \end{aligned}$$

Example 1.6.2. *Let $Q = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ and we use the integer notation $0 \equiv \langle 0, 0\rangle$, $1 \equiv \langle 0, 1\rangle$, $2 \equiv \langle 1, 0\rangle$, $3 \equiv \langle 1, 1\rangle$. The quasigroup $(Q, *)$ given in Example 1.2.6 can be represented by the following vectorial Boolean function:*

$$\mathcal{F}(x_1, x_2, x_3, x_4) = \langle x_1 + x_3 + x_4 + x_2x_4, x_2 + x_4\rangle$$

The binary representation of the following quasigroup is as follows:

$*$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$
$\langle 0,0\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$	$\langle 1,0\rangle$	$\langle 0,1\rangle$
$\langle 0,1\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$	$\langle 1,0\rangle$
$\langle 1,0\rangle$	$\langle 1,0\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$
$\langle 1,1\rangle$	$\langle 1,1\rangle$	$\langle 1,0\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$

1.7 Isotopic quasigroups

Using any quasigroup with algebraic operation and three bijections (isotopism) over the elements of that quasigroup, we can construct other quasigroups which are known as isotopic quasigroups having relatively different algebraic properties. The isotopy in quasigroup is defined as follows,

Definition 1.7.1. *Let $(Q, *)$ and $(K, \star)$ be two quasigroups of the same order. An ordered triple (α, β, γ) of bijections α, β, γ of the set Q onto the set K is called an isotopy or isotopism of $(Q, *)$ upon $(K, \star)$ if $\alpha(x) \star \beta(y) = \gamma(x * y)$ for all $x, y \in Q$. The quasigroups $(Q, *)$ and $(K, \star)$ are then said to be isotopic. If $(Q, *) = (K, \star)$ then (α, β, γ) is called an autotopy or autotopisms of Q.*

When γ is chosen as identity mapping, then

$$x * y = \alpha(x) \star \beta(y),$$

for each $x, y \in Q$. It is called the principal isotopism and denoted by $(Q_{\alpha,\beta}, *)$. For given $(K, \star)$, the set of all permutation is denoted by S_K.
In example 1.2.6 we defined a modular subtraction quasigroup, we take as $(K, \star)$. The isotopic quasigroup $(Q_{\alpha,\beta,\gamma}, *)$ to the $(K, \star)$ is defined as:

$$x * y = \gamma^{-1}((\alpha(x) - \beta(y)) mod\ n).$$

Let $\alpha = [0\ 2\ 1\ 3]; \beta = [0\ 1\ 2\ 3]$ and $\gamma^{-1} = [0\ 1\ 2\ 3]$, then Caley table of isotopic quasigroup is as follows:

$*$	0	1	2	3
0	0	3	2	1
1	2	1	0	3
2	1	0	3	2
3	3	2	1	0

We see that quasigroup $(K, \star)$ with order 4 for which $a(K) = 32$ and isotopic quasigroup $(Q_{\alpha,\beta,\gamma}, *)$ with order 4 for which $a(Q_{\alpha,\beta,\gamma}) = 16$. The associativity index of isotopic quasigroup depends on the combinations of isotopism.

1.8 Complete mapping permutations

Definition 1.8.1. *Suppose Q is an additive group and I is the identity mapping on Q. Then, $\theta : Q \to Q$ is called a complete mapping permutation if both θ and $\theta - I$ are permutations. A group Q is admissible if there is a complete mapping $\theta : Q \to Q$.*

Example 1.8.2. *Let $Q = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ and we use the integer notation $0 \equiv \langle 0, 0\rangle$, $1 \equiv \langle 0, 1\rangle$, $2 \equiv \langle 1, 0\rangle$, $3 \equiv \langle 1, 1\rangle$. Define $\theta : Q \to Q$ by*

$$\theta(\langle x_1, x_2\rangle) = \langle x_2 + 1, x_1 + x_2 + 1\rangle.$$

Then we see that θ and $\theta + I$ both are bijective.

x	θ	$I + \theta$
$\langle 0, 0\rangle$	$\langle 1, 1\rangle$	$\langle 1, 1\rangle$
$\langle 0, 1\rangle$	$\langle 0, 0\rangle$	$\langle 0, 1\rangle$
$\langle 1, 0\rangle$	$\langle 1, 0\rangle$	$\langle 0, 0\rangle$
$\langle 1, 1\rangle$	$\langle 0, 1\rangle$	$\langle 1, 0\rangle$

The following proposition is proved by Sade [143].

Proposition 1.8.3. [143, 14] *Let $(Q, +)$ be an admissible group with complete mapping θ. Then, $* : Q \times Q \to Q$ is defined as:*

$$x * y = \theta(x - y) + y$$

where $x, y \in Q$. Then $(Q, *)$ is a quasigroup.

Example 1.8.4. *The derived quasigroup of order 4 given by complete mapping permutation in Example 1.7.2 is*

$*$	*0*	*1*	*2*	*3*
0	*3*	*1*	*0*	*2*
1	*0*	*2*	*3*	*1*
2	*2*	*0*	*1*	*3*
3	*1*	*3*	*2*	*0*

1.9 Hash function and its security criteria

Hash functions are functions that compress an input of arbitrary length to a result with a fixed length. A cryptographic hash function can provide assurance of data integrity. Let x be a binary string of arbitrary length, then the corresponding hash value or message digest is defined as $y = h(x)$. Suppose that the pair (x, y) can be transmitted over an insecure channel from Alice to Bob. When Bob receives the pair (x, y), he can varify it. If it is satisfied the condition, then he is confident that neither x nor y was changed by an adversary. Therefore the corresponding hash function is secure. Keyed hash functions are also useful and oftenly used as a message authentication code (MAC).

Hash function

A hash family is a four-tuple $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$ where the following conditions are satisfied :

- $\mathcal{X}$ is a set of possible messages.
- $\mathcal{Y}$ is set of finite messages.
- $\mathcal{K}$ is set of finite possible keys, is called keyspace.
- For each $k \in \mathcal{K}$, there is a hash function $h_k \in \mathcal{H}$ such that $h_k : \mathcal{X} \to \mathcal{Y}$.

If $\mathcal{X}$ is a finite set, a hash function is sometimes called a compression function. Let $|\mathcal{X}| = n$, $\mathcal{Y} = m$ and the set of all functions fom $\mathcal{X}$ to $\mathcal{Y}$ be defined as $\mathcal{F}_{\mathcal{X},\mathcal{Y}}$. Obviously, $|\mathcal{F}_{\mathcal{X},\mathcal{Y}}| = m^n$. Any hash family $\mathcal{H} \subseteq \mathcal{F}_{\mathcal{X},\mathcal{Y}}$ is termed an $(n, m)-$hash family.

Security of Hash function

A hash function is said to be secure if these three problems are difficult to solve:

Preimage

Instance : A hash function $h : \mathcal{X} \to \mathcal{Y}$ and an element $y \in \mathcal{Y}$.

Find : $x \in \mathcal{X}$ such that $h(x) = y$.

Second preimage

Instance : A hash function $h : \mathcal{X} \to \mathcal{Y}$ and an element $x \in \mathcal{X}$.

Find : $x' \in \mathcal{X}$ such that $x' \neq x$ and $h(x') = h(x)$.

Collision

Instance : A hash function $h : \mathcal{X} \to \mathcal{Y}$.

Find : $x, x' \in \mathcal{X}$ such that $x' \neq x$ and $h(x') = h(x)$.

To illustrate an example, let hash function $h : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ be defined as

$$h(x, y) = ax + by \ mod(n),$$

$a, b \in \mathbb{Z}_n$ and $n \geq 2$. Suppose that we have

$$h(x_1, y_1) = z_1 \text{ and } h(x_2, y_2) = z_2.$$

Let $r, s \in \mathbb{Z}_n$, then

$$\begin{aligned} h(rx_1 + sx_2 \ mod(n), ry_1 + sy_2 \ mod(n)) =& a(rx_1 + sx_2) + b(ry_1 + sy_2) \ mod(n) \\ =& r(ax_1 + by_1) + s(ax_2 + by_2) \ mod(n) \\ =& rh(x_1, y_1) + sh(x_2, y_2) \ mod(n). \end{aligned}$$

From the given hash values at (x_1, y_1) and (x_2, y_2) we can evaluate its value at various other point without evaluating h at those points. Therefore a hash function $h : \mathcal{X} \to \mathcal{Y}$ is choosen randomly from $\mathcal{F}_{\mathcal{X},\mathcal{Y}}$ and the only assurance for h is oracle acess. Bellare and Rogaway introduced a model for hash functions which is independent from the mathematical formula or algorithm called as random oracle model. The only way to compute a value $h(x)$ is to query the oracle. A true random oracle model does not exist in real life. Whenever a well-defined hash function satisfy the following property which is equivalent to random oracle model.

Theorem 1.9.1. [159, Theorem 4.1] *Suppose that $h \in \mathcal{F}_{\mathcal{X},\mathcal{Y}}$ is choosen randomly, and let $\mathcal{X}_0 \subseteq \mathcal{X}$. Suppose that the values $h(x)$ have been determined (by querying an oracle for h) if and only if $x \in \mathcal{X}_0$. Then $Pr[h(x) = y] = 1/m$ for all $x \in \mathcal{X} \setminus \mathcal{X}_0$ and all $y \in \mathcal{Y}$.*

Example 1.9.2. [159, Example 4.1] *Suppose*

$$\mathcal{X} = \mathcal{Y} = \mathbb{Z}_3$$

and

$$\mathcal{K} = \mathbb{Z}_3 \times \mathbb{Z}_3.$$

For each $K = (a, b) \in \mathcal{K}$ *and each* $x \in \mathcal{X}$*, define*

$$h_{(a,b)}(x) = ax + b \ mod(3)$$

and then define

$$\mathcal{H} = \{h_{(a,b)} : (a, b) \in \mathbb{Z}_3 \times \mathbb{Z}_3\}.$$

The authentication matrix of the hash family $(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{H})$ *is given by*

key	*0*	*1*	*2*
(0,0)	*0*	*0*	*0*
(0,1)	*1*	*1*	*1*
(0,2)	*2*	*2*	*2*
(1,0)	*0*	*1*	*2*
(1,1)	*1*	*2*	*0*
(1,2)	*2*	*0*	*1*
(2,0)	*0*	*2*	*1*
(2,1)	*1*	*0*	*2*
(2,2)	*2*	*1*	*0*

Any value of x *for which adversary queries the tag* y *and for any pair* (x', y') *(where* $x' \neq x$*), adversary determines a value as his forgery. For each choice of* (x', y') *(where* $x' \neq x$*), there is only one key out of three possible keys under which* y' *is the correct authentication tag for* x'*. Then* $Pr[h(x') = y'] = 1/3$.

1.9.1 Hash function in cryptography

The cryptographic hash functions can be used to protect information authenticity and to protect against the threat of repudiation. It is also used in password's identification and encryption algorithm.

Information authentication

Mainly cryptographic hash function reduce the protection of the authenticity of information of arbitrary length to the protection of the authenticity of quantities of fixed length. First, a distinction will be made between protection of authentication with and without secrecy.

The second option is whether the protection of authenticity will depend on the secrecy and authenticity of a key or on the authenticity of an information dependent hashcode. As authentication without secrecy, there is only a plaintext available, which significantly reduces the number of options. If both authentication and secrecy are protected, this can be used in certain cases to simplify the overall system. For an outsider, an attack on the scheme becomes in general harder, as his knowledge decreases. The additional protection offered by the encryption is dependent on the encryption algorithm and on the mode of the encryption algorithm.

Threat of repudiation

The technical term *non-repudiation of origin* denotes a service whereby the recipient is given guarantee of the messages authenticity, in the sense that the recipient can subsequently prove to a third party that the message is authentic even if its originator subsequently revokes it.

1.10 Construction of Hash function using quasigroups

Let $(Q, *)$ be a quasigroup and $Q^\star$ be a set of all finite strings over Q by the elements $m_i \in Q$, $1 \leq i \leq k$. Let $(m_1 m_2 ... m_k)$ be the finite string and the hash function [64] is defined as:

$$H : Q \times Q^\star \to Q$$
$$H(a, m_1 m_2 ... m_k) = a * (m_1 * (m_2 * ... * (m_{k-1} * m_k))),$$

where $a \in Q$ is fixed. We can also write

$$H(a, m_1 m_2 ... m_k) = H_a(m_1, m_2, ..., m_k),$$

for simplicity.

Security criteria

A hash function $h : X \to Y$ is said to be collision resistant if it computationally infeasible to fine $x, x' \in X$ such that $x' \neq x$ and $h(x') = h(x)$. Now, we check if our designed hash function is collision resistant or not. If (m_{k-1}, x, y) satisfies associativity axiom in Q and

$m_k = x * y$ then we choose $(m_1, m_2, m_3, ..., m_{k-1}, m_k)$ and $(m_1, m_2, m_3, ..., m_{k-1} * x, y)$ two arbitrary finite strings over Q so that:

$$\begin{aligned} H_a(m_1, m_2, m_3, ..., m_{k-1}, m_k) &= a * (m_1 * (m_2 * (m_3 * (... * (m_{k-1} * m_k))))) \\ &= a * (m_1 * (m_2 * (m_3 * (... * (m_{k-1} * (x * y)))))) \\ &= a * (m_1 * (m_2 * (m_3 * (... * ((m_{k-1} * x) * y))))) \\ &= H_a(m_1, m_2, m_3, ..., m_{k-1} * x, y), \end{aligned}$$

or

$$H_a(m_1, m_2, m_3, ..., m_{k-1}, m_k) = H_a(m_1, m_2, m_3, ..., m_{k-1} * x, y).$$

Hence the messages $(m_1 m_2 m_3 ... m_{k-1} m_k)$ and $(m_1 m_2 m_3 ... m_{k-1} * xy)$ in Q such that

$$(m_1, m_2, m_3, ..., m_{k-1}, m_k) \neq (m_1, m_2, m_3, ..., m_{k-1} * x, y),$$

but both have the same hash value. Here we see that the problem of collision depends on associative triples in Q. If we have less number of associative triples in Q then our hash function is more secure.

1.11 Literature review

The algebra of quasigroup was extensively studied by Drápal [44–48], Norton [127], Ježek and Kepka [71, 77–82, 126]. To facilitate our discussion we set $a(n)$=min$\{a(Q)\}$, where the minimum is taken over all quasigroups Q of order n. Let Q be a finite non-associative quasigroup of order n isotopic to a group. Then Drápel and Kepka [46] proved that

$$\begin{aligned} a(Q) &\leq n^3 - 4n^2 + 6n, \ \textit{provided } n \geq 3, \\ a(Q) &\leq n^3 - 4n^2 + 8n, \ \textit{provided } n \textit{ is even}. \end{aligned}$$

To our knowledge, the only infinite class of quasigroups Q with $a(Q) < n^2$ was provided in [87].

Proposition 1.11.1. [87, Proposition 8] *For every even integer $n \leq 6$, $n \equiv 0, 2$ (mod 6) there exist a non-commutative idempotent quasigroup Q with $a(Q) < n^2$.*

Kotzig and Reischer [87] also proved that for each $n \equiv 0, 2$ (*mod* 6) there exist a quasigroup with $a(Q) = n^2 - 3n + 3$. Then Grošek and Horák [64] showed that lim inf $a(n)$ is at most $n^{1.5131}$ which is significantly lower.

As to upper bounds on $a(n)$, the best bound so far states that $a(n) \leq 2n^2$. The following corollary is proven by Kotzig and Reischer [87].

Corollary 1.11.2. [87, Corollary] *For a commutative quasigroup we have $a(Q) \geq n^2$. This lower bound is sharp for every $n \not\equiv 2$ (mod 4). For $n \equiv 2$ (mod 4) there is a commutative quasigroup with associativity index $a(Q) = 2n^2$.*

Further some useful results on quasigroups are given below.

Proposition 1.11.3. [87, Proposition 7] *For every n odd there exist a commutative idempotent quasigroup Q with $a(Q) = n^2$.*

Proposition 1.11.4. [87, Proposition 10] *For every $n < 7$ every anticommutative idempotent quasigroup Q has associative index $a(Q) = n^2$.*

For every $n \geq 1$ the set of the numbers $a(Q)$ denote by $assspec(n)$, where Q runs over the quasigroups of order n. This set, called the associativity spectrum of n, is contained in $\{n, n+1, ..., n^3\}$. Ježek and Kepka [71] defined the associativity spectrum:

$$
\begin{aligned}
&assspec(1) = \{1\}\\
&assspec(2) = \{8\}\\
&assspec(3) = \{9, 27\}\\
&assspec(4) = \{16, 24, 32, 64\}\\
&assspec(5) = \{15, ..., 57, 59, 62, 63, 74, 79, 80, 89, 125\}\\
&assspec(6) = \{16, 19, ..., 114, 116, 117, 118, 120, 121, 122, 124, ..., 128, 130, ...\\
&\qquad ..., 137, 141, 142, 144, 148, 152, 160, 162, 168, 172, 184, 189, 216\},
\end{aligned}
$$

and also illustrated inequity for $a(n)$:

$$n \leq a(n) \leq n^2 \ for \ n \geq 3, n \neq 4k + 2,$$

$$n \leq a(n) \leq 2n^2 \text{ for every } n \geq 3.$$

If Q is a quasigroup of order $n \geq 3$ such that $a(Q) = n$, then Q is idempotent and not isotopic to a group [77]. An element $a \in Q$ with the property $a * a = a$ is called an idempotent. Denote by $I(Q)$ the set of all idempotent elements of Q and set $i(Q) = |I(Q)|$. Grošek and Horák [64] provided new lower bound:

Theorem 1.11.5. [64, Theorem 1.1] *Let Q be a quasigroup of order n. Then $a(Q) \geq 2n - i(Q)$.*

Therefore if there were a quasigroup Q of order n with $a(Q) = n$, then Q would have to be an idempotent quasigroup. Based on a supporting evidence, which includes extensive computational experiments, we strongly believe that the following conjecture is true:

Conjecture: [64, Conjecture 1.2] For all $n \in \mathbb{N}$, it holds $a(n) \geq n + 1$.

In spite of an intensive effort we were not able to prove the conjecture for any significant subclass of idempotent quasigroups although our computation results indicate that a quasigroup Q of order n with $a(Q) = a(n)$ is not an idempotent quasigroup. Up to now there has been described no infinite series of quasigroups Q for which the value of $a(Q)$ would be linear in $n = |Q|$.

There are several examples of quasigroups of order n with n^2 associative triples. More concretely, for each $n \neq 10 (mod\ 12)$, there is a quasigroup Q of order n with $a(Q) \leq n^2$.

The best asymptotic construction presented in [64], which is obtained by taking products of a quasigroup Q of order 5, 6 and 7 with the least possible number of associative triples, which are claimed to be 15, 19 and 19 respectively. This gives

$$a(Q) = \begin{cases} |Q|^{1.6826} & \text{when } |Q| = 5^m,\ m \in \mathbb{N}, \\ |Q|^{1.5474} & \text{when } |Q| = 6^m,\ m \in \mathbb{N}, \\ |Q|^{1.5131} & \text{when } |Q| = 7^m,\ m \in \mathbb{N}. \end{cases}$$

Later Valent [163] updated the above results for quasigroup Q of order 5, 6, 7 and 8 with the least possible number of associative triples, which are claimed to be 15, 16, 17 and 21

respectively as follows:

$$a(Q) = \begin{cases} |Q|^{1.6826} & \text{when } |Q| = 5^m,\ m \in \mathbb{N}, \\ |Q|^{1.5474} & \text{when } |Q| = 6^m,\ m \in \mathbb{N}, \\ |Q|^{1.4559} & \text{when } |Q| = 7^m,\ m \in \mathbb{N}, \\ |Q|^{1.4641} & \text{when } |Q| = 8^m,\ m \in \mathbb{N}. \end{cases}$$

As far we know, the only lim inf $a(Q)$ is at most $|Q|^{1.4641}$ when $|Q| = 8^m$, $m \in \mathbb{N}$.

The associativity index of isotopic quasigroups is studied by Drápel and Valent [48]. Valent [163] has shown that the average number of associative triples in the set of all isotopisms of any quasigroup $(K, \star)$ of order n is given by:

$$\frac{\sum_{\alpha,\beta,\gamma \in S_K} a(Q_{\alpha,\beta,\gamma})}{(n!)^3} = \frac{n^3}{(n-1)} = n^2 \cdot \left(1 + \frac{1}{n-1}\right).$$

Valent [163] also described that this average number is independent of using operation $\star$ of quasigroup. We see that this average number is always constant for many quasigroups with different operation but having same order. For $n \geq 2$, it can be regarded as a new upper bound on $a(n)$.

Now we are discussing some results on balanced Boolean functions. The quadruplet entry (n, d, nl, ac) indicates that a Boolean function on n variables with algebraic degree d, nonlinearity nl and autocorrelation ac. We plan to evolve the best profile (n, d, nl, ac) using simulated annealing. Clark et al. [31] have best achieved profiles $(8, 7, 116, 24)$ and $(8, 5, 112, 16)$. Later Kavut and Yücel [73] have best achieved profiles $(8, 7, 116, 24)$ and $(8, 5, 114, 16)$ using simulated annealing. Comparing the nonlinearity of 8 variables balanced Boolean functions:

	Nonlinearity		Autocorrelation
Lowest Upper Bound	118	Zhang and Zheng [170]	24
Best known Example ([135], [68])	116	Maitra Construction [98]	24
Dobertin's Conjecture [42]	116	Maitra Conjecture [98]	24
Bent Concatenation	112		
Random	112		
Random Plus Hill-Climb	114		
Genetic Algorithms ([122])	116		

Table 1.5: Nonlinearity table of 8 variables balanced Boolean functions

1.12 Overview of the thesis

A chapter wise brief description of this thesis is given below:

Chapter 1. It is the introductory chapter of the thesis, containing mathematical notations and definitions with examples. A brief literature review is also given to illuminate the idea presented in the thesis. The necessary concepts of quasigroups in cryptography and its formations by complete mapping permutations are highlighted. Some cryptographic characteristics, i.e., nonlinearity, differential uniformity and Strict Avalanche Criteria (SAC), which are required to analyze existing and implemented quasigroups are stated here. We provide some basics on finite fields which is useful to our work.

Chapter 2. In this chapter, we describe two heuristic techniques, i.e., simulated annealing and Genetic algorithm, for the purpose of evolving balanced Boolean functions and quasigroups with low associative index respectively. We have best achieved profile $(8, 7, 114, 32)$ for 8 variables balanced Boolean function by simulated annealing. For evolving quasigroups, we propose a new cost function which is inspired by Valent's result [163]. By using our Genetic technique and proposed cost function we find the quasigroups whose associative indeces are relatively less than the square of their order.

Chapter 3. Markovski and Mileva [104] have shown that the quasigroup defined by Feistel function is highly non-associative, since Feistel function works as complete mapping permutation when using function is bijective. They believe that any bijection can hardly statisfies the governing equations of associativity. We solve these equations by using linear permutations, quadratic permutations, APN (almost perfect nonlinear functions) permutations, differentially 4-uniform permutations and differentially δ-uniform permutations over $\mathbb{F}_2^n$. We prove that the number of associative triples for any such quasigroups Q is equal to the square of $|Q|$, where Q is the order of quasigroup, except the quadratic permutations. For quadratic permutations, we prove the lower bound for any such quasigroups Q is equal to $2|Q|^2$. We further identify the relation between the cryptographic characteristics, i.e., nonlinearity, differential uniformity and Strict Avalanche Criteria (SAC), of bijective mapping and Feistel network based quasigroup.

Chapter 4. The main focus of this chapter is to construct the quasigroups using permutations over finite fields. Kotzig and Reischer [87] proposed the construction of quasigroups by finite commutative, but not necessarily associative or unitary, rings. We implement

this construction by using two different permutations over finite fields. We further obtain the equations satisfy by associativity condition. We solve these equations by using linear permutations, affine permutations, quadratic permutations and linear complete mapping permutations over $\mathbb{F}_{2^n}$. For some permutations we prove that lower bound of associative index is equal to $2|Q|^2$ and for some permutations we get associative index exactly $|Q|^2$.

Chapter 5. The purpose of this chapter is to construct the complete mapping permutations. Construction of complete mapping permutations by using Feistel structure has been proposed by Markovski and Mileva [104] which they used to construct large quasigroups. The theory of XS-circuits as proposed by Agievich [2] is described in this chapter. First we construct complete mapping permutations from functions over finite fields by using XS-circuits and give the counts for particular order. We enumerate for the order $2, 3, 4$ and 5. Winterhof [167] described the concept of $\mathcal{K}$-complete mapping permutation which can be used to define uniformly distributed sequences. Uniform distribution is a desirable feature of a sequence for both Monte Carlo-methods and cryptography. Therefore we further construct $\mathcal{K}$-complete mapping permutations by using XS-circuits. Later we extend the XS-circuits, we see its peculiar behave. By using extended model we find a recursive constrictions that extend a complete mapping of dimension r to a complete mapping of dimension n, where $r \leq n$. We also enumerate the total counts of complete mapping permutations for $r = 2$ and $n = 4$.

Chapter 6. This chapter concludes the thesis and presents some open problems for future work.

Chapter 2

Quasigroups as vectorial Boolean functions and their heuristics techniques of evolving

2.1 Introduction

The security of any stream cipher depends upon the cryptographic properties of Boolean function. The Boolean function used as a nonlinear filter function and combiner function for generating the key stream sequence for stream cipher with strong cryptographic properties. Since the total search space for any n variables Boolean function is 2^{2^n}, the problem of finding cryptographically strong Boolean function is considered as an NP hard problem. There are three different ways to construct a Boolean function such as algebraic construction, random generation and heuristic optimization. There are lot of research had already done using algebraic techniques and heuristic technique to construct a cryptographically strong Boolean function. But, heuristic technique is not able to find the result that is achieved by the algebraic construction. So there are lot of scope to improve the heuristic technique to make it more efficient in terms of both performance and results. We apply simulated annealing to construct 8 variable Boolean function with high nonlinearity and low autocorrelation.

In 1983 Kirkpatrick et al. [84] suggested a new heuristic search technique simulated annealing motivated by the cooling processes of molten metals. He implemented the ap-

propriate Metropolis algorithm into simulated annealing of a combinatorial optimization problem. In optimization problem, an objective function is either a minimizing function (cost function) or maximizing function (fitness function). Clark and Jacob [29] showed that the power of optimization methods for the synthesizing of Boolean functions is affected by choice of cost function. In particular, they showed simulated annealing conjugate with a new cost function motivated by Parseval's identity. Those Boolean functions showing strong cryptographic characteristics to be included in the design of secure cryptosystems with essential cryptographic primitive. Clark et al. [31] have been identified many desirable properties for Boolean functions with cryptographic purpose and obtained compromising exchange among such properties. First we use simulated annealing based on [84]. We demonstrate how to evolve an optimizing Boolean function with best profile. We shall also show how the capabilities of different cost functions invariant and nonlinearity Boolean functions can be enhanced by random shifting (permutations) their positions in truth table. In Section 2.3, we describe the important definition to understand the cost function and than how to use simulated annealing algorithm for evolution of optimizing Boolean functions.

In Section 2.2, we extend our Boolean function construction into quasigroup to be treated as an vectorial or multi-output Boolean function. Quasigroup is an algebraic structure which is used for the designing of secure hash function. In introductory chapter [Section 1.10, Chapter 1] we already discussed importance of associative triple of quasigroups when it is used as construction of hash functions. Then we focus on to evolve quasigroups with relatively minimum number of associative triples. Grošek and Horák [64] state that best known upper bound for the number of associative triples of any quasigroup Q is less than or equal to $2|Q|^2$, where $|Q|$ is the cardinality of the set Q. Up to till now the only infinite class of quasigroups Q with associative triples less than $|Q|^2$ was provided by Kotzig and Reischer [87]. Therefore, our concern is to evaluate the counts of associative triples less than the previous known. The avarage number of associative triples in the set of all isotopisms of quasigroup is proved by Valent [163]. This number depends solely upon $|Q|$ rather than the isotopisms. By Genetic algorithm, Snášel et al. [154] also evolved isotopic quasigroups where used fittness function was not completely motivated by associative triples of isotopic quasigroups. They considered only those triples as associative triples from all distinct combinations of three elements out of $|Q|$ whose satisfy the associativie axiom under same

operation. But any quasigroup not only has those triples as associative triples it has more. In Section 2.4, we propose a new cost function for evolving the isotopic quasigroups which is motivated by Valent's result [221, Lemma 3.6] and than how to use Genetic algorithm for evolution of isotopic quasigroups with low number of associative triples, usally we get associativity index less than the square of quasigroups's order.

2.2 Preliminaries

Isotopy in Quasigroups

Using any quasigroup with algebraic operation and three bijections (isotopism) over the elements of that quasigroup, we can construct other quasigroups which are known as isotopic quasigroups having relatively different algebraic properties. The isotopy in quasigroup is defined as follows,

Definition 2.2.1. *Let $(Q, *)$ and $(K, \star)$ be two quasigroups of the same order. An ordered triple (α, β, γ) of bijections α, β, γ from Q onto K is called an isotopy or isotopism of $(Q, *)$ upon $(K, \star)$ if $\alpha(x) \star \beta(y) = \gamma(x * y)$ for all $x, y \in Q$. The quasigroups $(Q, *)$ and $(K, \star)$ are then said to be isotopic. If $(Q, *) = (K, \star)$ then (α, β, γ) is called an autotopy or autotopisms of Q.*

When γ is chosen as identity mapping, then

$$x * y = \alpha(x) \star \beta(y)$$

for each $x, y \in Q$. It is called the principal isotopism and denoted by $(Q_{\alpha,\beta}, *)$. For given $(K, \star)$, the set of all permutation is denoted by S_K.

Let $(K, \star)$ be a quasigroup with finite order n, i.e., $|K| = n$. The operation $\star : K \times K \to K$ is defined as:

$$x \star y = (x - y) mod\ n.$$

Then $(K, \star)$ is a quasigroup.

Suppose that $K = \{0, 1, 2, 3, 4, 5, 6, 7\}$, i.e., $|K| = 8$, then the Caley table of $(K, \star)$ is given by

$\star$	0	1	2	3	4	5	6	7
0	0	7	6	5	4	3	2	1
1	1	0	7	6	5	4	3	2
2	2	1	0	7	6	5	4	3
3	3	2	1	0	7	6	5	4
4	4	3	2	1	0	7	6	5
5	5	4	3	2	1	0	7	6
6	6	5	4	3	2	1	0	7
7	7	6	5	4	3	2	1	0

Associative axiom:

$$(x \star y) \star z = x \star (y \star z),$$
$$i.e., \quad ((x-y) mod\ n) \star z = x \star ((y-z) mod\ n),$$
$$i.e., \quad 2 \cdot z = (0) mod\ n.$$

The above congruence has exactly e solutions, where $e = gcd(2, n)$. If x and y may be chosen from K, then the associative triples of $(K, \star)$ is given by

$$a(Q) = \begin{cases} n^2 & \text{when } n \text{ odd,} \\ 2n^2 & \text{when } n \text{ even.} \end{cases}$$

The isotopic quasigroup $(Q_{\alpha,\beta,\gamma}, *)$ to the $(K, \star)$ is defined as:

$$x * y = \gamma^{-1}((\alpha(x) - \beta(y)) mod\ n).$$

Let $\alpha = [0\ 1\ 4\ 5\ 2\ 3\ 6\ 7]$; $\beta = [0\ 2\ 4\ 6\ 1\ 3\ 5\ 7]$ and $\gamma^{-1} = [0\ 2\ 1\ 3\ 4\ 6\ 5\ 7]$, then Caley table of isotopic quasigroup is as follows:

$*$	0	1	2	3	4	5	6	7
0	0	5	4	1	7	6	3	2
1	2	7	6	3	0	5	4	1
2	4	1	0	5	3	2	7	6
3	6	3	2	7	4	1	0	5
4	1	0	5	4	2	7	6	3
5	3	2	7	6	1	0	5	4
6	5	4	1	0	6	3	2	7
7	7	6	3	2	5	4	1	0

Associative axiom:

$$(x * y) * z = x * (y * z),$$

$$i.e., \gamma^{-1}((\alpha(x) - \beta(y)) mod\ n) * z = x * \gamma^{-1}((\alpha(y) - \beta(z)) mod\ n),$$

$$i.e., (\alpha(\gamma^{-1}((\alpha(x) - \beta(y)) mod\ n)) - \beta(z)) mod\ n = (\alpha(x) - \beta(\gamma^{-1}((\alpha(y) - \beta(z)) mod\ n))) \ mod\ n.$$

The solution of the above congruence depends upon α, β and γ in S_K. It varies according to the different combinations of α, β and γ in S_K. As for above example, $a(Q_{\alpha,\beta,\gamma}) = 64$. Therefore we can obtain many isotopic quasigroups $(Q_{\alpha,\beta,\gamma}, *)$ from the modular subtraction quasigroup $(K, \star)$ by choosing permutations α, β and γ in S_K with different combination. Interesting fact is that we do not need Cayley table for evaluting the associative triples.

Binary representations of Quasigroup elements

We know that there are $n!$ (factorial of a non-negative integer n) different permutation for n elements. The total search space for isotopisms (α, β, γ) is equal to $n! \cdot n! \cdot n!$. When $n > 2^5, 2^6, \ldots$, it is difficult to handle. That's why we convert all elements of the quasigroups into bit strings. When $|K| = 2^m$, we need only m bit to represent all elements of the quasigroups. The binary representation of $K = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is as follows:

Q	3 bit
0 →	000
1 →	001
2 →	010
3 →	011
4 →	100
5 →	101
6 →	110
7 →	111

The bit permutation [154] is an efficient way of implementing permutations over K. Although only few $log_2(n)! \cdot log_2(n)! \cdot log_2(n)!$ isotopisms are constructed but a chance to meet the criteria of less associativity.

Example 2.2.2. *Let $|Q| = 2^3$, then we need 3 bit to represent all elements of the quasigroups. All permutations of the bit are as follows:*

$$(1\ 2\ 3), (1\ 3\ 2), (2\ 3\ 1), (2\ 1\ 3), (3\ 2\ 1), (3\ 1\ 2).$$

The corresponding elements of the quasigroups are permuted as follows:

123	132	231	213	321	312
000	000	000	000	000	000
001	010	010	001	100	100
010	001	100	100	010	001
011	011	110	101	110	101
100	100	001	010	001	010
101	110	011	011	101	110
110	101	101	110	011	011
111	111	111	111	111	111

Table 2.1: All combinations of output for 3 bit.

Bit Permutation as Permutations over $\mathbb{F}_2^m$

We get the algebraic normal form for the combination (1 3 2) which is denoted by $f_{(1\ 2\ 3)}(x_1, x_2, x_3)$

$$f_{(1\ 2\ 3)}(x_1, x_2, x_3) = (x_1, x_2, x_3).$$

Similarly we get

$$f_{(1\ 3\ 2)}(x_1, x_2, x_3) = (x_1, x_3, x_2),$$

$$f_{(2\ 3\ 1)}(x_1, x_2, x_3) = (x_2, x_3, x_1),$$

$$f_{(2\ 1\ 3)}(x_1, x_2, x_3) = (x_2, x_1, x_3),$$

$$f_{(3\ 2\ 1)}(x_1, x_2, x_3) = (x_3, x_2, x_1),$$

$$f_{(3\ 1\ 2)}(x_1, x_2, x_3) = (x_3, x_1, x_2).$$

Therefore we can also use algebraic normal form (ANF) instead of bit strings representation. It is known that $\mathbb{F}_2^m$ and $\mathbb{F}_{2^m}$ (i.e., finite fields) both are isomorphic under vector isomorphism over $\mathbb{F}_2$.

Theorem 2.2.3. [96, Theorem 7.8]

(*i*) *Every linear polynomial over* $\mathbb{F}_{2^m}$ *is a permutation polynomial of* $\mathbb{F}_{2^m}$.

(*ii*) *The monomial* x^r *is a permutation polynomial of* $\mathbb{F}_{2^m}$ *if and only if* $gcd(r, 2^m - 1) = 1$.

Example 2.2.4. *Let* $f(x) = x^2$ *over* $\mathbb{F}_{2^3}$ *and* s *be a primitive element in* $\mathbb{F}_{2^3}$. *Then we have*

$$\mathbb{F}_{2^3} = \{0, 1, s, s^2, s^3, s^4, s^5, s^6\}.$$

Using the irreducible polynomial $s^3 + s + 1 = 0$, *which can also be represented as*

$$\mathbb{F}_{2^3} = \{0, 1, s, s^2, s + 1, s^2 + s, s^2 + s + 1, s^2 + 1\}.$$

Then $f(x) = x^2$ *over* $\mathbb{F}_{2^3}$ *are permuted as follows:*

x		$f(x) = x^2$
0	$\rightarrow$	*0*
1	$\rightarrow$	*1*
s	$\rightarrow$	s^2
s^2	$\rightarrow$	$s^2 + s$
$s + 1$	$\rightarrow$	$s^2 + 1$
$s^2 + s$	$\rightarrow$	s
$s^2 + s + 1$	$\rightarrow$	$s + 1$
$s^2 + 1$	$\rightarrow$	$s^2 + s + 1$

Then binary representation of $f(x) = x^2$ over $\mathbb{F}_2^3$ is as follows:

$x = (x_1, x_2, x_3)$	$f(x)$
(0,0,0) $\rightarrow$	(0,0,0)
(0,0,1) $\rightarrow$	(0,0,1)
(0,1,0) $\rightarrow$	(1,0,0)
(0,1,1) $\rightarrow$	(1,0,1)
(1,0,0) $\rightarrow$	(1,1,0)
(1,0,1) $\rightarrow$	(1,1,1)
(1,1,0) $\rightarrow$	(0,1,0)
(1,1,1) $\rightarrow$	(0,1,1)

Table 2.2: Bit representation of $f(x) = x^2$ over $\mathbb{F}_2^3$.

By Equation (1.5.1) the algebraic normal form of $f(x) = x^2$ over $\mathbb{F}_2^3$ is written as

$$f(x_1, x_2, x_3) = (x_1 + x_2, x_1, x_3).$$

Similarly we have x^3, x^4, x^5 and x^6 monomials over $\mathbb{F}_2^3$. In Table 3, we showed the binary representation of all possible monomials over $\mathbb{F}_2^3$.

$f(x) = x$	$f(x) = x^2$	$f(x) = x^3$	$f(x) = x^4$	$f(x) = x^5$	$f(x) = x^6$
000	000	000	000	000	000
001	001	001	001	001	001
010	100	011	110	111	101
011	101	100	111	010	110
100	110	101	010	011	111
101	111	110	011	100	010
110	010	111	100	101	011
111	011	010	101	110	100

Table 2.3: Bit representation of all possible monomials over $\mathbb{F}_2^3$.

Now we have total $(3!+5)\cdot(3!+5)\cdot(3!+5)$ isotopisms for $|Q| = 8$ by Table 1 and 3. Berger et al. [11] and Mandi [100] defined the special class of permutations (quadratic permutations, APN permutation, e.t.c.) over $\mathbb{F}_2^m$ (or, equivalently $\mathbb{F}_{2^m}$). To enhance the search space for isotopisms we use such type of permutations, we refer to [92, 108, 124, 140, 149].

2.3 Heuristic optimization of Boolean function

It is a class of artificial intelligence which is defined by concerned algorithms. These algorithms are called evolutionary algorithms based on Darwinian principle. The characteristics

of these algorithms are varied and repeated attempts until the success or stops trying. Thats why it can be considered as a global optimization method with heuristic search. Evolutionary computation used iterative process because of growth and development of population. During the process we select a random search for achieving the targeted result. Essentially, this computation is inspired by biological mechanism of evolution. Some evolutionary methods are very useful for solving cryptographic problems with the help of heuristic techniques like as hill climbing, simulated annealing and Genetic algorithm.

Cost function

We want to improve nonlinearity of Boolean function. It is known that its depend on the $WH_{max}(f)$ by Equation (1.5.2). Hence our optimizing parameter is defined as

$$Opt_{para}(\hat{f}) = WH_{max}(f).$$

Essentially, we seek to minimize this $Opt_{para}(\hat{f})$ say cost value. By simulated annealing, we consider the effect of a move only on those values of $W_f(w)$ where the values are maximum or near to maximum for the current solution. There is an indirect approach for that given by Parseval's identity (1.5.4)

$$\sum_{w\in\mathbb{F}_2^n} |W_f(w)|^2 = 2^{2n}.$$

It can be shown that $|W_f(w)| \geq 2^{n/2}$ and $WH_{max}(f) = \max_{w\in\mathbb{F}_2^n} |W_f(w)|$ to be at least $2^{n/2}$. When $|W_f(w)| \doteq 2^{n/2}$ for each w would get the upper bound but in practice it may be impossible. Bent Boolean functions achieve this bound and only exist for even value of n. If some $|W_f(w)|$ values are greater than upper bound then some other $|W_f(w)|$ values must be less than it because of Parseval's identity. When we seek to minimize the spectrum of absolute values of $|W_f(w)|$, we would seem to be a possible means of achieving high nonlinearity. Thus a suggested cost function is defined as

$$\sum_{w\in\mathbb{F}_2^n} ||W_f(w)| - 2^{n/2}|. \tag{2.3.1}$$

This suggested cost function is required for attacking nonlinearity. In the above cost func-

tion, there is a chance to achieve $|W_f(0)| = 2^{n/2}$. It is known that balanced Boolean functions have $W_f(0) = 0$ and bent Boolean functions are not balanced. Clark et al. [31] modified this cost function for evolving highly nonlinear balanced Boolean functions. Therefore the plausible Equation (2.3.1) consider as cost function for Nonlinearity Targeted (NLT):

$$cost(\hat{f}) = \sum_{w \in \mathbb{F}_2^n} ||W_f(w)| - X|^R. \tag{2.3.2}$$

Here X and R are two parameter which is provide accessibility to experiment. It is too much tough to say which values of X and R for imposing a balance requirement and how much effected with odd n. The Autocorrelation Targeted (ACT) technique was adopted only after it was noticed that the NLT approach generated Boolean functions with high autocorrelation.

Related to Autocorrelation function

The autocorrelation function $\mathcal{C}_f(w)$ is defined as

$$\mathcal{C}_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+w)}$$

We shall write $\mathcal{C}_f(w)$ if there is no danger of confusion. Note that $\mathcal{C}_f(0)$ equals 2^n. Then cost functions for ACT is given by

$$cost(\hat{f}) = \sum_{w \in \mathbb{F}_2^n} ||\mathcal{C}_f(w)| - X|^R. \tag{2.3.3}$$

Heuristic search

If classical methods are too slow for finding an approximate result or any exact solution then we use heuristic search algorithms for the problems. It is more quick rather than any other techniques for solving a problem and provide a best result. The characteristics of the techniques are trading optimality, accuracy and legitimacy of speed. The fundamental axioms of heuristic techniques as follows:

- gives the authentication for a good solution in required time,
- the efficiency always increases because of avoiding completeness,
- this technique is useful for such type of problems when problems,

- could not be solved by any classical methods,
- computationally hard,

Now, we are demonstrating one kind of heuristic search algorithm called as simulated annealing.

2.3.1 Simulated annealing for evolving Boolean functions

This search techniques is implementation of hill climbing [120] techniques. In hill climbing, we accept only best moves and avoid the worst moves but in simulated annealing techniques we accept worst moves also with some probability which is randomly generated between 0 to 1. Essentially, simulated annealing merges with hill climbing through probabilistic acceptance of worst moves. Now, we are get rid of plateau and ridge conditions effect and exploring the whole space which is less sensitive from the initial point. We seek to minimization rather than creating maxima and use objective function rather than heuristic.
The simplest way to implement simulated annealing is as follows:

- Evaluate the truth table of Boolean function $[f(0,\ldots,0,0), f(0,\ldots,0,1), f(0,\ldots,1,0),\ldots, f(1,\ldots,1,1)]$ of given length n as current state.
- If $|W_f(w)| \doteq 2^{n/2}$ for each w would get the upper bound then quit otherwise make the current state this initial state and proceed.
- Generate all 2-neighborhood strings from the current state
- Choose one string among them randomly say neighborhood state
- If this neighborhood state is attained the upper bound then quit
- Set stopping criteria according to result perfection
- Repeat
  - δ, Evaluate difference between the cost value of current state and neighborhood states $(N(S))$
  - Now, check the conditions
  - If $\delta < 0$ than this state makes the current new state which is better function comparatively previous current state
  - If it is not better then make it better with probability p, where $p = exp(-\delta/T)$. Now, we generate a random number U between 0 to 1 and comparing it with p. If U is greater than p do nothing and if it is less then p accept this state as the next current state.

∘ Revise T with multiply by $\alpha \in (0, 1)$, because during annealing schedule is dependent on a number of moves (Moves in Inner Loop, MIL) to the new states.

Until a solution is found or no more new states.

• Return with the best answer.

Algorithm 1: Simulated annealing algorithm:

```
1  S = S_0
   T = T_0
   while do
2      for int i = 0; i < MIL; i++ do
3          Select Y ∈ N(S)
           δ = f(Y) − f(S)
           if δ < 0 then
4              S = Y
               else
5              Generate U = U(0, 1)
               if U = exp(−δ/T) then
6                  S = Y
               end
7          end
8      end
9      end
10     end
11     T = T × α
       Until stopping criteria is met;
12 end
```

2.3.2 Experimental details

We evolved Boolean function for 8 variables using cost function by Equation (2.3.2) for $R = 3$ and $X = 3$ in Matlab. The value R is positive mostly $R = 3$ and range of X from -16 to 30 used [31]. The cubic power puts the more impact on any large deviation of a term rather than the small deviation. That means cubic term has more chance of being

minimized or maximized comparatively the other powers.

n	d	nl	ac
8	7	116	16

Now we take the value of $R = 4$ and $X = 0$. Then we show that with two different parameters we got the same optimizing Boolean function with same characteristics. This result also unique for us.

n	d	nl	ac
8	7	116	16

After getting this optimizing Boolean function, we have to check its balancedness. Using "Sage" we have found the positions of 0s and 1s of the given function and count also. After replacing either 0s or 1s which are more and make the given optimum function balanced with high nonlinearity among the all. We have to find the other characteristics also. These are the characteristics of the evolved balanced Boolean function:

n	d	nl	ac
8	7	112	40

Now we generate the random permutation ($randperm()$ in Matlab) of a number which is equal to the length of the truth table. Basically, this is a vector of the random permutations of a number say r. If we choose first two element of r than change the corresponding indices of the truth table of evolved balanced Boolean function and check the nonlinearity. If our result not improved than take next two (omit the first element) of r and so on. This process follow up to when we will not get improved result. Thus we find the better result rather than the previous one.

These are the updated characteristics of the evolved balanced Boolean function:

n	d	Previous nl	New nl	ac
8	7	112	114	32

2.4 Heuristic optimization of quasigroups

Proposed Cost Function

Valent [163] has shown that the average number of associative triples in the set of all

isotopisms of any quasigroup $(K, \star)$ of order n is given by:

$$\frac{\sum_{\alpha,\beta,\gamma \in S_K} a(Q_{\alpha,\beta,\gamma})}{(n!)^3} = \frac{n^3}{(n-1)} = n^2 \cdot \left(1 + \frac{1}{n-1}\right).$$

Valent [163] also described that this avarage number is independent of using operation $\star$ of quasigroup. We see that this average number is always constant for many quasigroups with different operation but having same order. It is possible that for some α, β and γ in S_K, the value of $a(Q_{\alpha,\beta,\gamma})$ is given by

$$a(Q_{\alpha,\beta,\gamma}) \geq n^2 \cdot \left(1 + \frac{1}{n-1}\right),$$

and for some α, β and γ in S_K, the value of $a(Q_{\alpha,\beta,\gamma})$ is given by

$$a(Q_{\alpha,\beta,\gamma}) \leq n^2 \cdot \left(1 + \frac{1}{n-1}\right). \tag{2.4.1}$$

Here we focus on finding the quasigroups with low associative triples. Therefore the above inequality [Equation (2.4.1)] can be regarded as an upper bound on $a(Q_{\alpha,\beta,\gamma})$, when $n \geq 2$. For any quasigroup $(Q, *)$ we get the new upper bound for associative triples

$$a(Q) \leq n^2 \cdot \left(1 + \frac{1}{n-1}\right).$$

So we find the best combination of α, β and γ in S_K which provide the least value of $a(Q_{\alpha,\beta,\gamma})$. According to the cost function, the following form of Equation (2.4.1) is used:

$$cost(Q) = \min_{\alpha,\beta,\gamma \in S_K} \left(a(Q_{\alpha,\beta,\gamma}) - n^2 \cdot \left(1 + \frac{1}{n-1}\right)\right).$$

Take $\lambda = (1 + \frac{1}{n-1})$ and 2 assign as a variable k, then modified form is as follows:

$$cost(Q) = \min_{\alpha,\beta,\gamma \in S_K} (a(Q_{\alpha,\beta,\gamma}) - \lambda \cdot n^k),$$

$$\text{or,} \quad cost(Q) = \min_{\alpha,\beta,\gamma \in S_K} |a(Q_{\alpha,\beta,\gamma}) - \lambda \cdot n^k|.$$

To analyse the values of λ and k for achieving the minimum cost value, i.e., $cost(Q) = 0$ as follows:

- When $\lambda = 1$ and $k = 1$, we get

$$a(Q) = n,$$

which is annihilated the given conjecture [93, Conjecture 1.2], i.e., $a(Q) \geq n + 1$. Up to now there has not been described any quasigroup with $a(Q) = |Q|$.

- When $\lambda = 1$, we get the different combinations of k

$$a(Q) = \begin{cases} n^{1.6826} & \text{when } n = 5^m,\ m \in \mathbb{N}, \\ n^{1.5474} & \text{when } n = 6^m,\ m \in \mathbb{N}, \\ n^{1.4559} & \text{when } n = 7^m,\ m \in \mathbb{N}, \\ n^{1.4641} & \text{when } n = 8^m,\ m \in \mathbb{N}. \end{cases}$$

which are shown by Valent [163].

- When $\lambda = 1$, we get the different combinations of k

$$a(Q) = \begin{cases} n^{1.6826} & \text{when } n = 5^m,\ m \in \mathbb{N}, \\ n^{1.5474} & \text{when } n = 6^m,\ m \in \mathbb{N}, \\ n^{1.5131} & \text{when } n = 7^m,\ m \in \mathbb{N}. \end{cases}$$

which are shown by Grošek and Horák [64].

- When $\lambda \in (0, 1)$ and $k = 2$, we get

$$a(Q) < n^2,$$

which is shown by Kotzig and Reischer [87].

- When $\lambda \in (0, 2]$ and $k = 2$, we get

$$a(Q) \leq 2 \cdot n^2,$$

which is the best bound so far [64].

In the experiment reported here, we use quasigroups with modular subtraction operation.

First, we check the associative triples for small order $|Q| = 3, 4, \ldots, 10$ and later for large order $|Q| = 2^3, 2^4, \ldots, 2^8$. We see that our achieved optimal results are quiet similar to Kotzig and Reischer's results [87].

2.4.1 Genetic algorithm for evolving isotopic quasigroups

The Genetic algorithm presented in this chapter uses random keys to encode the solutions. The use of random keys is described in [155] and is useful for problems that require permutations of the integers and for which crossover presents feasibile conditions. The technique is best illustrated with an example.

Consider a permutation (5 3 2 1 4), the solution 5 3 2 1 4 represents $4 \to 3 \to 2 \to 5 \to 1$, not $5 \to 3 \to 2 \to 1 \to 4$. In one-point crossover, may result in children with some nodes visited more than once and others not visited at all.

For example, the parents

$$\begin{array}{ccc|cc} 5 & 3 & 2 & 1 & 4 \\ 1 & 5 & 4 & 2 & 3 \end{array}$$

For example, the children

$$\begin{array}{ccc|cc} 5 & 3 & 2 & 2 & 3 \\ 1 & 5 & 4 & 1 & 4 \end{array}$$

In the random key method, we assign each gene a random number drawn uniformly from [0,1). To decode the chromosome, we visit the nodes in ascending order of their genes. For example:

$$\begin{array}{lccccc} \text{Random key:} & 0.25 & 0.31 & 0.03 & 0.87 & 0.69 \\ \text{Decodes as:} & 2 & 3 & 1 & 5 & 4 \end{array}$$

Nodes that early in the tour tend to evolve genes closer to 0 and those come later tend to evolve genes closer to 1. By this technique, crossover will generate children that are guaranteed to be feasible.

Encoding and Decoding for Isotopisms

Bean [9] suggests encoding for generalized traveling salesman problem (GTSP) as follows:

Suppose that set V has a gene consisting of an integer part (drawn from $\{1, ..., |V|\}$) and a fractional part (drawn from $[0, 1)$). The integer part indicates which node from the cluster is included on the tour, and the nodes are sorted by their fractional part as described above. For example, consider a instance with $V = \{1, ..., 20\}$ and breaks into clusters of four as $V_1 = \{1, ..., 5\}$, $V_2 = \{6, ..., 10\}$, $V_3 = \{11, ..., 15\}$, $V_4 = \{16, ..., 20\}$. The random key encoding is written as:

$$1.4130\ 4.5979\ 5.9808\ 2.7727$$

decodes as the tour $1 \rightarrow 9 \rightarrow 17 \rightarrow 15$: the integer parts of the genes represent the indexes of the elements from sets $V_1, \ldots, V_4$ respectively, i.e., 1st element from the set V_1, 4th element from the set V_2, 5th element from the set V_3 and 2nd element from the set V_4. The fractional parts is sorted by random key method which define that selected elements should be visited in the order $1 \rightarrow 2 \rightarrow 4 \rightarrow 3$.

Similarly we can consider three clusters V_1, V_2 and V_3 for permutations α, β and γ in S_K respectively. Each cluster has $n!$ permutations, so the integral part for random key encoding is drawn from $\{1, 2, \ldots, (n! - 1), n!\}$ and fractional part is drawn from $[0, 1)$. Now step-wise description of using Genetic algorithm is as follows:

Initial Populations: The initial population is created by generating N chromosomes (say, N = 20), each chromosomes has three genes for V_1, V_2 and V_3 respectively. The integer part of each gene is drawn randomly from $\{1, 2, \ldots, (n! - 1), n!\}$ and fractional part drawn randomly from $[0, 1)$. We improved this population by choosing the best combination among all via cost value.

GA Operator: At each generation, 20% of the population comes directly from the previous population via reproduction; chromosomes with crossover rate 0.5 are spawned via crossover; and genes from the selected chromosomes with mutation rate 0.1 are generated via mutation. We describe each of these operators next.

Reproductions: Our algorithm uses an elitist strategy of copying the best solutions in the population to the next generation. This guarantees monotonic non-degradation of the best solution from one generation to the next and ensures a constant supply of good individuals for mating.

Algorithm 2: The workflow of the using Genetic algorithms is as follows:

Form intial population (N) by using the technique described above;

$i \leftarrow 0$

while *Number of generations* **do**

  Compute the cost value of each chromosome by using cost function;

  Select best 20% of the population (which does not take part into crossovering):
  $\{P_1, P_2, \ldots, P_k\}$ is selected with index $\{p_1, p_2, \ldots, p_k\}$, where $k = N$ of 20%;

  Apply crossover strategy according to Section 2.4.1 on remaining population:
  Select $(P1, P2)$ with index (p_i, p_j)
  $Cross(P1, P2) = (C1, C2)$
  Define $X = \{C1, C2, S_{C1}, S_{C2}\}$
  $m = \text{cost}(C1)$
  $Y = X \setminus \{C1\}$
  $i \leftarrow 0$
  while $i < size(Y)$ **do**
    $c = \text{cost}(Y[i])$
    if $c > m$ **then**
      $m = c$
      New chromosome=$Y[i]$
    end
    $i = i + 1$
  end
  migrate (New chromosome) $\rightarrow N_{p_i}$;
  Apply mutation strategy according to Section 2.4.1 on updated population;
  New chromosomes = $\{N_{p_1}, N_{p_2}, \ldots, N_{p_k}, chromosomes\ after\ mutation\}$;
  $i = i + 1$

end

Crossover: We use parametrized uniform crossover [156] to generate offspring. First, two parents are chosen at random from the old population and the number of mate chromosomes is controlled by crossover rate (δ). Suppose we set that the crossover rate at 50%,

then chromosome number i will be selected for crossover if random generated value (R is generated from 0 to 1) for chromosome i is below 0.50. The following pseudocode is to select the parents for crossovering:

begin
  $i \leftarrow 0$
  while ($i < N$ of 80%) **do**
    Generate $R = R(0, 1)$
    if ($R < \delta$) **then**
      Parent = **chromosome[i]**
    end
    $i = i + 1$
  end
end

The crossovering technique is described in the above workflow chart from step 17 to 23. One child is generated from the two parents, and it inherits each gene from parent 1 with probability 0.7 and from parent 2 with probability 0.3.

Mutation: A small number of new individuals (Number of genes in choromosome $\times$ (N of 80%) $\times$ Mutation rate) are created in each generation, this mutation process helps to ensure a diverse population. Mutation process is done by generating a random integer between 1 and total genes (Number of genes in choromosome $\times$ (N of 80%)). If random generated value (R is generated from 0 to 1) is smaller than mutation rate (δ') then marked the position of gene in chromosomes. The pseudocode for mutation is as follows:

begin
  Total Genes = Number of genes in choromosome $\times$ (N of 80%)
  Mutated Genes = floor(Mutation rate $\times$ Total Genes)
  Generate U = [1, . . . ,Total Genes]
  $P = \{U_1, U_2, \ldots, U_{Mutated\ Genes}\}$
  while ($i < size(P)$) **do**
    Generate $R = R(0, 1)$
    if ($R < \delta'$) **then**
      Find the position of gene U_i,

Gene$[U_i] = (n!) \cdot R + 1$

end

$i = i + 1$

end

2.4.2 Comparison of results

Snášel et al. [154] constructed isotopic quasigroups to the quasigroup of modular subtraction by Genetic algorithm. Suppose that $(Q, *)$ is isotopic quasigroup to the given quasigroup $(K, \star)$, let X be the set of distinct triplets where elements are taken from K and Y be the set of distinct elements pairs where elements are taken from K, where the order does not matter and the repetitions are not allowed. They used the following fitness function for evolution:

$$f(n, n_a, n_c, \alpha) = \alpha \frac{n_2 - n_c}{n_2} + (1 - \alpha) \frac{n_3 - n_a}{n_3},$$

where $n = |K|$, $n_3 = |X|$, i.e., $C(n, 3)$, $n_2 = |Y|$, i.e., $C(n, 2)$ and

$$\begin{aligned} n_a =& |\{(x, y, z) \text{ in } X : \ (x * y) * z = x * (y * z)\}| \qquad \text{(i.e., associativity)}, \\ n_c =& |\{(x, y) \text{ in } Y : \ x * y = y * x\}| \qquad \text{(i.e., commutativity)}. \end{aligned}$$

The coefficient $\alpha \in [0, 1]$ is used to prioritize between commutativity and associativity. After 10 independent runs, they achieved the average value of best profile (n, n_a, n_c, α) by setting:

Parameters	Values
Population size	20
Selection operator	Elitist
Crossover rate	0.8
Mutation rate	0.02
Number of generations	1000

By using their fitness function and our Genetic approach, we get the following profile
We see that isotopic quasigroup to the modular subtraction quasigroup $(K, \star)$ also implies di-associativity and mono-associativity. By given isotopic quasigroup (In Section 2.2), we

Snášel et al. [154]	$(32, \mathbf{127.9}, 4.3, 0.5)$ $(64, \mathbf{543}, 5, 0.5)$ $(128, \mathbf{2593}, 24, 0.5)$
Our Algorithm	$(32, \mathbf{117}, 9.1, 0.5)$ $(64, \mathbf{531.7}, 19.6, 0.5)$ $(128, \mathbf{2512.6}, 63, 0.5)$

Table 2.4: Results for average value of n_a over 10 independent runs.

also get $(0, 6, 0)$, $(1, 3, 1)$, $(0, 0, 0)$, $(2, 2, 2)$ as associative triples and there also exist many more. Therefore we can not compare all associative triples of $(K, \star)$ with n_3.

On the purpose of finding all associative triples, we can not use the above fitness function for the evolution of isotopic quasigroups with minimum associative triples. In contrast, our proposed cost function is designed to reduce the upper bound of associative triples. Now we describe the exprimental details of proposed cost function and Genetic algorithm.

2.4.3 Exprimental details

We implemented the algorithm in MATLAB programming. Upto $|K| = 10$, we can easily carried out all permutations. However, the search space of all possible permutations is too large for an exhaustive search. Using proposed cost function and Genetic algorithm, we get the optimal isotopisms among all after carrying out many runs. For small orders, the best optimal value of associative triples is recorded in Table 2.5.

The permutations are generated for large order of quasigroups $(2^5, 2^6, \dots)$ by the technique described in Section 2.2. For large orders, the optimal value of associative triples is recorded in Table 2.6. The settings of Genetic algorithm are as follows:

Parameters	Values
Population size	20
Selection operator	Elitist
Crossover rate	0.5
Mutation rate	0.1
Number of generations	1000

$\|K\|$	$a(Q_{\alpha,\beta,\gamma})$	$\|K\|^2$
3	9	9
4	16	16
5	20	25
6	26	36
7	40	49
8	48	64
9	70	81
10	94	100

Table 2.5: Associativity index of small quasigroups.

$\|K\|$	$a(Q_{\alpha,\beta,\gamma})$	$\|K\|^2$
2^4	240	256
2^5	944	1024
2^6	3556	4096
2^7	14890	16384
2^8	60800	65536
2^9	245964	262144

Table 2.6: Associativity index of large quasigroups.

Chapter 3

The cryptographic properties of Feistel network based quasigroups

3.1 Introduction

The algebra of quasigroups was extensively studied by Drápal [44], Norton [127], Ježek and Kepka [71]. There are numerous applications of quasigroups in cryptography. The quasigroup structures and their properties are applied to many areas like: authentication schemes, secret sharing schemes, DES block cipher, pseudo random number generators and cryptographic hash functions for some applications we refer to ([7], [54], [61], [97], [153]) and for more details see [86, 147]. Gligoroski et al. [61] defined quasigroups as Boolean functions, Markovski and Mileva [104] generated huge quasigroups from small non-linear bijections via extended Feistel network. Mihajloska and Gligoroski [113] proposed a technique for constructing cryptographically strong 4 bit S-boxes via quasigroups of order 4. S-boxes ([17], [95]) were also constructed by use of Feistel and MISTY structures. In [94], Leander and Poschmann classified all optimal 4 bit S-boxes on the cryptographic point of view. For preventing many attacks on the ciphers, S-boxes are required to satisfy certain cryptographic properties ([107], [128], [130], [161]) for example having high nonlinearity, low differential uniformity and strict avalanche criteria (SAC) etc.

In introductory chapter [Section 1.10, Chapter 1] we already discussed importance of associative triple of quasigroups when it is used as construction of hash functions. In this chapter, we define the Feistel network based quasigroups. To evaluate the associative triples

for the corresponding quasigroups we obtain system of equations, and show that these equations depend on a certain permutation polynomial. Mollin and Small [124], Rivest [140], Singh and Maity [149] seek conditions on the coefficients of a polynomial which are necessary and sufficient for it to represent a permutation polynomial over finite fields. Therefore using different permutations over finite fields we solve these equations and get the counts for associative triples. Then we give the representation of Feistel network based quasigroups as vectorial Boolean functions. In the last Section, we find the relation between the cryptographic characterstics, i.e., nonlinearity, differential uniformity and SAC, of bijective mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ and Feistel network based quasigroups.

3.2 Preliminaries

Definition 3.2.1. *Suppose f is a bijective mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ and F is defined as:*

$$F : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$$
$$F(l, r) = (r, l + f(r)) \qquad \forall\ (l, r) \in \mathbb{F}_2^n \times \mathbb{F}_2^n.$$

This is known as Feistel network, where F is also a bijective on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ for $n \in \mathbb{N}$.

The following proposition is proved by Sade [143].

Proposition 3.2.2. [143, 14] *Let $(Q, +)$ be an admissible group with complete mapping θ. Then, $* : Q \times Q \to Q$ is defined as:*

$$x * y = \theta(x - y) + y,$$

where $x, y \in Q$. Then $(Q, *)$ is a quasigroup.

Proof. From the definition of quasigroup,

$$x * a = b \implies \theta(x - a) + a = b,$$
$$i.e., \quad \theta(x - a) = b - a \implies x - a = \theta^{-1}(b - a),$$
$$\text{or,} \quad x = a + \theta^{-1}(b - a).$$

Because θ is complete mapping then θ^{-1} is also permutation. Similarly

$$a * y = b \implies \theta(a - y) + y = b$$

$$\begin{aligned} i.e., \quad & \theta(a-y)+y-a=b-a \implies \theta(a-y)-(a-y)=(b-a) \\ i.e., \quad & (\theta-I)(a-y)=(b-a). \end{aligned}$$

Since θ is complete mapping then ϕ and ϕ^{-1} both are also permutations, where $(\theta-I)=\phi$ and $\phi^{-1}=\varphi$.

$$\begin{aligned} & \phi(a-y)=(b-a) \implies a-y=\varphi(b-a), \\ \text{or,} \quad & y=a-\varphi(b-a) \qquad \forall\ a,b\in Q. \end{aligned}$$

Here x and y are unique. Thus $(Q,*)$ is a quasigroup. ∎

Lemma 3.2.3. [104, Definition 3.1] *The Feistel network F is bijective with inverse*

$$F^{-1}(l,r)=(r+f(l),l).$$

Proof. Since

$$F(l,r)=(r,l+f(r)).$$

We define the function $F^{-1}\colon \mathbb{F}_2^n\times\mathbb{F}_2^n\to\mathbb{F}_2^n\times\mathbb{F}_2^n$ by

$$F^{-1}(l,r)=(r+f(l),l).$$

We have

$$F^{-1}\circ F(l,r)=F^{-1}(r,l+f(r))=(l+f(r)+f(r),r)$$

$$=(l,r)$$

Similarly,

$$F\circ F^{-1}(l,r)=F(r+f(l),l)=(l,r+f(l)+f(l))$$

$$=(l,r)$$ ∎

We have $F\circ F^{-1}=F^{-1}\circ F=I$, i.e., F and F^{-1} both are bijective. Here we see that the bijection of F does not depend on f but for complete mapping it is required that f should be bijective.

Lemma 3.2.4. [104, Theorem 3.1] *If F is Feistel network created by bijection f then F is a complete mapping.*

Proof. Let $\Omega = F - I$ where I is an identity mapping on $\mathbb{F}_2^n \times \mathbb{F}_2^n$. Then

$$\begin{aligned}\Omega : \mathbb{F}_2^n \times \mathbb{F}_2^n &\to \mathbb{F}_2^n \times \mathbb{F}_2^n \\ \Omega(l,r) &= (r+l, l+r+f(r)) \qquad \forall\ (l,r) \in \mathbb{F}_2^n \times \mathbb{F}_2^n.\end{aligned}$$

We have to show Ω is also permutation with inverse

$$\Omega^{-1}(l,r) = (l + f^{-1}(l+r), f^{-1}(l+r)).$$

Then

$$\begin{aligned}\Omega^{-1} \circ \Omega(l,r) &= \Omega^{-1}(r+l, l+r+f(r)) \\ &= (r+l+f^{-1}(r+l+l+r+f(r)), f^{-1}(r+l+l+r+f(r))) \\ &= (r+l+r, r) = (l,r).\end{aligned}$$

Similarly,

$$\begin{aligned}\Omega \circ \Omega^{-1}(l,r) &= \Omega(l + f^{-1}(l+r), f^{-1}(l+r)) \\ &= (f^{-1}(l+r) + l + f^{-1}(l+r), l + f^{-1}(l+r) + f^{-1}(l+r) + f(f^{-1}(l+r)) \\ &= (l, l+l+r) = (l,r).\end{aligned}$$

We have $\Omega \circ \Omega^{-1} = \Omega^{-1} \circ \Omega = I$, i.e., Ω and Ω^{-1} both are bijective mapping. ∎

Therefore $(\mathbb{F}_2^{2n}, +)$ is admissible with a complete mapping F. Let $Q = \mathbb{F}_2^n \times \mathbb{F}_2^n$. Then, $* : Q \times Q \to Q$ is defined as a binary operation on Q as follows:

$$\begin{aligned}* : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} &\to \mathbb{F}_2^{2n} \\ x * y &= F(x+y) + y.\end{aligned}$$

Then Q is also a quasigroup with respect to $*$ by Proposition 3.2.2. It is shown that quasigroups derived from additive groups or $(\mathbb{F}_2^{2n}, +)$ in Example 1.8.4 for $n = 2$.

3.3 Equations satisfied by associativity condition

In this section, we estimate the number of associative triples $a(Q)$ based on the different selection of f. We have to find those triples x, y and z in Q which satisfy

$$(x * y) * z = x * (y * z).$$

Let $x = (l_1, r_1), y = (l_2, r_2), z = (l_3, r_3)$, then

$$((l_1, r_1) * (l_2, r_2)) * (l_3, r_3) = \quad (l_1, r_1) * ((l_2, r_2) * (l_3, r_3)). \tag{3.3.1}$$

First of all we solve for

$$\begin{aligned}(l_1, r_1) * (l_2, r_2) &= F((l_1, r_1) + (l_2, r_2)) + (l_2, r_2) \\ &= F(l_1 + l_2, r_1 + r_2) + (l_2, r_2) \\ &= (r_1 + r_2, l_1 + l_2 + f(r_1 + r_2)) + (l_2, r_2) \\ &= (l_2 + r_1 + r_2, l_1 + l_2 + r_2 + f(r_1 + r_2)),\end{aligned}$$

or

$$(l_1, r_1) * (l_2, r_2) = (l_2 + r_1 + r_2, l_1 + l_2 + r_2 + f(r_1 + r_2)). \tag{3.3.2}$$

From Equation (3.3.2) we solve

$$\begin{aligned}((l_1, r_1) * (l_2, r_2)) * (l_3, r_3) &= (l_2 + r_1 + r_2, l_1 + l_2 + r_2 + f(r_1 + r_2)) * (l_3, r_3) \\ &= F((l_2 + r_1 + r_2, l_1 + l_2 + r_2 + f(r_1 + r_2)) + (l_3, r_3)) + (l_3, r_3) \\ &= F(l_2 + l_3 + r_1 + r_2, l_1 + l_2 + r_2 + r_3 + f(r_1 + r_2)) + (l_3, r_3) \\ &= (l_1 + l_2 + r_2 + r_3 + f(r_1 + r_2), l_2 + l_3 + r_1 + r_2 + \\ &\quad f(l_1 + l_2 + r_2 + r_3 + f(r_1 + r_2))) + (l_3, r_3) \\ &= (l_1 + l_2 + l_3 + r_2 + r_3 + f(r_1 + r_2), l_2 + l_3 + r_1 + r_2 + r_3 + \\ &\quad f(l_1 + l_2 + r_2 + r_3 + f(r_1 + r_2))),\end{aligned}$$

or

$$((l_1,r_1)*(l_2,r_2))*(l_3,r_3) = (l_1+l_2+l_3+r_2+r_3+f(r_1+r_2), l_2+l_3+r_1+r_2+r_3+ f(l_1+l_2+r_2+r_3+f(r_1+r_2))). \tag{3.3.3}$$

Similarly, firstly we solve for

$$\begin{aligned}(l_2,r_2)*(l_3,r_3) &= F((l_2,r_2)+(l_3,r_3))+(l_3,r_3)\\ &= F(l_2+l_3,r_2+r_3)+(l_3,r_3)\\ &= (r_2+r_3, l_2+l_3+f(r_2+r_3))+(l_3,r_3)\\ &= (l_3+r_2+r_3, l_2+l_3+r_3+f(r_2+r_3)),\end{aligned}$$

or

$$(l_2,r_2)*(l_3,r_3) = (l_3+r_2+r_3, l_2+l_3+r_3+f(r_2+r_3)), \tag{3.3.4}$$

then from Equation (3.3.4)

$$\begin{aligned}(l_1,r_1)*((l_2,r_2)*(l_3,r_3)) &= (l_1,r_1)*(l_3+r_2+r_3, l_2+l_3+r_3+f(r_2+r_3))\\ &= F((l_1,r_1)+(l_3+r_2+r_3, l_2+l_3+r_3+f(r_2+r_3)))+\\ &\quad (l_3+r_2+r_3, l_2+l_3+r_3+f(r_2+r_3))\\ &= F(l_1+l_3+r_2+r_3, l_2+l_3+r_1+r_3+f(r_2+r_3))+\\ &\quad (l_3+r_2+r_3, l_2+l_3+r_3+f(r_2+r_3))\\ &= (l_2+l_3+r_1+r_3+f(r_2+r_3), l_1+l_3+r_2+r_3+f(l_2+l_3+\\ &\quad r_1+r_3+f(r_2+r_3))+(l_3+r_2+r_3, l_2+l_3+r_3+f(r_2+r_3))\\ &= (l_2+2l_3+r_1+r_2+2r_3+f(r_2+r_3), l_1+l_2+2l_3+r_2+\\ &\quad 2r_3+f(r_2+r_3)+f(l_2+l_3+r_1+r_3+f(r_2+r_3)),\end{aligned}$$

or

$$(l_1,r_1)*((l_2,r_2)*(l_3,r_3)) = (l_2+2l_3+r_1+r_2+2r_3+f(r_2+r_3), l_1+l_2+2l_3+r_2+ 2r_3+f(r_2+r_3)+f(l_2+l_3+r_1+r_3+f(r_2+r_3))). \tag{3.3.5}$$

With the help of Equations (3.3.3) and (3.3.5) we simplify Equation (3.3.1)

$$((l_1, r_1) * (l_2, r_2)) * (l_3, r_3) = (l_1, r_1) * ((l_2, r_2) * (l_3, r_3)).$$

Doing component-wise comparison, the first component gives us

$$l_1 + l_2 + l_3 + r_2 + r_3 + f(r_1 + r_2) = l_2 + 2l_3 + r_1 + r_2 + 2r_3 + f(r_2 + r_3)$$
$$f(r_1 + r_2) + f(r_2 + r_3) = l_1 + l_3 + r_1 + r_3$$

$$f(r_1 + r_2) + f(r_2 + r_3) = l_1 + l_3 + (r_1 + r_2) + (r_2 + r_3). \tag{3.3.6}$$

Now, the second component gives us

$$l_2 + l_3 + r_1 + r_2 + r_3 + f(l_1 + l_2 + r_2 + r_3 + f(r_1 + r_2))$$
$$= l_1 + l_2 + 2l_3 + r_2 + 2r_3 + f(r_2 + r_3) + f(l_2 + l_3 + r_1 + r_3 + f(r_2 + r_3)),$$

or

$$l_1+l_3+r_1+r_3+f(r_2+r_3)+f(l_2+l_3+r_1+r_3+f(r_2+r_3))+f(l_1+l_2+r_2+r_3+f(r_1+r_2)) = 0,$$

or

$$l_1 + l_3 = (r_1 + r_2) + (r_2 + r_3) + f(r_2 + r_3) + f(l_2 + l_3 + r_1 + r_3 + f(r_2 + r_3)) + f(l_1 + l_2 + r_2 + r_3 + f(r_1 + r_2)). \tag{3.3.7}$$

So, finally we get two Equations (3.3.6) and (3.3.7)

$$f(r_1 + r_2) + f(r_2 + r_3) = l_1 + l_3 + (r_1 + r_2) + (r_2 + r_3)$$
$$l_1 + l_3 = (r_1 + r_2) + (r_2 + r_3) + f(r_2 + r_3) + f(l_2 + l_3 + r_1 + r_3 + f(r_2 + r_3)) + f(l_1 + l_2 + r_2 + r_3 + f(r_1 + r_2)).$$

Now we choose $X = r_1 + r_2$ and $Y = r_2 + r_3$ such that $X + Y = r_1 + r_3$ then the modified form of Equations (3.3.6) and (3.3.7) for fix $L = l_1 + l_3$ and $M = l_1 + l_2$ are as follows :

$$f(X) + f(Y) = X + Y + L \tag{3.3.8}$$

and

$$L = X + Y + f(Y) + f(l_2 + l_3 + X + Y + f(Y)) + f(l_1 + l_2 + Y + f(X)),$$

using Equation (3.3.8) we get

$$L = L + f(X) + f(l_2 + l_3 + L + f(X)) + f(l_1 + l_2 + Y + f(X))$$
$$f(X) = f(l_1 + l_2 + f(X)) + f(l_1 + l_2 + Y + f(X)),$$

or

$$f(X) = f(M + f(X)) + f(Y + M + f(X)). \tag{3.3.9}$$

3.4 Counting the number of associative triples for linear and quadratic permutation monomials

Theorem 3.4.1. [96, Theorem 7.8]

(*i*) *Every linear polynomial over* $\mathbb{F}_{2^n}$ *is a permutation polynomial of* $\mathbb{F}_{2^n}$.

(*ii*) *The monomial* x^n *is a permutation polynomial of* $\mathbb{F}_{2^n}$ *if and only if* $gcd(n, 2^n - 1) = 1$.

It is known that $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$ both are isomorphic under vector isomorphism over $\mathbb{F}_2$.

Case 1. In general, a linear application will not change the properties of the function. Here we introduced the polynomial corresponding to linear applications. Let $f(X) = X^{2^i}$ where $X \in \mathbb{F}_{2^n}$. By Equation (3.3.8) we get

$$X^{2^i} + Y^{2^i} = X + Y + L \tag{3.4.1}$$

and by Equation (3.3.9) we get

$$\begin{aligned} X^{2^i} &= (M + X^{2^i})^{2^i} + (M + Y + X^{2^i})^{2^i} \\ &= (M)^{2^i} + (X^{2^i})^{2^i} + (M)^{2^i} + (Y)^{2^i} + (X^{2^i})^{2^i} \\ &= Y^{2^i} \\ i.e., \quad X &= Y \\ r_1 + r_2 &= r_3 + r_2 \\ r_1 &= r_3. \end{aligned}$$

By Equation (3.4.1) we get $L = 0 \Rightarrow l_1 + l_3 = 0 \Rightarrow l_1 = l_3$.

So, $(l_1, r_1) \equiv (l_3, r_3)$.

Thus the number of associative triples are exactly N^2, where $N = 2^n \times 2^n$.

Case 2. Now we check for quadratic permutation polynomials. Let $f(X) = X^{2^i+1}$ where $X \in \mathbb{F}_{2^n}$. By Equation (3.3.9) we get

$$X^{2^i+1} = (M + X^{2^i+1})^{2^i+1} + (M + X^{2^i+1} + Y)^{2^i+1}$$

$$= (M + X^{2^i+1})^{2^i+1} + (M + X^{2^i+1})^{2^i+1} + (M + X^{2^i+1})^{2^i}Y + (M + X^{2^i+1})Y^{2^i} + Y^{2^i+1}$$

$$X^{2^i+1} + Y^{2^i+1} = (M + X^{2^i+1})^{2^i}Y + (M + X^{2^i+1})Y^{2^i}$$

$$M^{2^i}Y + (X^{2^i+1})^{2^i}Y + MY^{2^i} + (X^{2^i+1})Y^{2^i} = X^{2^i+1} + Y^{2^i+1}$$

$$M^{2^i}Y + MY^{2^i} = X^{2^i+1} + Y^{2^i+1} + (X^{2^i+1})^{2^i}Y + (X^{2^i+1})Y^{2^i}.$$

Suppose that $X^{2^i+1} + Y^{2^i+1} + (X^{2^i+1})^{2^i}Y + (X^{2^i+1})Y^{2^i} = C$ is fixed in $\mathbb{F}_2^n$, then

$$M^{2^i}Y + MY^{2^i} = C. \tag{3.4.2}$$

If $C = 0$ then

$$M^{2^i}Y + MY^{2^i} = 0 \implies M^{2^i-1} = Y^{2^i-1}$$

$$M \in Y(G\backslash\{0\}).$$

Where G is the subfield of $\mathbb{F}_{2^n}$ of order 2^e, $e = gcd(i, n)$. Thus the number of choices for M is at most 2^e that satisfy the homogeneous part of Equation (3.3.9) for fixed Y in $\mathbb{F}_{2^n}$.

If $C \neq 0$, the solutions of Equation (3.4.2) is either zero or equal to same number of solutions of homogeneous part. Therefore we have at most 2^e solutions of Equation (3.4.2) in any case. When $e = 1$, then Equation (3.4.2) works as almost perfect nonlinear (APN) functions and when $e = 2$, then Equation (3.4.2) works as inverse functions. Thus the maximum number of solutions of Equation (3.3.9) is $2^e \cdot 2^{n-1} \cdot 2^n \cdot 2^n \cdot 2^n$ or $2^{e-1} \cdot N^2$, where $N = 2^n \cdot 2^n$.

3.5 Counting the number of associative triples for various permutation monomials

With the help of these equations we can count the number of associative triples $a(Q)$ for taking different types of permutations. In this Section we found the value of $a(Q)$ after using almost perfect nonlinear (APN) permutations, differentially 4-uniform functions and differentially δ-uniform functions over $\mathbb{F}_2^n$.

3.5.1 APN permutations over $\mathbb{F}_2^n$

Definition 3.5.1. [100, Definition 1.2.6] *Let f is mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. For $0 \neq a \in \mathbb{F}_2^n$, $D_a(f)$ is defined as :*

$$D_a(f) = \{f(x) + f(x+a) : x \in \mathbb{F}_2^n\}.$$

Then, f is APN (almost perfect nonlinear) if $|D_a(f)| = 2^{n-1}$ for all $0 \neq a \in \mathbb{F}_2^n$.

as well as:

Definition 3.5.2. [100, Definition 1.2.7] *A function f is APN if and only if the system of equations*

$$\begin{cases} x + y & = a \\ f(x) + f(y) & = b \end{cases}$$

has 0 or 2 solutions (x, y) for any $0 \neq a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^n$.

However, these functions correspond to APN permutations and the number of solutions of the above equations is always even number for any f on $\mathbb{F}_2^n$.
We have two Equations (3.3.8) and (3.3.9)

$$f(X) + f(Y) = X + Y + L \tag{3.5.1}$$

and

$$f(X) = f(M + f(X)) + f(Y + M + f(X)). \tag{3.5.2}$$

Suppose $z = M + f(X)$. Then from Equation (3.5.2), we get

$$f(z) + f(z + Y) = f(X). \tag{3.5.3}$$

With the help of these Equations (3.5.1) and (3.5.3) we can count the number of associative triples after putting the condition over Y.

Case-1: Let $Y = 0$, then from Equation (3.5.3)

$$f(X) = 0.$$

Hence $X = 0$ because f is bijective. If $Y = 0$ and $X = 0$ then $L = 0$ by Equation (3.5.1). That means $X = r_1 + r_2 = 0 \Rightarrow r_1 = r_2$, $Y = r_2 + r_3 = 0 \Rightarrow r_2 = r_3$ and $L = l_1 + l_3 = 0 \Rightarrow l_1 = l_3$. So,

$$(l_1, r_1) \equiv (l_3, r_3),$$

and only l_2 is fixed in $\mathbb{F}_2^n$. Thus the number of possible solutions of the Equations (3.5.1) and (3.5.3) is $N.\sqrt{N}$.

Case-2: Let $Y \neq 0$, then from Equation (3.5.3), f is APN (almost perfect nonlinear) with

$$D_Y(f) = \{f(z + Y) + f(z) : z \in \mathbb{F}_2^n\},$$

$|D_Y(f)| = 2^{n-1}$ for all $0 \neq Y \in \mathbb{F}_2^n$. The system of Equations (3.5.1) and (3.5.3) for every $(Y, f(X)) \neq (0, 0)$ have 0 or 2 solutions. Here $X, Y, f(X)$ and $f(Y)$ are fixed, so L is also fix by Equation (3.5.1) in $\mathbb{F}_2^n$. Thus the number of possible solutions of these equations are $2 \cdot (2^n - 1) \cdot (2^{n-1}) \cdot 2^n \cdot 2^n$ or

$$N^2 - N \cdot \sqrt{N}.$$

Hence the total number of counts for APN over $\mathbb{F}_2^n$ are $a(Q) = N^2 - N \cdot \sqrt{N} + N \cdot \sqrt{N} = N^2$, where $N = 2^n \times 2^n$.

3.5.2 Differentially 4-uniform permutations

Similarly, let f be differentially 4-uniform, i.e., for any $0 \neq a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^n$, the equation

$$f(x + a) + f(x) = b$$

has at most 4 solutions.

Definition 3.5.3. *A function f is differentially 4-uniform if and only if the system of equations*

$$\begin{cases} x+y & = a \\ f(x)+f(y) & = b \end{cases}$$

has at most 4 solutions (x, y) for any $0 \neq a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^n$.

From Equation (3.5.3), $0 \neq Y \in \mathbb{F}_2^n$ that means Y takes value $(2^n - 1)$ and we vary z in $\mathbb{F}_2^n$

$$f(z_i) + f(z_i + Y) = f(X) \text{ , where } i = 0, 1, 2, \ldots, 2^{n-1}.$$

Let n_1 combination of right hand side of this equation goes to 2 solution and n_2 combination goes to 4 solution. The total number of possibilies are

$$2n_1 + 4n_2 = 2^n,$$
$$n_1 + 2n_2 = 2^{n-1}.$$

Here $X, Y, f(X)$ and $f(Y)$ are fixed, so L is also fix by Equation (3.5.1) in $\mathbb{F}_2^n$. Thus the number of possible solutions of these equations is

$$\{(2^n - 1)n_1 \cdot 2 + (2^n - 1)n_2 \cdot 4\}2^n \cdot 2^n,$$
$$2 \cdot (2^n - 1)\{n_1 + 2 \cdot n_2\}2^n \cdot 2^n,$$
$$2 \cdot (2^n - 1) \cdot 2^{n-1} \cdot 2^n \cdot 2^n,$$
$$N^2 - N \cdot \sqrt{N}.$$

Hence the total number of counts for differentially 4-uniform over $\mathbb{F}_2^n$ is same as APN pemutations $a(Q) = N^2 - N \cdot \sqrt{N} + N \cdot \sqrt{N} = N^2$, where $N = 2^n \times 2^n$.

3.5.3 Differentially δ-uniform permutations

Let f be differentially δ-uniform, i.e., for any $0 \neq a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^n$, the equation

$$f(x + a) + f(x) = b$$

has at most δ solutions.

Definition 3.5.4. *A function f is differentially δ-uniform if and only if the system of equations*

$$\begin{cases} x + y & = a \\ f(x) + f(y) & = b \end{cases}$$

has at most δ solutions (x, y) for any $0 \neq a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^n$.

From Equation (3.5.3), $0 \neq Y \in \mathbb{F}_2^n$ that means Y takes value $(2^n - 1)$ and we vary z in $\mathbb{F}_2^n$

$$f(z_i) + f(z_i + Y) = f(X) \text{ , where } i = 0, 1, 2, \ldots, 2^{n-1}.$$

Let n_1 combination of right hand side of this equation goes to 2 solution, n_2 combination goes to 4 solution, n_3 combination goes to 6 solution and so on n_δ combination goes to δ solution. The total number of possibilies are

$$2n_1 + 4n_2 + 6n_3 + ... + \delta n_\delta = 2^n,$$
$$n_1 + 2n_2 + 3n_3 + ... + (\delta/2)n_\delta = 2^{n-1}.$$

Here $X, Y, f(X)$ and $f(Y)$ are fixed, so L is also fix by Equation (3.5.1) in $\mathbb{F}_2^n$. Thus the number of possible solutions of these equations is

$$\{(2^n - 1)n_1 \cdot 2 + (2^n - 1)n_2 \cdot 4 + (2^n - 1)n_3 \cdot 6 + \cdots + (2^n - 1)n_\delta \cdot \delta\}2^n \cdot 2^n,$$
$$2 \cdot (2^n - 1)\{n_1 + 2n_2 + 3n_3 + \cdots + (\delta/2)n_\delta\}2^n \cdot 2^n,$$
$$2 \cdot (2^n - 1) \cdot 2^{n-1} \cdot 2^n \cdot 2^n,$$
$$N^2 - N \cdot \sqrt{N}.$$

Hence the total number of counts for differentially δ-uniform over $\mathbb{F}_2^n$ is same as APN permutations $a(Q) = N^2 - N \cdot \sqrt{N} + N \cdot \sqrt{N} = N^2$, where $N = 2^n \times 2^n$.

3.6 Cryptographic properties for Feistel network based quasigroup

In this Section, we give details proof of the results, using Canteaut et al. [17] technique which shows the dependency of the cryptographic properties (nonlinearity, differential uniformity and SAC) of the resulting G (Feistel network based quasigroup) on the f (bijective

mapping). We can write the Feistel network based quasigroup as vectorial Boolean function using that $x \equiv (x_l, x_r)$ and $y \equiv (y_l, y_r)$ and let G be its corresponding representation as vectorial Boolean function. Then, From Definition 3.2.1 we get

$$\begin{aligned} x * y &= F((x_l, x_r) + (y_l, y_r)) + (y_l, y_r) \\ &= F(x_l + y_l, x_r + y_r) + (y_l, y_r) \\ &= (x_r + y_r, x_l + y_l + f(x_r + y_r)) + (y_l, y_r) \\ &= (x_r + y_l + y_r, x_l + y_l + y_r + f(x_r + y_r)), \end{aligned}$$

or, we can write

$$G(x_L, x_R) = G(x_L \| x_R) = (x_r \oplus y_l \oplus y_r, x_l \oplus y_l \oplus y_r \oplus f(x_r \oplus y_r)).$$

The generalized results and their proofs are given in the following section.

3.6.1 Nonlinearity

Proposition 3.6.1. *Let f be an n bit vectorial Boolean function and G be an $2n$ bit function defined by Feistel network. Then, we get:*

$$W_G((a,b) \parallel (c,d), e \parallel k) = \begin{cases} 2^{3n} \cdot W_f(b \oplus e, k) & if\ a \oplus k = 0, c \oplus e \oplus k = 0 \\ & and\ b \oplus d \oplus k = 0, \\ 0 & else. \end{cases}$$

for all a, b, c, d, e and k in $\mathbb{F}_2^n$. Moreover, the linearity of f is

$$\mathcal{L}(f) = \max_{b \oplus e \in \mathbb{F}_2^n, k \in (\mathbb{F}_2^n)^*} \mid W_f(b \oplus e, k) \mid .$$

When $a \oplus k = 0$, $c \oplus e \oplus k = 0$ and $b \oplus d \oplus k = 0$, we get

$$\mathcal{L}(G) > \mathcal{L}(f),$$

and

$$nl(G) < nl(f).$$

Proof. The Walsh transform of G is the mapping $W_G : (\mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n}) \times \mathbb{F}_2^{2n} \to \mathbb{Z}$, defined as

$$W_G((u_1, u_2), v) = \sum_{(x,y)\in(\mathbb{F}_2^{2n}\times\mathbb{F}_2^{2n})} (-1)^{(u_1,u_2)\cdot(x,y)\oplus v\cdot G(x,y)}$$

or

$$W_G(u_1\|u_2, v) = \sum_{(x,y)\in(\mathbb{F}_2^{2n}\times\mathbb{F}_2^{2n})} (-1)^{(u_1\|u_2)\cdot(x\|y)\oplus v\cdot G(x\|y)}.$$

Let $u_1 \equiv (a, b)$, $u_2 \equiv (c, d)$ and $v \equiv (e, k)$, the following result corresponding to the

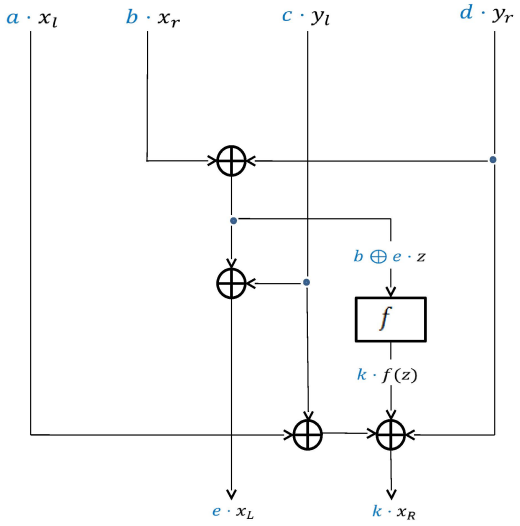


Figure 3.1: Blue values indicate linear masks.

configurations depicted on 3.1.

$$\begin{aligned} W_G((a,b) \parallel (c,d), e \parallel k) &= \textstyle\sum_{(x_l,x_r,y_l,y_r)\in(\mathbb{F}_2^n)^4} (-1)^{((a,b)\|(c,d))\cdot((x_l,x_r)\|(y_l,y_r))\oplus(e,k)\cdot G(x_L\|x_R)} \\ &= \sum_{(x_l,x_r,y_l,y_r)\in(\mathbb{F}_2^n)^4} (-1)^{(a,b,c,d)\cdot(x_l,x_r,y_l,y_r)\oplus(e,k)\cdot(x_r\oplus y_l\oplus y_r, x_l\oplus y_l\oplus y_r\oplus f(x_r\oplus y_r))} \\ &= \sum_{(x_l,x_r,y_l,y_r)\in(\mathbb{F}_2^n)^4} (-1)^{a\cdot x_l\oplus b\cdot x_r\oplus c\cdot y_l\oplus d\cdot y_r\oplus e\cdot x_r\oplus e\cdot y_l\oplus e\cdot y_r\oplus k\cdot x_l\oplus k\cdot y_l\oplus k\cdot y_r\oplus k\cdot f(x_r\oplus y_r)} \end{aligned}$$

We set $x_r = y_r \oplus z$ and observe that, for any fixed y_r, z takes all possible values in $\mathbb{F}_2^n$ when x_r varies, implying that

$$\begin{aligned} W_G((a,b) \parallel (c,d), e \parallel k) &= \textstyle\sum_{x_l\in\mathbb{F}_2^n} (-1)^{(a\oplus k)\cdot x_l} \sum_{y_l\in\mathbb{F}_2^n} (-1)^{(c\oplus e\oplus k)\cdot y_l} \\ &\quad \textstyle\sum_{y_r\in\mathbb{F}_2^n} (-1)^{(b\oplus d\oplus k)\cdot y_r} \sum_{z\in\mathbb{F}_2^n} (-1)^{(b\oplus e)\cdot z\oplus k\cdot f(z)} \end{aligned}$$

$$W_G((a,b) \parallel (c,d), e \parallel k) = \sum_{x_l \in \mathbb{F}_2^n} (-1)^{(a \oplus k)\cdot x_l} \sum_{y_l \in \mathbb{F}_2^n} (-1)^{(c \oplus e \oplus k)\cdot y_l} \sum_{y_r \in \mathbb{F}_2^n} (-1)^{(b \oplus d \oplus k)\cdot y_r} W_f(b \oplus e, k).$$

If $w \in \mathbb{F}_2^n$, we have

$$\sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot w} = \begin{cases} 2^n & if\ w = 0, \\ 0 & else. \end{cases}$$

Then we drive the following bound

$$W_G((a,b) \parallel (c,d), e \parallel k) = \begin{cases} 2^{3n} \cdot W_f(b \oplus e, k) & if\ a \oplus k = 0, c \oplus e \oplus k = 0 \\ & and\ b \oplus d \oplus k = 0, \\ 0 & else. \end{cases}$$

■

3.6.2 Differential uniformity

Proposition 3.6.2. *Let f be an n bit vectorial Boolean function and G be an $2n$ bit function defined by Feistel network. Then, we get:*

$$\delta_G((a,b) \parallel (c,d), e \parallel k) = \delta_f(b \oplus d \to a \oplus b \oplus e \oplus k)$$

for all a, b, c, d, e and k in $\mathbb{F}_2^n$.

Proof. The following result corresponding to the configurations depicted on 3.2.

Then, (x_L, x_R) satisfies $G(x_L \| x_R) \oplus G((x_L \oplus u_1) \| (x_R \oplus u_2)) = e \| k$, where $u_1 \equiv (a,b)$ and $u_2 \equiv (c,d)$, if and only if

$$\begin{cases} x_r \oplus y_l \oplus y_r \oplus x_r \oplus b \oplus y_l \oplus c \oplus y_r \oplus d = e, \\ x_l \oplus y_l \oplus y_r \oplus f(x_r \oplus y_r) \oplus x_l \oplus a \oplus y_l \oplus c \oplus y_r \oplus d \oplus f(x_r \oplus b \oplus y_r \oplus d) = k. \end{cases}$$

$$\Leftrightarrow \begin{cases} b \oplus c \oplus d = e, \\ f(x_r \oplus y_r) \oplus f(x_r \oplus y_r \oplus b \oplus d) = a \oplus c \oplus d \oplus k. \end{cases}$$

Equivalently

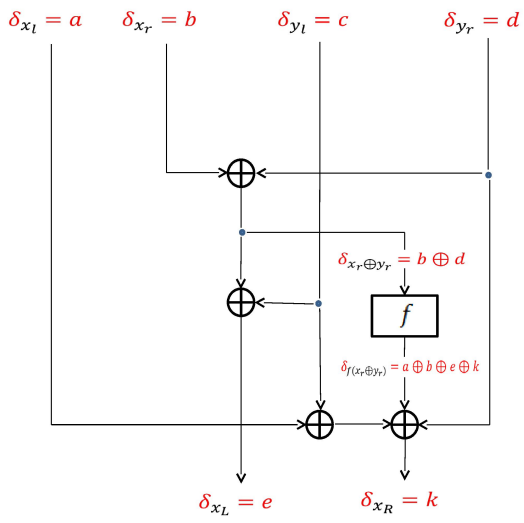


Figure 3.2: Red values indicate differences.

$x_r \oplus y_r \in D_f(b \oplus d \to a \oplus c \oplus d \oplus k)$ or $x_r \oplus y_r \in D_f(b \oplus d \to a \oplus b \oplus e \oplus k)$,

or

$y_r \in x_r \oplus D_f(b \oplus d \to a \oplus b \oplus e \oplus k)$.

Hence, for any fixed x_r in $\mathbb{F}_2^n$, a unique value of y_r is determined by above condition. Therefore the number of (x_L, x_R) satisfying the differential is exactly $1 \cdot 1 \cdot 1 \cdot \delta_f(b \oplus d \to a \oplus b \oplus e \oplus k)$ or $\delta_f(b \oplus d \to a \oplus b \oplus e \oplus k)$. ■

3.6.3 Strict Avalanche Criteria (SAC)

Proposition 3.6.3. *Let f be an n bit vectorial Boolean function and G be an $2n$ bit function defined by Feistel network. Then even if f satisfies SAC, G can never satisfy SAC.*

Proof. We have

$$G(x_L \| x_R) = (x_r \oplus y_l \oplus y_r, x_l \oplus y_l \oplus y_r \oplus f(x_r \oplus y_r)).$$

Here we see that the left part of G has n-coordinate functions and each coordinate function is either linear or affine. Kim et al. ([83], Theorem 1) proved that the affine functions can not satisfy SAC. Hence the left part of G never satisfies SAC even the right part of G somehow satisfies. Therefore G can never be satisfied SAC. ■

Chapter 4

Constructions of quasigroups via permutations over $\mathbb{F}_{2^n}$ and their cryptographic characteristics

4.1 Introduction

In this chapter, we propose an efficient construction of quasigroups which are based on two different permutations over $\mathbb{F}_{2^n}$ inspired by Kotzig and Reischer's construction [87] of quasigroups which is based on finite commutative, but not necessarily associative and unitary, ring. We see that the algebraic properties of this construction extensively depend on using permutations. It is known that number of associative triples or associativity index are connected to a security criterion of a quasigroup when used as a hash function. Therefore we investigate the counts of associative triples for different permuatations, i.e., linear permutations, affine permutations, quadractic permutations and complete mapping permutations over $\mathbb{F}_{2^n}$.

It is also known that quasigroups of order 2^n are represented as vectorial Boolean functions $f : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$, for further details we refer to [61]. Later we also investigate how the cryptographic characteristics, i.e., nonlinearity and differential uniformity affect the obtained quasigroups and using permutations as vectorial Boolean functions.

4.2 Construction of quasigroups inspired by Kotzig and Reischer

The following construction was proposed by Kotzig and Reischer [87]. Let $R = (Q, +, \cdot)$ be a finite commutative, but not necessarily associative and unitary, ring. Let $R' = \{r \in Q : rx = 0 \Leftrightarrow x = 0\}$. For $r, s \in R'$ and $t \in Q$, let define $R_{r,s,t} = (Q, *)$ where

$$x * y = rx + sy + t,$$

for all $x, y \in Q$. Clearly $R_{r,s,t}$ is a quasigroup [87].

Lemma 4.2.1. *$R_{r,s,t}$ is a group if and only if R is unitary and $r = s = 1_R$.*

Proof. We say $R_{r,s,t}$ is a group under this operation if the following three properties, i.e., associativity, existence of identity and inverse are satisfied.

Associativity. The operation is associative, i.e., $x * (y * z) = (x * y) * z, \forall\ x, y, z \in Q$. So we get,

$$(r^2 - r) \cdot x - (s^2 - s) \cdot z = (s - r) \cdot t \tag{4.2.1}$$

Identity. There is an element e (called the identity) in Q, such that $x * e = e * x = x, \forall\ x \in Q$. So we get,

$$\begin{aligned} r \cdot (x - e) &= s \cdot (x - e) && \{\text{by Cancellation property}\} \\ r &= s \end{aligned}$$

Inverses. For each element x in Q, there is an element x' in Q (called an inverse of x) such that $x * x' = x' * x = e$. So we get

$$\begin{aligned} r \cdot (x - x') &= s \cdot (x - x') && \{\text{by Cancellation property}\} \\ r &= s \end{aligned}$$

Put $r = s$ in Equation (4.2.1), then we get

$$(r^2 - r) \cdot (x - z) = 0$$

$$\begin{aligned} r[(r-1)\cdot(x-z)] &= 0 \\ (r-1)\cdot(x-z) &= 0 \qquad \{\text{by definition of } R'\} \\ r\cdot(x-z) &= 1\cdot(x-z) \end{aligned}$$

$$r\cdot(x-z) = (x-z)\cdot r = 1\cdot(x-z) = (x-z)\cdot 1 = (x-z)$$

We know that the multiplicative indentity in ring is unique. Then $r = 1 = s$. Therefore R is unitary. ■

Let order of quasigroup be $|Q| = N$. The set $a(Q)$ of associative triples of $R_{r,s,t}$ is

$$a(Q) = \{(x, y, z) \in Q^3 : (r^2 - r)x - (s^2 - s)z = (s - r)t\}.$$

Since y is not involved in the defining relation, the associativity index $a(Q)$ equals $m \cdot N$ where m denotes the number of solutions (x_1, z_1) of the linear equation

$$(r^2 - r)x_1 - (s^2 - s)z_1 = (s - r)t.$$

In particular, if at least one of $r^2 - r$ and $s^2 - s$ belongs to R' then

$$(r^2 - r)x_1 = (s^2 - s)z_1 + (s - r)t.$$

Let ϕ be a mapping Q to Q and defined as

$$\phi(x_1) = (r^2 - r)x_1.$$

It is clear that ϕ is linear mapping Thus

$$\begin{aligned} ker(\phi) &= \{x_1 \in Q : \phi(x_1) = 0\}, \\ &= \{x_1 \in Q : (r^2 - r)x_1 = 0\}, \\ &= \{0\}. \end{aligned}$$

Hence $m = |Q| = N$ and $a(Q) = N^2$.

Theorem 4.2.2. *Suppose $\mathbb{F}_{2^n} = Q$ is the extension field of degree n over $\mathbb{F}_2$. Let π and π'*

be permutations on $\mathbb{F}_{2^n}$. *For* $t \in \mathbb{F}_{2^n}\backslash\{0\}$, *let* $F_{\pi,\pi',t} = (Q, *)$ *where*

$$x * y = \pi(x) + \pi'(y) + t,$$

for all $x, y \in Q$. *Then* $F_{\pi,\pi',t}$ *is a quasigroup.*

Proof. For any $a, b \in Q$, consider the equation

$$\begin{aligned} a * x &= b \\ \pi(a) + \pi'(x) + t &= b \\ \pi'(x) + \pi(a) + t + b &= 0 \\ \pi'(x) + c &= 0, \end{aligned}$$

where $\pi(a) + t + b = c \in Q$. Suppose x_1 and x_2 both are solutions to our equation. Then we have:

$$\pi'(x_1) + c = 0,$$

and

$$\pi'(x_2) + c = 0.$$

Adding the above equations, we get

$$\pi'(x_1) = \pi'(x_2) \Leftrightarrow x_1 = x_2.$$

Here we see that considered equation has unique solution. Obviously, $y * a = b$ also has unique solution. Therefore both equations have unique solution for every $a, b \in Q$. Thus $(Q, *)$ is a quasigroup. ∎

$F_{\pi,\pi',t}$ is a group if we choose $\pi = \pi' = I$, where I is identity mapping. We are interested to investigate the associativity index of $F_{\pi,\pi',t}$ for π and π'.

Theorem 4.2.3. *Let* π *and* π' *be permutations on* $\mathbb{F}_{2^n}$. *For* $t \in \mathbb{F}_{2^n}\backslash\{0\}$, $F_{\pi,\pi',t} = (Q, *)$ *defined as* $x * y = \pi(x) + \pi'(y) + t$, *for all* $x, y \in Q$. *Then the following statements are true:*

i) If $\pi'(x) = \pi(x) = x^{2^i}$, $x \in \mathbb{F}_{2^n}$, then $a(Q) = 2^e \cdot N^2$, where $e = gcd(i, n)$ and $N = 2^n$.

ii) If $\pi(x) = x$ or identity mapping and $\pi'(x) = x^{2^i}$ then $a(Q) = 2^e \cdot N^2$, where $e = gcd(i, n)$ and $N = 2^n$.

iii) If $\pi(x) = x^{2^i}$ and $\pi'(x) = x^{2^j}$ then $a(Q) = 2^e \cdot N^2$, where $e = gcd(i, n)$ and $N = 2^n$.

Proof. i) If $(x, y, z) \in A(Q)$, then

$$\pi(\pi(x) + \pi'(y) + t) + \pi'(\pi(y) + \pi'(z) + t) = \pi(x) + \pi'(z). \tag{4.2.2}$$

Since $\pi'(x) = \pi(x) = x^{2^i}$,

$$\pi(x^{2^i} + y^{2^i} + t) + \pi(y^{2^i} + z^{2^i} + t) = x^{2^i} + z^{2^i}$$

$$(x^{2^i} + y^{2^i} + t)^{2^i} + (y^{2^i} + z^{2^i} + t)^{2^i} = x^{2^i} + z^{2^i}$$

$$(x^{2^i} + z^{2^i})^{2^i} = x^{2^i} + z^{2^i}$$

$$(x^{2^i} + z^{2^i})^{2^i - 1} = 1^{2^i - 1}$$

it follows that

$$\pi(x) + \pi(z) \in G \backslash \{0\},$$

where G is the subfield of $\mathbb{F}_{2^n}$ of order 2^e and $e = gcd(i, n)$. Hence given $\pi(x)$ in $\mathbb{F}_{2^n}$ the set of all possible values for $\pi(z)$ is $\pi(x) + G$ of cardinality 2^e. Therefore, $a(Q) = 2^e \cdot N^2$ where $N = 2^n$.

ii) Since π is identity and $\pi'(x) = x^{2^i}$, by Equation (4.2.2)

$$\pi(x + y^{2^i} + t) + \pi'(y + z^{2^i} + t) = x + z^{2^i}$$

$$x + y^{2^i} + t + (y + z^{2^i} + t)^{2^i} = x + z^{2^i}$$

$$y^{2^i} + (y + z^{2^i} + t)^{2^i} + t = z^{2^i}$$

$$(z^{2^i} + z)^{2^i} = t^{2^i} + t$$

$$z^{2^i} + z = (t^{2^i} + t)^{2^{n-i}}.$$

It is clear that

$$z^{2^i} + z = v,$$

where $v = (t^{2^i} + t)^{2^{n-i}} = t + t^{2^{n-i}}$ has always a particular solution.
Now $z^{2^i} + z = 0$ has kernel $\mathbb{F}_{2^e}$ where $e = gcd(n, i)$. So for all values of t the equation

$$z^{2^i} + z = v,$$

has exactly 2^e many solutions. Therefore, $a(Q) = 2^e \cdot N^2$ where $N = 2^n$.

iii) Since $\pi(x) = x^{2^i}$ and $\pi'(x) = x^{2^j}$, by Equation (4.2.2)

$$(x^{2^i} + x)^{2^i} + (z^{2^j} + z)^{2^j} = t^{2^i} + t^{2^j}.$$

If the above equation is consistent in $\mathbb{F}_{2^n}$. Since this equation is independent of y. Then $a(Q)$ equals $m \cdot n \cdot N$ where m and n are the number of choices for x and z in $\mathbb{F}_{2^n}$ respectively. If z is fixed in $\mathbb{F}_{2^n}$. Then for any t in $\mathbb{F}_{2^n} \backslash \{0\}$, we get

$$\begin{aligned}(x^{2^i} + x)^{2^i} &= (z^{2^j} + z)^{2^j} + t^{2^i} + t^{2^j} \\ (x^{2^i} + x)^{2^i} &= v \\ x^{2^i} + x &= v^{2^{n-i}},\end{aligned}$$

where $v = (z^{2^j} + z)^{2^j} + t^{2^i} + t^{2^j}$ has always a particular solution.
Now $x^{2^i} + x = 0$ has kernel $\mathbb{F}_{2^e}$ where $e = gcd(n, i)$. So for all values of t the equation

$$z^{2^i} + z = v^{2^{n-i}},$$

has exactly 2^e many solutions. Therefore, $a(Q) = 2^e \cdot N^2$ where $N = 2^n$. ■

Similarly we do all cases for affine permutations, i.e., $\pi(x) = x^{2^i} + c$ where c is constant in $\mathbb{F}_{2^n}$ and we got the same associativity index for all cases.

Lemma 4.2.4. *If we choose $\pi(x) = x^{2^i} + x^{2^j} + c$ is special type of affine permutations over $\mathbb{F}_{2^n}$, where c is constant and $\pi'(x) = x$, i.e., identity mapping. Then $a(Q) = N^2$, where $N = 2^n$.*

Proof. If $(x, y, z) \in A(Q)$, then

$$\pi(\pi(x) + \pi'(y) + t) + \pi'(\pi(y) + \pi'(z) + t) = \pi(x) + \pi'(z).$$

Since $\pi(x) = \pi'(x) = x^{2^i} + x^{2^j} + c$,

$$\pi(x^{2^i} + x^{2^j} + c + y + t) + \pi'(y^{2^i} + y^{2^j} + c + z + t) = x^{2^i} + x^{2^j} + c + z$$

$$(x^{2^i} + x^{2^j} + c + y + t)^{2^i} + (x^{2^i} + x^{2^j} + c + y + t)^{2^j} + c + y^{2^i} + y^{2^j} + c + z + t = x^{2^i} + x^{2^j} + c + z$$

$$(x^{2^i} + x^{2^j})^{2^i} + (x^{2^i} + x^{2^j})^{2^j} + x^{2^i} + x^{2^j} = t^{2^i} + t^{2^j} + t + c^{2^i} + c^{2^j} + c$$

$$(x^{2^i} + x)^{2^i} + (x^{2^i} + x)^{2^j} = t^{2^i} + t^{2^j} + t + c^{2^i} + c^{2^j} + c.$$

When y and z are chosen independently in $\mathbb{F}_{2^n}$, then above equation has uniuqe solution. Therefore, $a(Q) = N^2$ where $N = 2^n$. ∎

Lemma 4.2.5. *Suppose π and π' are special type of affine permutations on $\mathbb{F}_{2^n}$. Let $\pi'(x) = \pi(x) = x^{2^i} + x^{2^j} + c$, where $c \in \mathbb{F}_{2^n}$, be the permutations on $\mathbb{F}_{2^n}$. Then $a(Q)$ is equal to the size of the set*

$$\{(x, y, z) \in A(Q); (x^{2^i} + x)^{2^i} + (x^{2^j} + x)^{2^j} + (z^{2^i} + z)^{2^i} + (z^{2^j} + z)^{2^j} = 0\}$$

if the above equation is consistent in $\mathbb{F}_{2^n}$.

Proof. If $(x, y, z) \in A(Q)$, then

$$\pi(\pi(x) + \pi'(y) + t) + \pi'(\pi(y) + \pi'(z) + t) = \pi(x) + \pi'(z).$$

Since $\pi(x) = \pi'(x) = x^{2^i} + x^{2^j} + c$,

$$\pi(x^{2^i} + x^{2^j} + c + y^{2^i} + y^{2^j} + c + t) + \pi'(y^{2^i} + y^{2^j} + c + z^{2^i} + z^{2^j} + c + t) = x^{2^i} + x^{2^j} + c + z^{2^i} + z^{2^j} + c$$

$$\pi(x^{2^i} + x^{2^j} + y^{2^i} + y^{2^j} + t) + \pi'(y^{2^i} + y^{2^j} + z^{2^i} + z^{2^j} + t) = x^{2^i} + x^{2^j} + z^{2^i} + z^{2^j}$$

$$(x^{2^i}+x^{2^j}+y^{2^i}+y^{2^j}+t)^{2^i}+(x^{2^i}+x^{2^j}+y^{2^i}+y^{2^j}+t)^{2^j}+c+(y^{2^i}+y^{2^j}+z^{2^i}+z^{2^j}+t)^{2^i}$$

$$+(y^{2^i}+y^{2^j}+z^{2^i}+z^{2^j}+t)^{2^j}+c=x^{2^i}+x^{2^j}+z^{2^i}+z^{2^j}$$

$$(x^{2^i}+x^{2^j}+y^{2^i}+y^{2^j}+t)^{2^i}+(x^{2^i}+x^{2^j}+y^{2^i}+y^{2^j}+t)^{2^j}+(y^{2^i}+y^{2^j}+z^{2^i}+z^{2^j}+t)^{2^i}$$

$$+(y^{2^i}+y^{2^j}+z^{2^i}+z^{2^j}+t)^{2^j}=x^{2^i}+x^{2^j}+z^{2^i}+z^{2^j}$$

$$(x^{2^i})^{2^i}+(y^{2^i})^{2^i}+(x^{2^j})^{2^j}+(y^{2^j})^{2^j}+(y^{2^i})^{2^i}+(z^{2^i})^{2^i}+(y^{2^j})^{2^j}+(z^{2^j})^{2^j}=x^{2^i}+x^{2^j}+z^{2^i}+z^{2^j}$$

$$(x^{2^i})^{2^i}+(x^{2^j})^{2^j}+(z^{2^i})^{2^i}+(z^{2^j})^{2^j}=x^{2^i}+x^{2^j}+z^{2^i}+z^{2^j}$$

$$(x^{2^i}+x)^{2^i}+(x^{2^j}+x)^{2^j}+(z^{2^i}+z)^{2^i}+(z^{2^j}+z)^{2^j}=0.$$

If the above equation is consistent and say m is the number of solutions for above equation in $\mathbb{F}_{2^n}$. Then $a(Q)=m\cdot N$. ∎

Since the above equation is independent of y. Then $a(Q)$ equals $m\cdot N$ where m is the number of solutions for above equation in $\mathbb{F}_{2^n}$. Using SageMath for calculation, we calculate for individual n and see that the solutions of this equation have very peculiar behavior. Then the value of m for different n as follows:

$n=3$, *either* $2\cdot N$ *or* $2^n\cdot N$,

$n=4$, *either* $2\cdot N$ *or* $4\cdot N$,

$n=5$, *exactly* $2\cdot N$,

$n=6$, *either* $2\cdot N, 4\cdot N, 8\cdot N, 8\cdot 2\cdot N$ *or* $8\cdot 2^3\cdot N$,

$n=7$, *either* $2\cdot N$ *or* $8\cdot 2\cdot N$,

$n=8$, *either* $2\cdot N, 4\cdot N$ *or* $8\cdot 2\cdot N$,

$n=9$, *either* $2\cdot N$ *or* $8\cdot N$,

$n=10$, *either* $2\cdot N, 4\cdot N$ *or* $8\cdot 2^2\cdot N$,

$n=11$, *exactly* $2\cdot N$,

and so on.

Theorem 4.2.6. *Suppose* π *and* π' *are the same quadratic permutations on* $\mathbb{F}_{2^n}$. $\pi(x)=\pi'(x)=x^{2^i+1}$ *for all* $x\in\mathbb{F}_{2^n}$. *Then the maximum number of associative triples for* $F_{\pi,\pi',t}$

is $2^e \cdot N^2$ *where* $e = gcd(i, n)$ *and* $N = 2^n$.

Proof. If $(x, y, z) \in A(Q)$, then

$$\pi(\pi(x) + \pi'(y) + t) + \pi'(\pi(y) + \pi'(z) + t) = \pi(x) + \pi'(z).$$

Since $\pi(x) = \pi'(x) = x^{2^i+1}$,

$$\pi(x^{2^i+1} + y^{2^i+1} + t) + \pi(y^{2^i+1} + z^{2^i+1} + t) = x^{2^i+1} + z^{2^i+1}$$

$$(x^{2^i+1} + y^{2^i+1} + t)^{2^i+1} + (y^{2^i+1} + z^{2^i+1} + t)^{2^i+1} = x^{2^i+1} + z^{2^i+1}$$

$$(x^{2^i+1} + y^{2^i+1} + t)(x^{2^i+1} + y^{2^i+1} + t)^{2^i} + (y^{2^i+1} + z^{2^i+1} + t)(y^{2^i+1} + z^{2^i+1} + t)^{2^i} = x^{2^i+1} + z^{2^i+1}$$

$$(x^{2^i+1})x^{2^i(2^i+1)} + (y^{2^i+1})x^{2^i(2^i+1)} + (t)x^{2^i(2^i+1)} + (x^{2^i+1})y^{2^i(2^i+1)} + (y^{2^i+1})y^{2^i(2^i+1)} + (t)y^{2^i(2^i+1)}$$

$$+(x^{2^i+1})t^{2^i} + (y^{2^i+1})t^{2^i} + t^{2^i+1} + (y^{2^i+1})y^{2^i(2^i+1)} + (z^{2^i+1})y^{2^i(2^i+1)} + (t)y^{2^i(2^i+1)} + (y^{2^i+1})z^{2^i(2^i+1)}$$

$$+(z^{2^i+1})z^{2^i(2^i+1)} + (t)z^{2^i(2^i+1)} + (y^{2^i+1})t^{2^i} + (z^{2^i+1})t^{2^i} + t^{2^i+1} = x^{2^i+1} + z^{2^i+1}$$

$$(x^{2^i+1})x^{2^i(2^i+1)} + (y^{2^i+1})x^{2^i(2^i+1)} + (t)x^{2^i(2^i+1)} + (x^{2^i+1})y^{2^i(2^i+1)} + (x^{2^i+1})t^{2^i} + (z^{2^i+1})y^{2^i(2^i+1)}$$

$$+(y^{2^i+1})z^{2^i(2^i+1)} + (z^{2^i+1})z^{2^i(2^i+1)} + (t)z^{2^i(2^i+1)} + (z^{2^i+1})t^{2^i} = x^{2^i+1} + z^{2^i+1}$$

$$(x^{2^i+1}+y^{2^i+1}+t)x^{2^i(2^i+1)}+(y^{2^i+1}+z^{2^i+1}+t)z^{2^i(2^i+1)}+(x^{2^i+1})y^{2^i(2^i+1)}+(x^{2^i+1})t^{2^i}+(z^{2^i+1})y^{2^i(2^i+1)}$$

$$+(z^{2^i+1})t^{2^i} = x^{2^i+1} + z^{2^i+1}$$

$$(x^{2^i+1}+y^{2^i+1}+t)x^{2^i(2^i+1)}+(y^{2^i+1}+z^{2^i+1}+t)z^{2^i(2^i+1)}+x^{2^i+1}(y^{2^i(2^i+1)}+t^{2^i}+1)+z^{2^i+1}(y^{2^i(2^i+1)}$$

$$+t^{2^i} + 1) = 0$$

$$(x^{2^i+1} + y^{2^i+1} + t)x^{2^i(2^i+1)} + (y^{2^i+1} + z^{2^i+1} + t)z^{2^i(2^i+1)} + (x^{2^i+1} + z^{2^i+1})(y^{2^i(2^i+1)} + t^{2^i} + 1) = 0.$$

If $x = z$ fixed in $\mathbb{F}_{2^n}$ then we get exactly N^2 solutions.

Suppose $x \neq z$ is fixed in $\mathbb{F}_{2^n}$ and let $x^{2^i+1} + z^{2^i+1} = A$ (say) and $x^{2^i+1} + z^{2^i+1} + x^{2^i+1} \cdot x^{2^i(2^i+1)} + z^{2^i+1} \cdot z^{2^i(2^i+1)} = B$ (say) in $\mathbb{F}_{2^n}$. Then

$$(y^{2^i+1} + t)(x^{2^i+1} + z^{2^i+1})^{2^i} + (y^{2^i+1} + t)^{2^i}(x^{2^i+1} + z^{2^i+1})$$

$$= x^{2^i+1} + z^{2^i+1} + x^{2^i+1} \cdot x^{2^i(2^i+1)} + z^{2^i+1} \cdot z^{2^i(2^i+1)},$$

or

$$(y^{2^i+1} + t)(A)^{2^i} + (y^{2^i+1} + t)^{2^i}(A) = B. \tag{4.2.3}$$

If $B = 0$ then

$$(y^{2^i+1} + t)(A)^{2^i} + (y^{2^i+1} + t)^{2^i}(A) = 0,$$

or equivalently,

$$(\pi(y) + t)^{2^i-1} = A^{2^i-1}$$

or,

$$(\pi'(y) + t)^{2^i-1} = A^{2^i-1}$$

it follows that

$$\pi(y) + t \in A(G\backslash\{0\})$$

or

$$\pi(y) \in A(G\backslash\{0\}).$$

From above equation we get exactly 2^e many value for $\pi(y)$, where G is the subfield of $\mathbb{F}_{2^n}$ of order 2^e and $e = gcd(i, n)$. Thus the number of choices for $\pi(y)$ is at most 2^e that satisfy the homogeneous part of Equation (4.2.3) for fixed A in $\mathbb{F}_{2^n}$.

If $B \neq 0$, the solutions of Equation (4.2.3) is either zero or equal to same number of solutions of homogeneous part. Therefore we have at most 2^e solutions of Equation (4.2.3) for any choice of B in $\mathbb{F}_{2^n}$. Therefore, $a(Q) = 2^e \cdot N^2$ where $N = 2^n$. ∎

Theorem 4.2.7. *If we choose π' is identity mapping and π is a quadratic permutation on $\mathbb{F}_{2^n}$. $\pi(x) = x^{2^i+1}$ for all $x \in \mathbb{F}_{2^n}$. Then the maximum number of associative triples for $F_{\pi,\pi',t}$ is $2^e \cdot N^2$ where $e = gcd(i, n)$ and $N = 2^n$.*

Proof. If $(x, y, z) \in A(Q)$, then

$$\pi(\pi(x) + \pi'(y) + t) + \pi'(\pi(y) + \pi'(z) + t) = \pi(x) + \pi'(z).$$

Since $\pi'(x) = x$ and $\pi(x) = x^{2^i+1}$,

$$\pi(x^{2^i+1} + y + t) + \pi'(y^{2^i+1} + z + t) = x^{2^i+1} + z$$

$$(x^{2^i+1}+y+t)^{2^i+1}+y^{2^i+1}+z+t=x^{2^i+1}+z$$

$$(x^{2^i+1}+y+t)^{2^i+1}+y^{2^i+1}+t=x^{2^i+1}.$$

Here we get the associativity index $a(Q)=m\cdot N$, where m is the number of solutions of the above equation. We further solve the equation

$$(x^{2^i+1}+y+t)(x^{2^i+1}+y+t)^{2^i}+y^{2^i+1}+t=x^{2^i+1}$$

$$(x^{2^i+1}+t+y)((x^{2^i+1}+t)^{2^i}+y^{2^i})+y^{2^i+1}+t=x^{2^i+1}$$

$$(x^{2^i+1}+t)^{2^i+1}+(x^{2^i+1}+t)^{2^i}y+(x^{2^i+1}+t)y^{2^i}+y^{2^i+1}+y^{2^i+1}+t=x^{2^i+1}$$

$$(x^{2^i+1}+t)^{2^i+1}+(x^{2^i+1}+t)^{2^i}y+(x^{2^i+1}+t)y^{2^i}+x^{2^i+1}+t=0$$

$$(x^{2^i+1}+t)^{2^i+1}+(x^{2^i+1}+t)^{2^i}y+(x^{2^i+1}+t)(y^{2^i}+1)=0.$$

For given t, we say x is fixed in $\mathbb{F}_{2^n}$ then $x^{2^i+1}+t=A$ (say). Then

$$A^{2^i+1}+A^{2^i}y+A(y^{2^i}+1)=0,$$

or equivalently,

$$Ay^{2^i}+A^{2^i}y+A(A^{2^i}+1)=0.$$

Let $B=A(A^{2^i}+1)$, then

$$Ay^{2^i}+A^{2^i}y+B=0. \tag{4.2.4}$$

If $B=0$, then

$$Ay^{2^i}+A^{2^i}y=0$$

or equivalently,

$$y^{2^i-1}=A^{2^i-1}$$

it follows that

$$y\in A(G\backslash\{0\}).$$

From above equation we get exactly 2^e many value for y, where G is the subfield of $\mathbb{F}_{2^n}$ of order 2^e and $e=gcd(i,n)$. Thus the number of choices for y is at most 2^e that satisfy the

homogeneous part of Equation (4.2.4) for fixed A in $\mathbb{F}_{2^n}$.

If $B \neq 0$, the solutions of Equation (4.2.4) is either zero or equal to same number of solutions of homogeneous part. Therefore we have at most 2^e solutions of Equation (4.2.4) for any choice of B in $\mathbb{F}_{2^n}$. Hence we get the associativity index $a(Q) = 2^e \cdot N \cdot N$. Therefore, $a(Q) = 2^e \cdot N^2$ where $N = 2^n$. ∎

Similarly we do for $\pi(x) = x^{2^i+1}$ and $\pi'(x) = x^{2^j+1}$ in $\mathbb{F}_{2^n}$ and we get quadratic equation in y

$$(z^{2^j+1}+t)^{2^j}y^{2^i+1} + (y^{2^i+1})^{2^j}y^{2^i+1} + (x^{2^i+1}+t)^{2^i}y^{2^j+1} + (y^{2^j+1})^{2^i}y^{2^j+1} + (x^{2^i+1}+t)(y^{2^j+1})^{2^i}$$
$$+ (z^{2^j+1}+t)(y^{2^i+1})^{2^j} = x^{2^i+1} + z^{2^j+1} + (x^{2^i+1}+t)^{2^i+1} + (z^{2^j+1}+t)^{2^j+1}.$$

Using SageMath for calculation, we get exactly N^3 solutions of the above equation. Therefore the number of associative triples is N^3.

Now we investigate the associative index by using complete mapping polynomials on $\mathbb{F}_{2^n}$ that constitute a special class of permutation polynomials [92] [96].

Lemma 4.2.8. *If we choose π is linear complete mapping permutation and π' is any permutation then we get associative index exactly N^2, where $N = 2^n$.*

Proof. By Equation (4.2.2)

$$\begin{aligned}
\pi(\pi(x)+\pi'(y)+t)+\pi'(z) &= \pi(x)+\pi'(\pi(y)+\pi'(z)+t)\\
\pi(\pi(x))+\pi(\pi'(y))+\pi(t)+\pi'(z) &= \pi(x)+\pi'(\pi(y)+\pi'(z)+t)\\
\pi(\pi(x))+\pi(x) &= \pi(\pi'(y))+\pi(t)+\pi(\pi'(z))+\pi'(\pi(y)+\pi'(z)+t)\\
(\pi+I)\pi(x) &= \pi(\pi'(y))+\pi(t)+\pi(\pi'(z))+\pi'(\pi(y)+\pi'(z)+t)\\
\pi(x) &= (\pi+I)^{-1}(\pi(\pi'(y))+\pi(t)+\pi(\pi'(z))+\pi'(\pi(y)+\pi'(z)\\
&\quad +t))\\
x &= \pi^{-1}\{(\pi+I)^{-1}(\pi(\pi'(y))+\pi(t)+\pi(\pi'(z))+\pi'(\pi(y)+\\
&\quad \pi'(z)+t))\}.
\end{aligned}$$

Then y and z are free to choose in $\mathbb{F}_{2^n}$. Hence we get exactly N^2 number of solution of the above equation. ∎

In the following table we list the values of $a(Q)$ for different choices of π and π' over $\mathbb{F}_{2^n}$.

$\pi(x)$	$\pi'(x)$	$a(Q)$
x^{2^i}	x^{2^i}	$2^e \cdot N^2$
Identity	x^{2^i}	$2^e \cdot N^2$
x^{2^i}	x^{2^j}	$2^e \cdot N^2$
$x^{2^i} + c$	$x^{2^i} + c$	$2^e \cdot N^2$
Identity	$x^{2^i} + c$	$2^e \cdot N^2$
$x^{2^i} + c$	$x^{2^j} + c$	$2^e \cdot N^2$
$x^{2^i} + x^{2^j} + c$	$x^{2^i} + x^{2^j} + c$	$\leq 2 \cdot N^2$
$x^{2^i} + x^{2^j} + c$	Identity	N^2
x^{2^i+1}	x^{2^i+1}	$2^e \cdot N^2$
x^{2^i+1}	Identity	$2^e \cdot N^2$
x^{2^i+1}	x^{2^j+1}	N^3
Linear complete mapping	Any permutation	N^2

where $e = gcd(i, n)$ and $N = 2^n$. When $e = 1$, we get the best known lower bound for associative triples [64].

4.3 $F_{\pi,\pi',t}$ - quasigroups as vectorial Boolean functions

We already have explained $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$ are vector isomorphism over $\mathbb{F}_2$. Therefore we can be considered $F_{\pi,\pi',t} : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ as vectorial Boolean function and defined by

$$F_{\pi,\pi',t}(x, y) = \pi(x) + \pi'(y) + t,$$

where $x, y \in \mathbb{F}_{2^n}$ and $t \in \mathbb{F}_{2^n} \backslash \{0\}$. Now we can check the cryptographic characteristics of obtained vectorial Boolean function.

4.4 Walsh-Hadamard transform and nonlinearity of $F_{\pi,\pi',t}$

Besides the coordinates, all linear combinations of the coordinates are usually involved for determining the cryptographic properties of a vectorial Boolean function, in the sense of

the following definition.

The Walsh-Hadamard transform of $F_{\pi,\pi',t}$ is the mapping $W_{F_{\pi,\pi',t}} : (\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}) \times \mathbb{F}_{2^n} \longrightarrow \mathbb{R}$, defined as

$$W_{F_{\pi,\pi',t}}((u_1, u_2), v) = \sum_{(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}} (-1)^{tr_1^n(vF_{\pi,\pi',t})+tr_1^n(u_1x)+tr_1^n(u_2y)} \tag{4.4.1}$$

Moreover, the linearity [16] of $F_{\pi,\pi',t}$ is

$$\mathcal{L}(F_{\pi,\pi',t}) = \max_{v\in\mathbb{F}_{2^n}^*} \mathcal{L}((F_{\pi,\pi',t})_v) = \max_{u_1,u_2\in\mathbb{F}_{2^n},v\in\mathbb{F}_{2^n}^*} \mid W_{F_{\pi,\pi',t}}((u_1, u_2), v) \mid \tag{4.4.2}$$

and the nonlinearity [19] of $F_{\pi,\pi',t}$ is

$$nl(F_{\pi,\pi',t}) = 2^{n-1} - (1/2)(\mathcal{L}(F_{\pi,\pi',t})),$$

or

$$nl(F_{\pi,\pi',t}) = 2^{n-1} - (1/2) \max_{u_1,u_2\in\mathbb{F}_{2^n},v\in\mathbb{F}_{2^n}^*} \mid W_{F_{\pi,\pi',t}}((u_1, u_2), v) \mid .$$

From Equations (4.4.1) and (4.4.2) we get

$$\begin{aligned}
W_{F_{\pi,\pi',t}}((u_1, u_2), v) &= \sum_{(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}} (-1)^{tr_1^n(vF_{\pi,\pi',t})+tr_1^n(u_1x)+tr_1^n(u_2y)} \\
&= \sum_{(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}} (-1)^{tr_1^n(v(\pi(x)+\pi'(y)+t))+tr_1^n(u_1x)+tr_1^n(u_2y)} \\
&= \sum_{(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}} (-1)^{tr_1^n(v\pi(x))+tr_1^n(v\pi'(y))+tr_1^n(vt)+tr_1^n(u_1x)+tr_1^n(u_2y)} \\
&= \sum_{(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}} (-1)^{tr_1^n(v\pi(x))+tr_1^n(u_1x)+tr_1^n(v\pi'(y))+tr_1^n(u_2y)+tr_1^n(vt)} \\
&= (-1)^{tr_1^n(vt)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(v\pi(x))+tr_1^n(u_1x)} \sum_{y\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(v\pi'(y))+tr_1^n(u_2y)} \\
&= (-1)^{tr_1^n(vt)} W_\pi(u_1, v) W_{\pi'}(u_2, v),
\end{aligned}$$

or

$$W_{F_{\pi,\pi',t}}((u_1,u_2),v) = (-1)^{tr_1^n(vt)} W_\pi(u_1,v) W_{\pi'}(u_2,v).$$

The linearity of $F_{\pi,\pi',t}$ is given by

$$\mathcal{L}(F_{\pi,\pi',t}) = \max_{u_1,u_2 \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^n}^*} \mid (-1)^{tr_1^n(vt)} W_\pi(u_1,v) W_{\pi'}(u_2,v) \mid .$$

The nonlinearity of $F_{\pi,\pi',t}$ is given by

$$nl(F_{\pi,\pi',t}) = 2^{n-1} - (1/2) \max_{u_1,u_2 \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^n}^*} \mid (-1)^{tr_1^n(vt)} W_\pi(u_1,v) W_{\pi'}(u_2,v) \mid .$$

$\mathcal{F}$ is bent, almost bent and semi-bent if and only if all of its component functions, i.e., $tr_1^m(\lambda \mathcal{F}(x))$ for any $\lambda \in \mathbb{F}_{2^m}$, are bent, almost bent and semi-bent respectively.

- Bent Functions: Only when n is even

  $$W_{\mathcal{F}_\lambda}(u,v) = \pm 2^{n/2} \text{ for any } \lambda \in \mathbb{F}_{2^m} \text{ and } u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^m}^*.$$

- Almost bent Functions (AB): Only when n is odd

  $$W_{\mathcal{F}_\lambda}(u,v) \in \{0, \pm 2^{(n+1)/2}\} \text{ for any } \lambda \in \mathbb{F}_{2^m} \text{ and } u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^m}^*.$$

- Semi-bent Functions:

  When n is even

  $$W_{\mathcal{F}_\lambda}(u,v) \in \{0, \pm 2^{(n+2)/2}\} \text{ for any } \lambda \in \mathbb{F}_{2^m} \text{ and } u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^m}^*.$$

  When n is odd

  $$W_{\mathcal{F}_\lambda}(u,v) \in \{0, \pm 2^{(n+1)/2}\} \text{ for any } \lambda \in \mathbb{F}_{2^m} \text{ and } u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^m}^*.$$

For more details we refer to [23] [58] [63]. Let the component functions of $F_{\pi,\pi',t}$ be denoted by $F^\lambda_{\pi,\pi',t}$ for any $\lambda \in \mathbb{F}_{2^n}$. Then we get the relationship between W_{π_λ}, $W_{\pi'_\lambda}$ and

$W_{F^\lambda_{\pi,\pi',t}}((u_1,u_2),v)$ for any $\lambda \in \mathbb{F}_{2^n}$ as follows:

W_{π_λ}	$W_{\pi'_\lambda}$	$W_{F^\lambda_{\pi,\pi',t}}((u_1,u_2),v)$	Property of $W_{F^\lambda_{\pi,\pi',t}}((u_1,u_2),v)$
Almost Bent	Almost Bent	$\{0, \pm 2^{(2n+2)/2}\}$	Can't say
Semi-bent (n even)	Semi-bent (n even)	$\{0, \pm 2^{(2n+4)/2}\}$	Can't say

This gives us information about the Walsh spectrum of $F_{\pi,\pi',t}$. Bent, almost bent and semi-bent functions are studied in cryptography because, besides having low Walsh spectrum which provides protection against fast correlation attacks [109] and linear cryptanalysis [106], they can possess desirable properties in addition to the propagation criterion and low additive autocorrelation, such as resiliency and high algebraic degree. On the cryptographic point of view, we choose π and π' either bent functions or semi-bent functions over $\mathbb{F}_{2^n}$.

4.5 Differential profile of $F_{\pi,\pi',t}$

The differential uniformity of $\pi, \pi' : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ is defined by

$$D_\pi(u_1,v_1) = \{x \in \mathbb{F}_{2^n} | \pi(x+u_1) + \pi(x) = v_1\} \tag{4.5.1}$$

$$\delta_1 = \max_{u_1 \neq 0, v_1} |D_\pi(u_1,v_1)| = \max_{u_1 \neq 0, v_1} |\{x \in \mathbb{F}_{2^n} | \pi(x+u_1) + \pi(x) = v_1\}|,$$

and

$$D_{\pi'}(u_2,v_2) = \{x \in \mathbb{F}_{2^n} | \pi'(x+u_2) + \pi'(x) = v_2\} \tag{4.5.2}$$

$$\delta_2 = \max_{u_2 \neq 0, v_2} |D_\pi(u_2,v_2)| = \max_{u_2 \neq 0, v_2} |\{x \in \mathbb{F}_{2^n} | \pi'(x+u_2) + \pi'(x) = v_2\}|.$$

Similarly Differential uniformity for $F_{\pi,\pi',t}$ is defined by

$$D_{F_{\pi,\pi',t}}((w_1,w_2),v) = \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | F_{\pi,\pi',t}((x,y)+(w_1,w_2)) + F_{\pi,\pi',t}(x,y) = v\} \tag{4.5.3}$$

and

$$\begin{aligned} \delta &= \max_{(w_1,w_2)\neq(0,0),v} |D_{F_{\pi,\pi',t}}((w_1,w_2),v)| \\ &= \max_{(w_1,w_2)\neq(0,0),v} |\{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | F_{\pi,\pi',t}((x,y)+(w_1,w_2)) + F_{\pi,\pi',t}(x,y) = v\}|. \end{aligned}$$

From Equation (4.5.3) we get

$$\begin{aligned} D_{F_{\pi,\pi',t}}((w_1,w_2),v) &= \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | F_{\pi,\pi',t}((x,y)+(w_1,w_2)) + F_{\pi,\pi',t}(x,y) = v\} \\ &= \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | \pi(x+w_1) + \pi'(y+w_2) + t + \pi(x) + \pi'(y) \\ &\quad + t = v\} \\ &= \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | \pi(x+w_1) + \pi'(y+w_2) + \pi(x) + \pi'(y) = v\} \\ &= \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | \pi(x+w_1) + \pi(x) + \pi'(y+w_2) + \pi'(y) = v\} \end{aligned}$$

$$D_{F_{\pi,\pi',t}}((w_1,w_2),v) = \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | \pi(x+w_1) + \pi(x) + \pi'(y+w_2) + \pi'(y) = v\}. \tag{4.5.4}$$

It is shown in [128] that for $n > m$ the minimum differential uniformity 2^{n-m} for $\mathcal{F} \in \mathcal{B}_{n,m}$ is reached if and only if $2m \leq n$ and n is even. Here we have $(2n, n)$ variables vectorial Boolean function, so, the possibility of achieving minimum bound is fair.

(APN) **Power Functions:**

More results on the APN property are known when we focus on the family of power functions, i.e., $F : x \to x^d$ over $\mathbb{F}_{2^n}$. For instance, if there is h which divides n and $d = k(2^h - 1) + 2^r$ for some k and r then F is not APN [28] [21]. Berger et al. [11] presented above result, indicated by Dobbertin [43], in a more general context.

Proposition 4.5.1. [11, Proposition 3] *Let r be a divisor of n and F be any function on $\mathbb{F}_{2^n}$. Assume that $F \in \mathbb{F}_{2^n}[x]$. If F satisfies for some $a \in \mathbb{F}_{2^r}$*

$$F(y) + F(y+a) = \beta, \ \beta \in \mathbb{F}_{2^r}$$

for some y such that $y \notin \mathbb{F}_{2^r}$ and $y^{2^r} + y + a \neq 0$, then F is not APN.
Consequently, if F is APN with $F(x) = x^d$, then $gcd(d, 2^n - 1) = 1$ for odd n and for even n, we get $gcd(d, 2^n - 1) = 3$.

For instance, $\pi(x) = x^3$ and $\pi'(x) = x^5$ over $\mathbb{F}_{2^3}$ both are APN permutations. Using the irreducible polynomial $\alpha^3 + \alpha + 1 = 0$, we have the following Difference Distribution Table:

Table 4.1: For $\pi(x) = x^3$ over $\mathbb{F}_{2^3}$

	0	α	α^2	α+1	$\alpha^2+\alpha$	$\alpha^2+\alpha$+1	α^2+1	1
0	-	-	-	-	-	-	-	-
α	-	$\{\alpha^2, \alpha^2+\alpha\}$	$\{\alpha^2+\alpha+1, \alpha^2+1\}$	$\{0, \alpha\}$	-	-	$\{\alpha+1, 1\}$	-
α^2	-	-	$\{\alpha, \alpha^2+\alpha\}$	-	$\{\alpha+1, \alpha^2+\alpha+1\}$	$\{\alpha^2+1, 1\}$	$\{0, \alpha^2\}$	-
$\alpha+1$	-	$\{\alpha, 1\}$	$\{0, \alpha+1\}$	-	-	$\{\alpha^2, \alpha^2+\alpha+1\}$	-	$\{\alpha^2+\alpha, \alpha^2+1\}$
$\alpha^2+\alpha$	-	$\{\alpha+1, \alpha^2+1\}$	-	$\{\alpha^2+\alpha+1, 1\}$	$\{\alpha, \alpha^2\}$	$\{0, \alpha^2+\alpha\}$	-	-
$\alpha^2+\alpha$+1	-	$\{0, \alpha^2+\alpha+1\}$	-	-	$\{\alpha^2+\alpha, 1\}$	-	$\{\alpha, \alpha^2+1\}$	$\{\alpha^2, \alpha+1\}$
α^2+1	-	-	$\{\alpha^2, 1\}$	$\{\alpha+1, \alpha^2+\alpha\}$	$\{0, \alpha^2+1\}$	-	-	$\{\alpha, \alpha^2+\alpha+1\}$
1	-	-	-	$\{\alpha^2, \alpha^2+1\}$	-	$\{\alpha, \alpha+1\}$	$\{\alpha^2+\alpha, \alpha^2+\alpha+1\}$	$\{0, 1\}$

Table 4.2: For $\pi'(x) = x^5$ over $\mathbb{F}_{2^3}$

	0	α	α^2	α+1	$\alpha^2+\alpha$	$\alpha^2+\alpha$+1	α^2+1	1
0	-	-	-	-	-	-	-	-
α	-	$\{\alpha^2+\alpha+1, \alpha^2+1\}$	-	$\{\alpha+1, 1\}$	$\{\alpha^2, \alpha^2+\alpha\}$	$\{0, \alpha\}$	-	-
α^2	-	$\{\alpha, \alpha^2+\alpha\}$	$\{\alpha+1, \alpha^2+\alpha+1\}$	$\{0, \alpha^2\}$	-	-	$\{\alpha^2+1, 1\}$	-
$\alpha+1$	-	$\{0, \alpha+1\}$	-	-	$\{\alpha, 1\}$	-	$\{\alpha^2, \alpha^2+\alpha+1\}$	$\{\alpha^2+\alpha, \alpha^2+1\}$
$\alpha^2+\alpha$	-	-	$\{\alpha, \alpha^2\}$	-	$\{\alpha+1, \alpha^2+1\}$	$\{\alpha^2+\alpha+1, 1\}$	$\{0, \alpha^2+\alpha\}$	-
$\alpha^2+\alpha$+1	-	-	$\{\alpha^2+\alpha, 1\}$	$\{\alpha, \alpha^2+1\}$	$\{0, \alpha^2+\alpha+1\}$	-	-	$\{\alpha^2, \alpha+1\}$
α^2+1	-	$\{\alpha^2, 1\}$	$\{0, \alpha^2+1\}$	-	-	$\{\alpha+1, \alpha^2+\alpha\}$	-	$\{\alpha, \alpha^2+\alpha+1\}$
1	-	-	-	$\{\alpha^2+\alpha, \alpha^2+\alpha+1\}$	-	$\{\alpha^2, \alpha^2+1\}$	$\{\alpha, \alpha+1\}$	$\{0, 1\}$

By Equations (4.5.1), (4.5.2) and (4.5.4) we get

$$D_{F_{\pi,\pi',t}}((u_1,u_2),v_1+v_2) = \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | \pi(x+u_1)+\pi(x)+\pi'(y+u_2)+ \pi'(y) = v_1+v_2\}. \tag{4.5.5}$$

With the help of Table 4.1 and Table 4.2,

- When $u_1 = \alpha, u_2 = \alpha, v_1 = \alpha$, and $v_2 = \alpha$, then

$$D_{F_{\pi,\pi',t}}((\alpha,\alpha),0) = \{(\alpha^2, \alpha^2+\alpha+1), (\alpha^2, \alpha^2+1), (\alpha^2+\alpha, \alpha^2+\alpha+1), (\alpha^2+\alpha, \alpha^2+1)\}.$$

- When $u_1 = \alpha, u_2 = \alpha, v_1 = \alpha$, and $v_2 = \alpha^2$, then

$$D_{F_{\pi,\pi',t}}((\alpha,\alpha),\alpha+\alpha^2) = \emptyset.$$

- When $u_1 = \alpha, u_2 = \alpha, v_1 = \alpha^2 + \alpha$, and $v_2 = \alpha$, then

$$D_{F_{\pi,\pi',t}}((\alpha,\alpha),\alpha^2) = \emptyset.$$

- When $u_1 = \alpha, u_2 = \alpha^2, v_1 = \alpha$, and $v_2 = \alpha^2$, then

$$D_{F_{\pi,\pi',t}}((\alpha,\alpha^2),\alpha^2{+}\alpha) = \{(\alpha^2,\alpha{+}1),(\alpha^2,\alpha^2{+}\alpha{+}1),(\alpha^2{+}\alpha,\alpha{+}1),(\alpha^2{+}\alpha,\alpha^2{+}\alpha{+}1)\}.$$

Similarly we can find for the other values of u_1, u_2, v_1 and v_2. Here we see that 4 is the maximum value in Difference Distribution Table of $F_{\pi,\pi',t}$ when π and π' both are unequal APN permutations.

If $\pi(x) = \pi'(x) = x^3$ over $\mathbb{F}_{2^3}$ both are equal APN permutations. Then from Equation (4.5.5)

$$D_{F_{\pi,\pi',t}}((u_1,u_2),v_1+v_2) = \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | \pi(x+u_1) + \pi(x) + \pi(y+u_2) + \pi(y) = v_1 + v_2\}.$$

With the help of Table 4.1,

- When $u_1 = \alpha, u_2 = \alpha, v_1 = \alpha$, and $v_2 = \alpha$, then

$$D_{F_{\pi,\pi',t}}((\alpha,\alpha),0) = \{(\alpha^2,\alpha^2),(\alpha^2,\alpha^2+\alpha),(\alpha^2+\alpha,\alpha^2),(\alpha^2+\alpha,\alpha^2+\alpha)\}.$$

- When $u_1 = \alpha, u_2 = \alpha, v_1 = \alpha$, and $v_2 = \alpha^2 + \alpha$, then

$$D_{F_{\pi,\pi',t}}((\alpha,\alpha),\alpha^2) = \{(\alpha^2,\alpha^2{+}\alpha{+}1),(\alpha^2,\alpha^2{+}1),(\alpha^2{+}\alpha,\alpha^2{+}\alpha{+}1),(\alpha^2{+}\alpha,\alpha^2{+}1)\}.$$

- When $u_1 = \alpha, u_2 = \alpha^2, v_1 = \alpha$, and $v_2 = \alpha$, then

$$D_{F_{\pi,\pi',t}}((\alpha,\alpha^2),0) = \emptyset.$$

- When $u_1 = \alpha, u_2 = \alpha^2, v_1 = \alpha$, and $v_2 = \alpha^2$, then

$$D_{F_{\pi,\pi',t}}((\alpha,\alpha),\alpha^2) = \{(\alpha^2,\alpha),(\alpha^2,\alpha^2+\alpha),(\alpha^2+\alpha,\alpha),(\alpha^2+\alpha,\alpha^2+\alpha)\}.$$

Similarly we can find for the other values of u_1, u_2, v_1 and v_2. Again 4 is the maximum value in Difference Distribution Table of $F_{\pi,\pi',t}$ when π and π' both are equal APN permutations.

If we choose π and π' both with either equal or unequal differentially 4-uniform then we get $4 \cdot 4$ is the maximum value in Difference Distribution Table of $F_{\pi,\pi',t}$. Hence for both π and π' differentially δ_1-uniform we get $\delta_1 \cdot \delta_1$ is the maximum value in Difference Distribution Table of $F_{\pi,\pi',t}$.

Theorem 4.5.2. *Let π be differentially δ_1-uniform and π' be differentially δ_2-uniform. Then $F_{\pi,\pi',t}$ is differentially $(\delta_1 \cdot \delta_2)$-uniform.*

Proof. We have

$$D_{F_{\pi,\pi',t}}((w_1,w_2),v) = \{(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} | \pi(x+w_1) + \pi(x) + \pi'(y+w_2) + \pi'(y) = v\}.$$

Let π be differentially δ_1-uniform then for particular w_1 and v_1 in $\mathbb{F}_{2^n}$ we get

$$D_{F_{\pi,\pi',t}}((w_1,w_2),v+v_1) = \{(x_1,y),(x_2,y),\ldots,(x_{\delta_1},y), y \in \mathbb{F}_{2^n} | \pi'(y+w_2) + \pi'(y) = v+v_1\}. \tag{4.5.6}$$

- When v can be split into $v_1 + v_2$, then Equation (4.5.6)

$$D_{F_{\pi,\pi',t}}((w_1,w_2),v_2) = \{(x_1,y),(x_2,y),\ldots,(x_{\delta_1},y), y \in \mathbb{F}_{2^n} | \pi'(y+w_2) + \pi'(y) = v_2\}$$

$$\begin{aligned} i.e., \quad D_{F_{\pi,\pi',t}}((w_1,w_2),v_2) = &\{(x_1,y_1),(x_1,y_2),\ldots,(x_1,y_{\delta_2}),(x_2,y_1),(x_2,y_2),\ldots, \\ &(x_2,y_{\delta_2}),\ldots,(x_{\delta_1},y_1),(x_{\delta_1},y_2),\ldots,(x_{\delta_1},y_{\delta_2})\}. \end{aligned}$$

- When $v = v_1$, then Equation (4.5.6)

$$D_{F_{\pi,\pi',t}}((w_1,w_2),0) = \{(x_1,y),(x_2,y),\ldots,(x_{\delta_1},y), y \in \mathbb{F}_{2^n} | \pi'(y+w_2) + \pi'(y) = 0\}$$

$$i.e., \quad D_{F_{\pi,\pi',t}}((w_1, w_2), v_2) = \emptyset.$$

- When v can be split into $v_1 + \beta$, where $\beta \in \mathbb{F}_{2^n}$, then Equation (4.5.6)

$$D_{F_{\pi,\pi',t}}((w_1, w_2), \beta) = \{(x_1, y), (x_2, y), \ldots, (x_{\delta_1}, y), y \in \mathbb{F}_{2^n} | \pi'(y + w_2) + \pi'(y) = \beta\}$$

$$i.e., \quad D_{F_{\pi,\pi',t}}((w_1, w_2), v_2) = \emptyset.$$

Therefore $F_{\pi,\pi',t}$ is differentially $(\delta_1 \cdot \delta_2)$-uniform. ■

APN functions [100] and differentially 4-uniform functions (inverse function) [168] are used in DES and AES cipher to resistance against differential cryptanalysis. When π and π' both are APN permuations then we get $F_{\pi,\pi',t}$ differentially 4-uniform.

Chapter 5

XS-circuits in Quasigroups

5.1 Introduction

A permutation π on $\mathbb{F}_{2^n}$ is said to be a complete mapping permutation if $\pi + I$ is also a permutation where I is the identity permutation on $\mathbb{F}_{2^n}$. Complete mapping permutations are used to construct quasigroups (equivalently, Latin squares) which in turn show promise of being applied to design hash functions and block ciphers. Construction of complete mapping permutations by using the Feistel structure has been proposed by Markovski and Mileva [104] which they used to construct large quasigroups. Complete mapping permutations have been extensively studied in [8, 34, 93, 123, 162]. Stănică et al. [158] used complete mapping permutations to construct a new class of bent-negabent functions.

Markovski and Mileva [104] proved that a Feistel function is a complete mapping permutation if the "inner" vectorial Boolean function is a permutation. Thus, they provide a way to construct complete mapping permutations from ordinary permutations. In this Chapter, we demonstrate that XS-circuits can be used to construct complete mapping permutations and under some very reasonable conditions it is possible to construct complete mapping permutations from any vectorial Boolean function. We also show how the question of counting the number of such complete mapping permutations is connected to counting the linear orthomorphisms over finite fields and counting the points on curves of intersections of certain bilinear forms over finite fields.

Later we construct $\mathcal{K}$-complete mapping permutation which can be used to define uniformly distributed sequences. We also find a recursive constrictions that extend a complete

mapping permutation of dimension r to a complete mapping permutation of dimension n, where $r \leq n$.

5.2 XS-circuits

The theory of XS-circuits as proposed by Agievich [2] is described in this section. Let $\mathbb{F}_2^n = \{(z_1, \ldots, z_n) : z_i \in \mathbb{F}_2, i \in [n]\}$ where $\mathbb{F}_2$ the prime field of characteristic 2 and $[n] = \{1, \ldots, n\}$. Let $a = (a_1, \ldots, a_n), c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n$ and $B = (b_{ij})_{n\times n}$, where $b_{ij} \in \mathbb{F}_2$, for all $i, j \in [n]$, be an $n \times n$ matrix over $\mathbb{F}_2$. Let $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be a vectorial Boolean function on $\mathbb{F}_2^m$. The output $y = (y_1, \ldots, y_n) \in (\mathbb{F}_2^m)^n$ of the XS-circuit $(a, B, c|S)$ for an input $x = (x_1, \ldots, x_n) \in (\mathbb{F}_2^m)^n$ is defined by

$$y = xB + S(xa^T)c, \tag{5.2.1}$$

where a^T is the transpose of the vector a. Since the entries of the vectors x and y are from the vector space $\mathbb{F}_2^m$ whereas the entries in a, c, B are from $\mathbb{F}_2$, for the sake of clarity we discuss the multiplications in details. The first term in the right-hand-side of Equation (5.2.1) is

$$\begin{aligned} xB &= (x_1, \ldots, x_n)(b_{ij})_{n\times n} \\ &= \Big(\sum_{i\in[n]} x_i b_{i1}, \ldots, \sum_{i\in[n]} x_i b_{in} \Big). \end{aligned}$$

The second term is

$$\begin{aligned} S(xa^T)c &= S(xa^T)(c_1, \ldots, c_n) \\ &= (S(xa^T)c_1, \ldots, S(xa^T)c_n). \end{aligned}$$

Thus, Equation (5.2.1) can be explicitly written as

$$\begin{aligned} (y_1, \ldots, y_n) &= \Big(\sum_{i\in[n]} x_i b_{i1}, \ldots, \sum_{i\in[n]} x_i b_{in}) + (S(xa^T)c_1, \ldots, S(xa^T)c_n \Big) \\ &= \Big(\sum_{i\in[n]} x_i b_{i1} + S(xa^T)c_1, \ldots, \sum_{i\in[n]} x_i b_{in} + S(xa^T)c_n \Big). \end{aligned}$$

It is to be noted carefully that $x_i, y_i, S(xa^T) \in \mathbb{F}_2^m$, whereas $a_i, c_i, b_{ij} \in \mathbb{F}_2$, for all $i \in [n]$.

Generalized XS-circuits

We can easily extend the model. Let $F = \mathbb{F}_2^m$ be a base field, $r \leq n$ and B, A, C be matrices over F of dimension $n \times n$, $n \times r$, $r \times n$ respectively. Let S be a mapping from F^r to F^r. The tuple $(A, B, C|S)$ determines the mapping $F^n \to F^n$:

$$x \mapsto y = xB + S(xA)C.$$

Comparing to the current model, we enrich S transferring its action from F to F^r and, correspondently, replace the vectors a, c by the matrices A, C. Due to the enrichment of S, we can use $m = 1$ (that is, make all matrices binary).

An $n \times 1$ matrix over $\mathbb{F}_2$ with all entries equal to zero is denoted by 0_n. The $n \times n$ identity matrix is denoted by I_n, its dimension is understood from the context.

5.3 A construction of a class of complete mapping permutations

Complete mapping permutations can be used to construct large quasigroups [104] as well as bent-negabent Boolean functions [158]. Feistel function is a special case of XS-circuits with $n = 2$, $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$, and

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and } a = c = (0, 1).$$

It is well known that Feistel function is a permutation irrespective of whether S is a bijective mapping or not. Markovski and Mileva [104] proved that if S is bijective then the above Feistel function is a complete mapping permutation. Thus Markovski and Mileva could associate a class of complete mapping permutations on $\mathbb{F}_2^{2m}$ to the class of permutations on $\mathbb{F}_2^m$, to which S belongs. Our question is to characterize XS-circuits which are complete mapping permutations for all functions $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$.

Theorem 5.3.1. *Suppose $x, y \in (\mathbb{F}_2^m)^n$, $a, c \in \mathbb{F}_2^n$, $B = (b_{ij})_{n \times n}$ where $b_{ij} \in \mathbb{F}_2$, and S is*

any function on $\mathbb{F}_2^m$. *Then*

$$y = xB + S(xa^T)c$$

is a complete mapping permutation if the following conditions are satisfied:

1. B *and* $B + I$ *both are invertible.*

2. *There exist* $a, c \in F_2^n \setminus \{0\}$ *such that*

$$cB^{-1}a^T = 0 \text{ and } c(B+I)^{-1}a^T = 0.$$

Proof. In order to be a complete mapping permutation both

$$y = xB + S(xa^T)c \tag{5.3.1}$$

and

$$y = x(B+I) + S(xa^T)c. \tag{5.3.2}$$

have to be invertible. Following arguments are due to Agievich [2] which we recall for completeness. Since B is invertible

$$\begin{aligned} & yB^{-1} = x + S(xa^T)cB^{-1} \\ i.e., \quad & yB^{-1}a^T = xa^T + S(xa^T)cB^{-1}a^T \\ i.e., \quad & xa^T = yB^{-1}a^T + S(xa^T)cB^{-1}a^T \\ i.e., \quad & xa^T = yB^{-1}a^T, \text{ since } cB^{-1}a^T = 0. \end{aligned}$$

Substituting $xa^T = yB^{-1}a^T$ above

$$\begin{aligned} & yB^{-1} = x + S(yB^{-1}a^T)cB^{-1} \\ i.e., \quad & x = yB^{-1} + S(yB^{-1}a^T)cB^{-1}. \end{aligned}$$

Therefore, Equation (5.3.1) is invertible, if B is invertible and $cB^{-1}a^T = 0$. Similarly, Equation (5.3.2) is invertible, if $B + I$ is invertible and $c(B+I)^{-1}a^T = 0$. ∎

Theorem 5.3.1 provides us a connection between any function on $\mathbb{F}_2^m$ to a complete

mapping permutation on $(\mathbb{F}_2^m)^n$.

Example 5.3.2. *Suppose*

$$B = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad B + I = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \text{ and } \quad a = (0, 1, 0), \quad c = (1, 1, 1).$$

It can be directly checked that

$$B^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad (B + I)^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

and

$$cB^{-1}a^T = 0, \quad c(B + I)^{-1}a^T = 0.$$

Thus, $y = xB + S(xa^T)c$ is a complete mapping permutation on $(\mathbb{F}_2^m)^3$, for any positive integer m and any function S on $\mathbb{F}_2^m$.

Theorem 5.3.3. *Suppose $x, y \in (\mathbb{F}_2^m)^n$, $a, c \in \mathbb{F}_2^n$, $B = (b_{ij})_{n\times n}$ where $b_{ij} \in \mathbb{F}_2$, and S is any bijective function on $\mathbb{F}_2^m$. Then*

$$y = xB + S(xa^T)c$$

is a complete mapping permutation if the following conditions are satisfied:

1. *The ranks of B and $B + I$ are n and $n - 1$, respectively.*
2. *There exist $a, c, \alpha \in F_2^n \setminus \{0\}$ such that*

$$cB^{-1}a^T = 0, (B + I)\alpha^T = 0_n \text{ and } c\alpha^T = 1.$$

Proof. When B is invertible, It was already described in Theorem 5.3.1. Consider the case when $B + I$ is non-invertible. To determine x from $y = x(B + I) + S(xa^T)c$ it is necessary to get the response $S(xa^T)$ of S. This response can be obtained either directly from y or indirectly by determining xa^T from y and then using the query xa^T to S.

1. To determine xa^T from y there must exist a row vector $\alpha \in F_2^n$ such that $(B+I)\alpha^T = a^T$, $c\alpha^T = 0$ and consequently $xa^T = y\alpha^T$. After determining $u = xa^T$ we can find $v = S(u)$ and obtain the equations $x(B + I) = y + vc$ and $xa^T = u$ in x. Both equations can have more than one soultions since the matrix $\begin{pmatrix} B + I & a^T \end{pmatrix}$ have full rank. Indeed, $B + I$ is non invertible and $a^T = (B + I)\alpha^T$ is a linear combination of columns of $(B + I)$.

2. Suppose that $S(xa^T)$ can be determined by y. Then α has to satisfy the equations $(B + I)\alpha^T = 0_n$ and $c\alpha^T = 1$ which can be used to calculate $v = S(xa^T) = y\alpha^T$ and $u = xa^T = S^{-1}(v)$. After determining u, we again obtain the equation $x(B + I) = y + vc$ and $xa^T = u$. In order that this equation has a unique solution, the matrix $\begin{pmatrix} B + I & a^T \end{pmatrix}$ has to have full rank. If rank $\begin{pmatrix} B + I & a^T \end{pmatrix} = n$ then rank $\begin{pmatrix} B + I \end{pmatrix} = n - 1$. Therefore, all nonzero row vectors $\beta \in F_2^n$ such that $(B + I)\beta^T = 0_n$ are collinear to α. Since $c\alpha^T = 1$ and consequently $c\beta^T \neq 0$, rank $\begin{pmatrix} B + I \\ c \end{pmatrix} = n$.

■

Example 5.3.4. *Suppose*

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad B + I = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \text{ and } \quad a = (0, 0, 1), \quad c = (0, 1, 0).$$

It can be directly checked that

$$B^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad cB^{-1}a^T = 0,$$

and there exist $\alpha = (0, 1, 0)$

$$(B + I)\alpha^T = 0_n, \quad c\alpha^T = 1.$$

Thus, $y = xB + S(xa^T)c$ *is a complete mapping permutation on* $(\mathbb{F}_2^m)^3$*, for any positive integer* m *and any bijective function* S *on* $\mathbb{F}_2^m$*.*

Corollary 5.3.5. *Suppose $x, y \in (\mathbb{F}_2^m)^n$, $a, c \in \mathbb{F}_2^n$, $B = (b_{ij})_{n\times n}$ where $b_{ij} \in \mathbb{F}_2$, and S is any bijective function on $\mathbb{F}_2^m$. Then*

$$y = xB + S(xa^T)c$$

is a complete mapping permutation if the following conditions are satisfied:

1. *The ranks of B and $B + I$ are $n - 1$ and n, respectively.*
2. *There exist $a, c, \alpha \in F_2^n \setminus \{0\}$ such that*

$$c(B + I)^{-1}a^T = 0, B\alpha^T = 0_n \text{ and } c\alpha^T = 1.$$

Example 5.3.6. *Suppose*

$$B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad B + I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } \quad a = (1, 1, 0), \quad c = (1, 1, 1).$$

It can be directly checked that

$$(B + I)^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad c(B + I)^{-1}a^T = 0,$$

and there exist $\alpha = (1, 0, 0)$

$$B\alpha^T = 0_n, \quad c\alpha^T = 1.$$

Thus, $y = xB + S(xa^T)c$ is a complete mapping permutation on $(\mathbb{F}_2^m)^3$, for any positive integer m and any bijective function S on $\mathbb{F}_2^m$.

Corollary 5.3.7. *Suppose $x, y \in (\mathbb{F}_2^m)^n$, $a, c \in \mathbb{F}_2^n$, $B = (b_{ij})_{n\times n}$ where $b_{ij} \in \mathbb{F}_2$, and S is any bijective function on $\mathbb{F}_2^m$. Then*

$$y = xB + S(xa^T)c$$

is a complete mapping permutation if the following conditions are satisfied:

1. *Both B and $B+I$ have same rank $n-1$.*

2. *There exist $a, c \in F_2^n \setminus \{0\}$ such that*
$\begin{pmatrix} B & a^T \end{pmatrix}$, $\begin{pmatrix} B \\ c \end{pmatrix}$, $\begin{pmatrix} B+I & a^T \end{pmatrix}$ *and* $\begin{pmatrix} B+I \\ c \end{pmatrix}$ *have same rank n.*

Example 5.3.8. *Suppose*

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } \quad a = (0,1,0), \quad c = (1,0,0).$$

It can be directly checked that

$$\begin{pmatrix} B & a^T \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} B \\ c \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

and

$$B+I = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} B & a^T \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} B \\ c \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Thus, $y = xB + S(xa^T)c$ is a complete mapping permutation on $(\mathbb{F}_2^m)^3$, for any positive integer m and any bijective function S on $\mathbb{F}_2^m$.

Theorem 5.3.1 provides us a connection between any function on $\mathbb{F}_2^m$ to a complete mapping permutation on $(\mathbb{F}_2^m)^n$. In this context we raise the following question:
Given any pair of positive integers n, m estimate the total number of complete mapping permutations obtained from Theorems 5.3.1 and 5.3.3, Corollaries 5.3.5 and 5.3.7

Dai et al. [34] defined an iterative formula for computing the number of all linear orthomorphisms for $n \geq 2$. Let $N_1 = 1$, $N_i = (2^n - 2^{i-1})N_{i-1}$, $2 \leq i \leq n$, and let $|O_0(\mathbb{F}_2)| = 1$

and $|O_1(\mathbb{F}_2)| = 0$, then:

$$|O_n(\mathbb{F}_2)| = \sum_{r=2}^{n} 2^{r-2} N_r 2^{r(n-r)} |O_{n-r}(\mathbb{F}_2)| \tag{5.3.3}$$

where $|O_n(\mathbb{F}_2)| = \{\sigma | \sigma \in B, \sigma \text{ is complete mapping permutation}\}$.
The cardinality of B and $B + I$, described in Theorem 5.3.1, are calculated by Equation (5.3.3) with the particular choices of B, $B + I$ and c how many a exist in $\mathbb{F}_2^n \setminus \{0\}$ is estimated when,

$$cB^{-1}a^T = 0 \text{ and } c(B + I)^{-1}a^T = 0$$

where cB^{-1} and $c(B + I)^{-1}$ are non-zero $1 \times n$. Therefore, we define

$$Ker(cB^{-1}) = \{a \in \mathbb{F}_2^n \setminus \{0\} | cB^{-1}a^T = 0\}$$

$$Ker(c(B + I)^{-1}) = \{a \in \mathbb{F}_2^n \setminus \{0\} | c(B + I)^{-1}a^T = 0\}.$$

From rank-nullity theorem we get

$$dim\{Ker(cB^{-1})\} = n - 1 \text{ and } dim\{Ker(c(B + I)^{-1})\} = n - 1.$$

If $Ker(cB^{-1})$ and $Ker(c(B + I)^{-1})$ have common vectors, then

$$\begin{aligned} & dim\{Ker(cB^{-1}) \cap Ker(c(B + I)^{-1})\} \in \{n - 1, n - 2\}, \\ i.e., \quad & dim\{Ker(cB^{-1}) \cap Ker(c(B + I)^{-1})\} \geq n - 2. \end{aligned}$$

For positive integers m, we get the bound for complete mapping permutations (CMP)

$$2^{m \times 2^m} \times (2^{n-2} - 1) \leq \text{CMP} \leq 2^{m \times 2^m} \times (2^{n-1} - 1).$$

Therefore total estimate of complete mapping permutations is given by

$$|O_n(\mathbb{F}_2)| \times 2^{m \cdot 2^m} \times (2^{n-2} - 1) \times (2^n - 1) \leq \text{Total CMP} \leq |O_n(\mathbb{F}_2)| \times 2^{m \cdot 2^m} \times (2^{n-1} - 1) \times (2^n - 1).$$

We calculated the total number of matrices B and $B + I$, described in Theorem 5.3.3,

which satisfy the ranks n and $n-1$ respectively by MATLAB, for certain values of n. For particular B, $B+I$ and α how many a and c exist in $\mathbb{F}_2^n \setminus \{0\}$ is estimated when,

$$(B+I)\alpha^T = 0 \text{ and } c\alpha^T = 1,$$

where rank of $B+I$ is $n-1$. Therefore, we define

$$Ker(B+I) = \{\alpha \in \mathbb{F}_2^n \setminus \{0\} | (B+I)\alpha^T = 0\}.$$

By rank-nullity theorem we get

$$dim\{Ker(B+I)\} = 1.$$

Since α is non-zero. Then space $Ker(B+I)$ has only one vector. For this α, we get 2^{n-1} number of c vectors. For particular $c \in \mathbb{F}_2^n \setminus \{0\}$, we define

$$Ker(cB^{-1}) = \{a \in \mathbb{F}_2^n \setminus \{0\} | cB^{-1}a^T = 0\}.$$

By rank-nullity theorem we get

$$dim\{Ker(cB^{-1})\} = n-1.$$

For positive integers m, we get counts for complete mapping permutations (CMP)

$$\text{CMP} = 2^m! \times (2^{n-1}) \times (2^{n-1}-1).$$

Therefore total estimate of complete mapping permutations is given by

$$\text{CMP} = M \times 2^m! \times (2^{n-1}) \times (2^{n-1}-1),$$

where M is total number of matrices which satisfies the given condition. Similarly, we get the same estimation for Corollary 5.3.5.

There is no formula for the cardinality of B and $B+I$, described in Corollary 5.3.7, which

satisfy the condition for complete mapping permutation. We calculated the total number of matrices B and $B+I$ who satisfy the same rank $n-1$, respectively by MATLAB. Let $r_1, r_2, \ldots, r_n$ be the rows of B. Then the *span* of its row vectors or row space is defined as

$$Row_B = \{u_1r_1 + u_2r_2 + \cdots + u_nr_n : u_1, u_2, \ldots, u_n \in \mathbb{F}_2\}.$$

Similarly, the column space is defined as

$$Col_B = \{u_1s_1 + u_2s_2 + \cdots + u_ns_n : u_1, u_2, \ldots, u_n \in \mathbb{F}_2\}$$

where $s_1, s_2, \ldots, s_n$ are the columns of B. Now we define the same for matrix $B+I$

$$Row_{B+I} = \{u_1r_{I_1} + u_2r_{I_2} + \cdots + u_nr_{I_n} : u_1, u_2, \ldots, u_n \in \mathbb{F}_2\}$$

and

$$Col_{B+I} = \{u_1s_{I_1} + u_2s_{I_2} + \cdots + u_ns_{I_n} : u_1, u_2, \ldots, u_n \in \mathbb{F}_2\}.$$

The dimension of the all spaces is $n-1$ and all spaces are subspaces of $\mathbb{F}_2^n$. So we get

$$dim\{Row_B \cap Row_{B+I}\} \in \{n-1, n-2\},$$
$$\text{Similarly,} \quad dim\{Col_B \cap Col_{B+I}\} \in \{n-1, n-2\}.$$

Then the possible choices for choosing $c \in \mathbb{F}_2^n \setminus \{0\}$ are exactly

$$2^{n-2} \leq \text{ Cardinality of } c \text{ - vectors } \leq 2^{n-1}.$$

Similarly for $a \in \mathbb{F}_2^n \setminus \{0\}$, we get the same estimation. These choices of a and c are independent from the corresponding spaces. Therefore total estimate of complete mapping permutations is given by

$$M \times 2^m! \times (2^{n-2}) \times (2^{n-2}) \leq \text{ Total CMP } \leq M \times 2^m! \times (2^{n-1}) \times (2^{n-1}),$$

where M is total number of matrices which satisfies the given condition.

We summerized the total counts on complete mapping permutations for any value of m and $n = 2, 3, 4, 5$ as follows:

n	By Theorem 5.3.1				By Theorem 5.3.3	
	$\lvert GL(n,\mathbb{F}_2)\rvert$	$\lvert O_n(\mathbb{F}_2)\rvert$	$dim\{Ker(cB^{-1}) \cap Ker(c(B+I)^{-1})\}$	**Total CMP**	B is invertible, $B+I$'s rank is $n-1$	**Total CMP**
2	6	2	n-2=0	**0** (LB)	3	$2^m!\times$**6**
3	168	48	n-2=1	$2^{m2^m}\times$**336** (LB)	98	$2^m!\times$**1176**
4	20160	5824	n-2=2	$2^{m2^m}\times$**262080** (LB)	11640	$2^m!\times$**651840**
5	9999360	2887680	n-2=3	$2^{m2^m}\times$**626626560** (LB)	5775424	$2^m!\times$**1386101760**

Table 5.1: Counts of complete mapping permutations obtained from Theorems 5.3.1 and 5.3.3

n	By Corollary 5.3.5		By Corollary 5.3.7	
	$B+I$ is invertible, B's rank is $n-1$	**Total CMP**	Both $B, B+I$ have rank $n-1$	**Total CMP**
2	3	$2^m!\times$**6**	6	$2^m!\times$**6** (LB)
3	98	$2^m!\times$**1176**	168	$2^m!\times$**672** (LB)
4	11640	$2^m!\times$**651840**	21840	$2^m!\times$**349440** (LB)
5	5775424	$2^m!\times$**1386101760**	11189760	$2^m!\times$**716144640** (LB)

Table 5.2: Counts of complete mapping permutations obtained from Corollaries 5.3.5 and 5.3.7

5.4 A construction of a class of $\mathcal{K}$-complete mapping permutations

Let $\mathbb{F}_q$ be the finite field of q elements and $f(x) \in \mathbb{F}_q[x]$ a permutation polynomial over $\mathbb{F}_q$. For $k = 0, 1, 2, \ldots$, the k-th iteration of $f(x)$, i.e. $f^{(k)}(x)$, is defined by the following recurrence relation

$$f^{(0)}(x) = x, \qquad f^{(k)}(x) = f(f^{(k-1)}(x)), \qquad k = 1, 2, \ldots$$

For a finite set of s positive integers $\mathcal{K} = \{k_1, \ldots, k_s\}$ we call $f(x)$ a $\mathcal{K}$-complete mapping permutation if

$$f_{\mathcal{K}}(x) = x + \sum_{k \in \mathcal{K}} f^{(k)}(x)$$

is also a permutation polynomial. The concept of $\mathcal{K}$-complete mapping permutation unifies several kinds of mappings studied before in view of applications to cryptography, coding theory and combinatorics, we refer to [167]. For $\mathcal{K} = \{1\}$, suppose $f^{(0)} = I$ is the identity transformation.

Theorem 5.4.1. *Suppose $x, y \in (\mathbb{F}_2^m)^n$, $a, c \in \mathbb{F}_2^n$, $B = (b_{ij})_{n\times n}$ where $b_{ij} \in \mathbb{F}_2$, and S is any function on $\mathbb{F}_2^m$. Then*

$$y = xB + S(xa^T)c$$

is a $\{2\}$-complete mapping permutation if the following conditions are satisfied:

1. *B and $(B + B^{-1})$ both are invertible.*
2. *There exist $a, c \in F_2^n \setminus \{0\}$ such that*

$$cB^{-1}a^T = 0, \quad c(B + B^{-1})^{-1}a^T = 0 \text{ and } cB^{-1}(B + B^{-1})^{-1}a^T = 0.$$

Proof. In order to be a complete mapping permutation both

$$y = xB + S(xa^T)c \tag{5.4.1}$$

and

$$y = x + (xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c \tag{5.4.2}$$

have to be invertible. We alredy proved Equation (5.4.1) is invertible, if B is invertible and $cB^{-1}a^T = 0$. For Equation (5.4.2), since B is invertible

$$\begin{aligned} yB^{-1} &= xB^{-1} + xB + S(xa^T)c + S((xB + S(xa^T)c)a^T)cB^{-1} \\ \textit{i.e.,}\quad yB^{-1} &= x(B + B^{-1}) + S(xa^T)c + S((xB + S(xa^T)c)a^T)cB^{-1}. \end{aligned}$$

Let $(B + B^{-1})$ be also invertible, then

$$\begin{aligned} yB^{-1}(B + B^{-1})^{-1} &= x + S(xa^T)c(B + B^{-1})^{-1} + S((xB + S(xa^T)c)a^T) \\ &\qquad cB^{-1}(B + B^{-1})^{-1} \\ \textit{i.e.,}\quad yB^{-1}(B + B^{-1})^{-1}a^T &= xa^T + S(xa^T)c(B + B^{-1})^{-1}a^T + S((xB + S(xa^T)c)a^T) \\ &\qquad cB^{-1}(B + B^{-1})^{-1}a^T \\ \textit{i.e.,}\quad xa^T &= yB^{-1}(B + B^{-1})^{-1}a^T + S(xa^T)c(B + B^{-1})^{-1}a^T + \\ &\qquad S((xB + S(xa^T)c)a^T)cB^{-1}(B + B^{-1})^{-1}a^T \\ \textit{i.e.,}\quad xa^T &= yB^{-1}(B + B^{-1})^{-1}a^T, \text{ since } c(B + B^{-1})^{-1}a^T = 0 \text{ and} \end{aligned}$$

$$cB^{-1}(B+B^{-1})^{-1}a^T = 0.$$

Substituting $xa^T = yB^{-1}(B+B^{-1})^{-1}a^T$ above and in the place of xB, for each $a \in \mathbb{F}_2^n \setminus \{0\}$ there exist a $\beta \in \mathbb{F}_2^n \setminus \{0\}$ such that

$$\begin{aligned} B =& a^T\beta \implies xB = xa^T\beta, \\ i.e., \quad xB =& yB^{-3}(B+B^{-3})^{-1}a^T\beta, \end{aligned}$$

express uniquely. Then we get

$$\begin{aligned} yB^{-1}(B+B^{-1})^{-1} &= x + S(xa^T)c(B+B^{-1})^{-1} + S((xB+S(xa^T)c)a^T) \\ & \quad cB^{-1}(B+B^{-1})^{-1} \\ i.e., \quad x &= yB^{-1}(B+B^{-1})^{-1} + S(yB^{-1}(B+B^{-1})^{-1}a^T)c(B+B^{-1})^{-1} + \\ & \quad S((yB^{-1}(B+B^{-1})^{-1}a^T\beta + S(yB^{-1}(B+B^{-1})^{-1}a^T)c)a^T). \end{aligned}$$

Therefore, Equation (5.4.2) is invertible, if B and $(B+B^{-1})$ both are invertible and $c(B+B^{-1})^{-1}a^T = 0$, $cB^{-1}(B+B^{-1})^{-1}a^T = 0$. ■

Theorem 5.4.1 provides us a connection between any function on $\mathbb{F}_2^m$ to a $\{2\}$-complete mapping permutation on $(\mathbb{F}_2^m)^n$.

Example 5.4.2. *Suppose*

$$B = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad and \quad a = (0,0,0,1), \quad c = (0,0,0,1).$$

It can be directly checked that

$$B^{-1} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad B+B^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$(B+B^{-1})^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (B^{-1})(B+B^{-1})^{-1} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

and

$$cB^{-1}a^T = 0, \quad c(B+B^{-1})^{-1}a^T = 0 \text{ and } cB^{-1}(B+B^{-1})^{-1}a^T = 0.$$

Thus, $y = xB + S(xa^T)c$ is a $\{2\}$-complete mapping permutation on $(\mathbb{F}_2^m)^4$, for any positive integer m and any function S on $\mathbb{F}_2^m$.

Theorem 5.4.3. *Suppose $x, y \in (\mathbb{F}_2^m)^n$, $a, c \in \mathbb{F}_2^n$, $B = (b_{ij})_{n\times n}$ where $b_{ij} \in \mathbb{F}_2$, and S is any function on $\mathbb{F}_2^m$. Then*

$$y = xB + S(xa^T)c$$

is a $\{1,2\}$-complete mapping permutation if the following conditions are satisfied:

1. *B and $(I + B + B^{-1})$ both are invertible.*
2. *There exist $a, c \in F_2^n \setminus \{0\}$ such that*

$$cB^{-1}a^T = 0,\ c(I+B+B^{-1})^{-1}a^T = 0 \text{ and } cB^{-1}(I+B+B^{-1})^{-1}a^T = 0.$$

Proof. In order to be a complete mapping permutation

$$y = xB + S(xa^T)c \tag{5.4.3}$$

$$y = (xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c \tag{5.4.4}$$

and

$$y = x + xB + S(xa^T)c + (xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c \tag{5.4.5}$$

have to be invertible. We alredy proved Equation (5.4.3) is invertible, if B is invertible and $cB^{-1}a^T = 0$. Similarly Equation (5.4.4) is also invertible under same conditions. For

Equation (5.4.5), since B is invertible

$$yB^{-1} = xB^{-1} + x + S(xa^T)cB^{-1} + xB + S(xa^T)c + S((xB + S(xa^T)c)a^T)cB^{-1}$$
$$i.e., \quad yB^{-1} = x(I + B + B^{-1}) + S(xa^T)cB^{-1} + S(xa^T)c + S((xB + S(xa^T)c)a^T)cB^{-1}.$$

Let $(I + B + B^{-1})$ be also invertible, then

$$yB^{-1}(I + B + B^{-1})^{-1} = x + S(xa^T)cB^{-1}(I + B + B^{-1})^{-1} + S(xa^T)c(I + B+$$
$$B^{-1})^{-1} + S((xB + S(xa^T)c)a^T)c(I + B + B^{-1})^{-1}$$
$$i.e., \quad yB^{-1}(I + B + B^{-1})^{-1}a^T = xa^T + S(xa^T)cB^{-1}(I + B + B^{-1})^{-1}a^T + S(xa^T)c(I+$$
$$B + B^{-1})^{-1}a^T + S((xB + S(xa^T)c)a^T)c(I + B + B^{-1})^{-1}a^T$$
$$i.e., \quad xa^T = yB^{-1}(I + B + B^{-1})^{-1}a^T + S(xa^T)cB^{-1}(I + B + B^{-1})^{-1}a^T + S(xa^T)c(I+$$
$$B + B^{-1})^{-1}a^T + S((xB + S(xa^T)c)a^T)c(I + B + B^{-1})^{-1}a^T$$
$$i.e., \quad xa^T = yB^{-1}(I + B + B^{-1})^{-1}a^T \text{ since } cB^{-1}(I + B + B^{-1})^{-1}a^T = 0 \text{ and}$$
$$c(I + B + B^{-1})^{-1}a^T = 0.$$

Substituting $xa^T = yB^{-1}(I + B + B^{-1})^{-1}a^T$ above and in the place of xB, for each $a \in \mathbb{F}_2^n \setminus \{0\}$ there exist a $\beta \in \mathbb{F}_2^n \setminus \{0\}$ such that

$$B = a^T\beta \implies xB = xa^T\beta,$$
$$i.e., \quad xB = yB^{-3}(B + B^{-3})^{-1}a^T\beta,$$

express uniquely. Then we get

$$yB^{-1}(I + B + B^{-1})^{-1} = x + S(xa^T)cB^{-1}(I + B + B^{-1})^{-1} + S(xa^T)c(I + B+$$
$$B^{-1})^{-1} + S((xB + S(xa^T)c)a^T)c(I + B + B^{-1})^{-1}$$
$$i.e., \quad x = yB^{-1}(I + B + B^{-1})^{-1} + S(yB^{-1}(I + B + B^{-1})^{-1}a^T)cB^{-1}(I + B + B^{-1})^{-1}$$
$$+ S(yB^{-1}(I + B + B^{-1})^{-1}a^T)c(I + B + B^{-1})^{-1} + S((yB^{-1}(I + B + B^{-1})^{-1}$$
$$a^T\beta + S(yB^{-1}(I + B + B^{-1})^{-1}a^T)c)a^T)c(I + B + B^{-1})^{-1}.$$

Therefore, Equation (5.4.5) is invertible, if B and $(I + B + B^{-1})$ both are invertible and

$cB^{-1}a^T = 0$, $c(I + B + B^{-1})^{-1}a^T = 0$ and $cB^{-1}(I + B + B^{-1})^{-1}a^T = 0$. ■

Theorem 5.4.3 provides us a connection between any function on $\mathbb{F}_2^m$ to a $\{1, 2\}$-complete mapping permutation on $(\mathbb{F}_2^m)^n$.

Example 5.4.4. *Suppose*

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \text{ and } \quad a = (0, 1, 0), \quad c = (0, 0, 1).$$

It can be directly checked that

$$B^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad (I + B + B^{-1})^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$(B^{-1})(I + B + B^{-1})^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

and

$$cB^{-1}a^T = 0, \ c(I + B + B^{-1})^{-1}a^T = 0 \text{ and } cB^{-1}(I + B + B^{-1})^{-1}a^T = 0.$$

Thus, $y = xB + S(xa^T)c$ is a $\{1, 2\}$-complete mapping permutation on $(\mathbb{F}_2^m)^3$, for any positive integer m and any function S on $\mathbb{F}_2^m$.

In this context we raise the following question:

Given any pair of positive integers n, m estimate the total number of $\{2\}$-complete mapping permutations and $\{1, 2\}$-complete mapping permutations obtained from Theorems 5.4.1 and 5.4.3.

There is no formula for the cardinality of B and $B + B^{-1}$, described in Theorem 5.4.1, which satisfy the condition for $\{2\}$-complete mapping permutation. We calculate the total number of $\{2\}$-complete mapping permutations, i.e., Total $\{2\}$-CMP, by MATLAB.

There is no formula for the cardinality of B and $I + B + B^{-1}$, described in Theorem 5.4.3, which satisfy the condition for $\{1, 2\}$-complete mapping permutation. We calculate the total

number of $\{1,2\}$-complete mapping permutations, i.e., Total $\{1,2\}$-CMP, by MATLAB.

We summerized the total counts on $\{2\}$-complete mapping permutations and $\{1,2\}$-complete mapping permutations for any value of m and $n = 2,3,4,5$ as follows:

n	By Theorem 5.4.1		By Theorem 5.4.3	
	B and $(B+B^{-1})$ both are invertible	**Total $\{2\}$-CMP**	B and $(I+B+B^{-1})$ both are invertible	**Total $\{1,2\}$-CMP**
2	2	**0**	4	**6**
3	48	**0**	112	**504**
4	5824	$2^{m2^m}\times$**100800**	13888	$2^{m2^m}\times$**315840**
5	2887680	$2^{m2^m}\times$**279982080**	6888448	$2^{m2^m}\times$**749952000**

Table 5.3: Counts of $\{2\}$-complete mapping permutations and $\{1,2\}$-complete mapping permutations obtained from Theorems 5.4.1 and 5.4.3

Similarly we can drive the expression for $\{r\}$-complete mapping permutations, $r = 3$ and 4. With factor $\{3\}$ and $\{4\}$, we have the combinations as follows:

With factor $\{3\}$	With factor $\{4\}$
$\{3\}$-CMP	$\{4\}$-CMP
$\{1,3\}$-CMP	$\{1,4\}$-CMP
$\{2,3\}$-CMP	$\{2,4\}$-CMP
$\{1,2,3\}$-CMP	$\{3,4\}$-CMP
	$\{1,2,4\}$-CMP
	$\{1,3,4\}$-CMP
	$\{2,3,4\}$-CMP
	$\{1,2,3,4\}$-CMP

Table 5.4: All combinations of complete mapping permutations

Here we are interested only to drive the expression for $\{3\}$, $\{1,2,3\}$, $\{4\}$ and $\{1,2,3,4\}$-complete mapping permutations. The following theorems and corollaries are as follows:

Theorem 5.4.5. *Suppose $x, y \in (\mathbb{F}_2^m)^n$, $a, c \in \mathbb{F}_2^n$, $B = (b_{ij})_{n\times n}$ where $b_{ij} \in \mathbb{F}_2$, and S is any function on $\mathbb{F}_2^m$. Then*

$$y = xB + S(xa^T)c$$

is a $\{3\}$-complete mapping permutation if the following conditions are satisfied:

1. *B and $(B + B^{-2})$ both are invertible.*

2. *There exist $a, c \in F_2^n \setminus \{0\}$ such that*

$$cB^{-1}a^T = 0,\ c(B+B^{-2})^{-1}a^T = 0,\ cB^{-1}(B+B^{-2})^{-1}a^T = 0$$
$$\text{and} \quad cB^{-2}(B+B^{-2})^{-1}a^T = 0.$$

Proof. In order to be a complete mapping permutation both

$$y = xB + S(xa^T)c \tag{5.4.6}$$

and

$$\begin{aligned} y = x + ((xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c)B + S(((xB + S(xa^T)c)B \\ + S((xB + S(xa^T)c)a^T)c)a^T)c \end{aligned} \tag{5.4.7}$$

have to be invertible. We alredy proved Equation (5.4.6) is invertible, if B is invertible and $cB^{-1}a^T = 0$. For Equation (5.4.7), since B is invertible

$$\begin{aligned} yB^{-1} &= xB^{-1} + (xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c + \\ &\quad S(((xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c)a^T)cB^{-1} \\ i.e., \quad yB^{-2} &= xB^{-2} + xB + S(xa^T)c + S((xB + S(xa^T)c)a^T)cB^{-1} + \\ &\quad S(((xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c)a^T)cB^{-2}. \end{aligned}$$

Let $(B + B^{-2})$ be also invertible, then

$$\begin{aligned} yB^{-2}(B + B^{-2})^{-1} &= x + S(xa^T)c(B + B^{-2})^{-1} + S((xB + S(xa^T)c)a^T)cB^{-1} \\ &\quad (B + B^{-2})^{-1} + S(((xB + S(xa^T)c)B + S((xB + S(xa^T)c) \\ &\quad a^T)c)a^T)cB^{-2}(B + B^{-2})^{-1} \\ i.e., yB^{-2}(B + B^{-2})^{-1}a^T &= xa^T + S(xa^T)c(B + B^{-2})^{-1}a^T + S((xB + S(xa^T)c)a^T) \\ &\quad cB^{-1}(B + B^{-2})^{-1}a^T + S(((xB + S(xa^T)c)B + S((xB + \\ &\quad S(xa^T)c)a^T)c)a^T)cB^{-2}(B + B^{-2})^{-1}a^T \\ i.e., xa^T &= yB^{-2}(B + B^{-2})^{-1}a^T + S(xa^T)c(B + B^{-2})^{-1}a^T + S((xB + S(xa^T)c)a^T) \\ &\quad cB^{-1}(B + B^{-2})^{-1}a^T + S(((xB + S(xa^T)c)B + S((xB + \\ &\quad S(xa^T)c)a^T)c)a^T)cB^{-2}(B + B^{-2})^{-1}a^T \\ i.e., \quad xa^T &= yB^{-2}(B + B^{-2})^{-1}a^T, \text{ since } c(B + B^{-2})^{-1}a^T = 0, \\ &\quad cB^{-1}(B + B^{-2})^{-1}a^T = 0 \text{ and } cB^{-2}(B + B^{-2})^{-1}a^T = 0. \end{aligned}$$

Substituting $xa^T = yB^{-2}(B+B^{-2})^{-1}a^T$ above and in the place of xB, for each $a \in \mathbb{F}_2^n \setminus \{0\}$

there exist a $\beta \in \mathbb{F}_2^n \setminus \{0\}$ such that

$$B = a^T\beta \implies xB = xa^T\beta,$$
$$i.e., \quad xB = yB^{-3}(B + B^{-3})^{-1}a^T\beta,$$

express uniquely. Then we get

$$yB^{-2}(B + B^{-2})^{-1} = x + S(xa^T)c(B + B^{-2})^{-1} + S((xB + S(xa^T)c)a^T)cB^{-1}$$
$$(B + B^{-2})^{-1} + S(((xB + S(xa^T)c)B + S((xB + S(xa^T)c)$$
$$a^T)c)a^T)cB^{-2}(B + B^{-2})^{-1}$$
$$i.e., \quad x = yB^{-2}(B + B^{-2})^{-1} + S(yB^{-2}(B + B^{-2})^{-1}a^T)c(B + B^{-2})^{-1} + S((yB^{-2}$$
$$(B + B^{-2})^{-1}a^T\beta + S(yB^{-2}(B + B^{-2})^{-1}a^T)c)a^T)cB^{-1}(B + B^{-2})^{-1} +$$
$$S(((yB^{-2}(B + B^{-2})^{-1}a^T\beta + S(yB^{-2}(B + B^{-2})^{-1}a^T)c)B + S((yB^{-2}(B + B^{-2})^{-1}$$
$$a^T\beta + S(yB^{-2}(B + B^{-2})^{-1}a^T)c)a^T)c)a^T)cB^{-2}(B + B^{-2})^{-1}.$$

Therefore, Equation (5.4.7) is invertible, if B and $(B + B^{-2})$ both are invertible and $cB^{-1}a^T = 0$, $c(B + B^{-2})^{-1}a^T = 0$, $cB^{-1}(B + B^{-2})^{-1}a^T = 0$ and $cB^{-2}(B + B^{-2})^{-1}a^T = 0$.

■

Theorem 5.4.5 provides us a connection between any function on $\mathbb{F}_2^m$ to a $\{3\}$-complete mapping permutation on $(\mathbb{F}_2^m)^n$.

Theorem 5.4.6. *Suppose $x, y \in (\mathbb{F}_2^m)^n$, $a, c \in \mathbb{F}_2^n$, $B = (b_{ij})_{n\times n}$ where $b_{ij} \in \mathbb{F}_2$, and S is any function on $\mathbb{F}_2^m$. Then*

$$y = xB + S(xa^T)c$$

is a $\{4\}$-complete mapping permutation if the following conditions are satisfied:

1. *B and $(B + B^{-3})$ are invertible.*

2. *There exist $a, c \in F_2^n \setminus \{0\}$ such that*

$$cB^{-1}a^T = 0,\ c(B + B^{-3})^{-1}a^T = 0,\ cB^{-1}(B + B^{-3})^{-1}a^T = 0,$$
$$cB^{-2}(B+B^{-3})^{-1}a^T = 0 \text{ and } cB^{-3}(B + B^{-3})^{-1}a^T = 0.$$

Proof. In order to be a complete mapping permutation both

$$y = xB + S(xa^T)c \tag{5.4.8}$$

and

$$\begin{aligned} y = x + (((xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c)B + S(((xB + S(xa^T)c)B + \\ S((xB + S(xa^T)c)a^T)c)a^T)c)B + S((((xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c)B \\ + S(((xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c)a^T)c)a^T)c \end{aligned} \tag{5.4.9}$$

have to be invertible. We alredy proved Equation (5.4.8) is invertible, if B is invertible and $cB^{-1}a^T = 0$. For Equation (5.4.9), since B is invertible

$$\begin{aligned} yB^{-1} = xB^{-1} + ((xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c)B + S(((xB + \\ S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c)a^T)c + S((((xB + S(xa^T)c)B + \\ S((xB + S(xa^T)c)a^T)c)B + S(((xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T) \\ c)a^T)c)a^T)cB^{-1} \end{aligned}$$

$$\begin{aligned} i.e., \quad yB^{-2} = xB^{-2} + (xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c + S(((xB + S(xa^T) \\ c)B + S((xB + S(xa^T)c)a^T)c)a^T)cB^{-1} + S((((xB + S(xa^T)c)B + S((xB + \\ S(xa^T)c)a^T)c)B + S(((xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c)a^T)c)a^T)cB^{-2} \end{aligned}$$

$$\begin{aligned} i.e., \quad yB^{-3} = xB^{-3} + xB + S(xa^T)c + S((xB + S(xa^T)c)a^T)cB^{-1} + S(((xB + S(xa^T) \\ c)B + S((xB + S(xa^T)c)a^T)c)a^T)cB^{-2} + S((((xB + S(xa^T)c)B + S((xB + \\ S(xa^T)c)a^T)c)B + S(((xB + S(xa^T)c)B + S((xB + S(xa^T)c)a^T)c)a^T)c)a^T)cB^{-3}. \end{aligned}$$

Let $(B + B^{-3})$ be also invertible, then

$$yB^{-3}(B + B^{-3})^{-1} = x + S(xa^T)c(B + B^{-3})^{-1} + S((xB + S(xa^T)c)a^T)cB^{-1}(B + B^{-3})^{-1}$$

$$+S(((xB+S(xa^T)c)B+S((xB+S(xa^T)c)a^T)c)a^T)cB^{-2}(B+B^{-3})^{-1}+S((((xB+S(xa^T)c)B+$$

$$S((xB+S(xa^T)c)a^T)c)B+S(((xB+S(xa^T)c)B+S((xB+S(xa^T)c)a^T)c)a^T)c)a^T)cB^{-3}(B+B^{-3})^{-1},$$

$$i.e., yB^{-3}(B+B^{-3})^{-1}a^T = xa^T+S(xa^T)c(B+B^{-3})^{-1}a^T+S((xB+S(xa^T)c)a^T)cB^{-1}(B+B^{-3})^{-1}a^T$$

$+S(((xB+S(xa^T)c)B+S((xB+S(xa^T)c)a^T)cB^{-2}(B+B^{-3})^{-1}a^T+S((((xB+S(xa^T)c)B+$

$S((xB+S(xa^T)c)a^T)c)B+S(((xB+S(xa^T)c)B+S((xB+S(xa^T)c)a^T)c)a^T)cB^{-3}(B+B^{-3})^{-1}a^T$

$$i.e., \quad xa^T = yB^{-3}(B+B^{-3})^{-1}a^T, \text{ since } c(B+B^{-3})^{-1}a^T = 0,\ cB^{-1}(B+B^{-3})^{-1}a^T = 0,$$

$$cB^{-2}(B+B^{-3})^{-1}a^T = 0 \text{ and } cB^{-3}(B+B^{-3})^{-1}a^T = 0.$$

Substituting $xa^T = yB^{-3}(B+B^{-3})^{-1}a^T$ above and in the place of xB, for each $a \in \mathbb{F}_2^n \setminus \{0\}$ there exist a $\beta \in \mathbb{F}_2^n \setminus \{0\}$ such that

$$B = a^T\beta \implies xB = xa^T\beta,$$
$$i.e., \quad xB = yB^{-3}(B+B^{-3})^{-1}a^T\beta,$$

express uniquely. Then we get

$$yB^{-3}(B+B^{-3})^{-1} = x + S(xa^T)c(B+B^{-3})^{-1} + S((xB+S(xa^T)c)a^T)cB^{-1}(B+B^{-3})^{-1}$$

$+S(((xB+S(xa^T)c)B+S((xB+S(xa^T)c)a^T)c)a^T)cB^{-2}(B+B^{-3})^{-1}+S((((xB+S(xa^T)c)B+$

$S((xB+S(xa^T)c)a^T)c)B+S(((xB+S(xa^T)c)B+S((xB+S(xa^T)c)a^T)c)a^T)cB^{-3}(B+B^{-3})^{-1}$

$i.e., \quad x = yB^{-3}(B+B^{-3})^{-1}+S(yB^{-3}(B+B^{-3})^{-1}a^T)c(B+B^{-3})^{-1}+S((yB^{-3}(B+B^{-3})^{-1}a^T\beta$

$+S(yB^{-3}(B+B^{-3})^{-1}a^T)c)a^T)cB^{-1}(B+B^{-3})^{-1}+S(((yB^{-3}(B+B^{-3})^{-1}a^T\beta+S(yB^{-3}(B+B^{-3})^{-1}$

$a^T)c)B + S((yB^{-3}(B+B^{-3})^{-1}a^T\beta + S(yB^{-3}(B+B^{-3})^{-1}a^T)c)a^T)c)a^T)cB^{-2}(B+B^{-3})^{-1}+$

$S((((yB^{-3}(B+B^{-3})^{-1}a^T\beta + S(yB^{-3}(B+B^{-3})^{-1}a^T)c)B + S((yB^{-3}(B+B^{-3})^{-1}a^T\beta+$

$S(yB^{-3}(B+B^{-3})^{-1}a^T)c)a^T)c)B + S(((yB^{-3}(B+B^{-3})^{-1}a^T\beta + S(yB^{-3}(B+B^{-3})^{-1}a^T)c)B$

$+S((yB^{-3}(B+B^{-3})^{-1}a^T\beta + S(yB^{-3}(B+B^{-3})^{-1}a^T)c)a^T)c)a^T)cB^{-3}(B+B^{-3})^{-1}.$

Therefore, Equation (5.4.9) is invertible, if B and $(B+B^{-2})$ both are invertible and $cB^{-1}a^T = 0$, $c(B+B^{-2})^{-1}a^T = 0$, $cB^{-1}(B+B^{-2})^{-1}a^T = 0$ and $cB^{-2}(B+B^{-2})^{-1}a^T = 0$.

■

Theorem 5.4.6 provides us a connection between any function on $\mathbb{F}_2^m$ to a $\{4\}$-complete

mapping permutation on $(\mathbb{F}_2^m)^n$.

Corollary 5.4.7. *Suppose $x, y \in (\mathbb{F}_2^m)^n$, $a, c \in \mathbb{F}_2^n$, $B = (b_{ij})_{n\times n}$ where $b_{ij} \in \mathbb{F}_2$, and S is any function on $\mathbb{F}_2^m$. Then*

$$y = xB + S(xa^T)c$$

is a $\{1, 2, 3\}$-complete mapping permutation if the following conditions are satisfied:

1. *B and $(I + B + B^{-1} + B^{-2})$ both are invertible.*
2. *There exist $a, c \in F_2^n \setminus \{0\}$ such that*

$$cB^{-1}a^T = 0,\ c(I + B + B^{-1} + B^{-2})^{-1}a^T = 0,\ cB^{-1}(I + B + B^{-1} + B^{-2})^{-1}a^T = 0,$$
$$\text{and} \quad cB^{-2}(I + B + B^{-1} + B^{-2})^{-1}a^T = 0.$$

Corollary 5.4.8. *Suppose $x, y \in (\mathbb{F}_2^m)^n$, $a, c \in \mathbb{F}_2^n$, $B = (b_{ij})_{n\times n}$ where $b_{ij} \in \mathbb{F}_2$, and S is any function on $\mathbb{F}_2^m$. Then*

$$y = xB + S(xa^T)c$$

is a $\{1, 2, 3, 4\}$-complete mapping permutation if the following conditions are satisfied:

1. *B and $(I + B + B^{-1} + B^{-2} + B^{-3})$ both are invertible.*
2. *There exist $a, c \in F_2^n \setminus \{0\}$ such that*

$$cB^{-1}a^T = 0,\ c(I+B+B^{-1}+B^{-2}+B^{-3})^{-1}a^T = 0,\ cB^{-1}(I+B+B^{-1}+B^{-2}+B^{-3})^{-1}a^T = 0,$$

$$cB^{-2}(I+B+B^{-1}+B^{-2}+B^{-3})^{-1}a^T = 0 \text{ and } cB^{-3}(I+B+B^{-1}+B^{-2}+B^{-3})^{-1}a^T = 0.$$

In this context we raise the following question:
Given any pair of positive integers n, m estimate the total number of $\{3\}$-complete mapping permutations, $\{1, 2, 3\}$-complete mapping permutations, $\{4\}$-complete mapping permutations and $\{1, 2, 3, 4\}$-complete mapping permutations obtained from Theorems 5.4.5 and 5.4.6, Corollaries 5.4.7 and 5.4.8 respectively.

Similarly we can estimate the total counts by MATLAB.

5.5 Extension on a complete mapping permutation S of dimension r to a complete mapping permutation of dimension n

Definition 5.5.1. *Let $S\colon F^r \to F^r$ and the mapping $S^+\colon F^r \to F^r$ be defined as $S^+(z) = S(z) + z$ for all $z \in F^r$. In particular, S is a complete mapping if and only if S and S^+ both are bijective.*

Theorem 5.5.2. *Suppose $x, y \in (\mathbb{F}_2)^n$, $A = (a_{ij})_{n\times r}, C = (c_{ij})_{r\times n}, B = (b_{ij})_{n\times n}$ where $a_{ij}, b_{ij}, c_{ij} \in \mathbb{F}_2$, and S is permutation on $(\mathbb{F}_2)^r$, where $n = 2r$. Then*

$$y = xB + S(xA)C$$

is a complete mapping permutation on $(\mathbb{F}_2)^n$ if the following conditions are satisfied:

1. $\begin{pmatrix} B & A \end{pmatrix}$ *and $B + I$ both are invertible.*
2. *There exist non-zero matrices $D = (d_{ij})_{n\times r}$ and $E = (e_{ij})_{n\times r}$, where $d_{ij}, e_{ij} \in \mathbb{F}_2$ such that*

$$BD = O_{n\times r},\ CD = I_r\ ,\ CE = 0_r \text{ and } (B + I)E = A.$$

Proof. In order to be a complete mapping permutation both

$$y = xB + S(xA)C \tag{5.5.1}$$

and

$$y = x(B + I) + S(xA)C \tag{5.5.2}$$

have to be invertible. Following arguments are due to Agievich [2] which we recall for completeness. Let D be a matrix of dimension $n \times r$ such that

$$\begin{aligned} & yD = xBD + S(xA)CD \\ i.e., \quad & yD = S(xA)I_r, \text{ since } BD = O_{n\times r} \text{ and } CD = I_r \\ i.e., \quad & xA = S^{-1}(yD). \end{aligned}$$

Since S is complete mapping permutation, xA can be uniquely determined from yD. After determining xA, we get

$$\begin{aligned} & xB = y + yDC \\ i.e., \quad & x\begin{pmatrix} B & A \end{pmatrix} = \begin{pmatrix} y + yDC & S^{-1}(yD) \end{pmatrix} \text{ since } \begin{pmatrix} B & A \end{pmatrix} \text{ is invertible.} \end{aligned}$$

Therefore, Equation (5.5.1) is invertible, if $\begin{pmatrix} B & A \end{pmatrix}$ is invertible, S is bijective and there exist a non-zero matrix D such that $BD = O_{n\times r}$ and $CD = I_r$. Similarly we check for Equation (5.5.2) with same B, A and C, let E be a matrix of dimension $n \times r$ such that

$$\begin{aligned} & yE = x(B + I)E + S(xA)CE \\ i.e., \quad & yE = xA, \text{ since } (B + I)E = A \text{ and } CE = 0_r. \end{aligned}$$

After determining xA, we get

$$\begin{aligned} & y = x(B + I) + S(yE)C \\ i.e., \quad & x = y(B + I)^{-1} + S(yE)C(B + I)^{-1} \text{ since } (B + I) \text{ is invertible.} \end{aligned}$$

Therefore, Equation (5.5.2) is invertible, if $B + I$ is invertible and there exist a non-zero matrix E such that $(B + I)E = A$ and $CE = O_r$. We see that by rank properties:

$$rank(C) = rank(D) = r, \text{ i.e., } rank(B) \leq n - r \text{ and } rank(E) \leq n - r.$$

Since $rank(B + I) = n$ and $rank\begin{pmatrix} B & A \end{pmatrix} = n$, then

$$rank(B + I) + rank(E) \leq rank(A) + n,$$

$$rank(E) \leq rank(A).$$

This inequality holds only when $n = 2r$. ∎

Theorem 5.5.2 provides us a connection between permutation on $(\mathbb{F}_2)^r$ to a complete mapping permutation on $(\mathbb{F}_2)^n$.

Example 5.5.3. *Suppose*

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \quad C = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

There exist D and E

$$D = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ and } \quad E = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

It can be directly checked that

$$(B+I) * E = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad BD = O_{n\times r},\ CD = I_r \text{ and } CE = 0_r.$$

Thus, $y = xB + S(xA)C$ is a complete mapping permutation on $(\mathbb{F}_2)^4$, for permutation S on $(\mathbb{F}_2)^2$.

Corollary 5.5.4. *Suppose $x, y \in (\mathbb{F}_2)^n$, $A = (a_{ij})_{n\times r}, C = (c_{ij})_{r\times n}, B = (b_{ij})_{n\times n}$ where $a_{ij}, b_{ij}, c_{ij} \in \mathbb{F}_2$, and S is complete mapping permutation on $(\mathbb{F}_2)^r$, where $n = 2r$. Then*

$$y = xB + S(xA)C$$

is a complete mapping permutation on $(\mathbb{F}_2)^n$ if the following conditions are satisfied:

1. $\begin{pmatrix} B & A \end{pmatrix}$ *and $B + I$ both are invertible.*
2. *We choose matrices B, A and C such that*

$$BA = O_{n\times r} \text{ and } CA = I_r.$$

Corollary 5.5.4 provides us a connection between any complete mapping permutation on $(\mathbb{F}_2)^r$ to a complete mapping permutation on $(\mathbb{F}_2)^n$.

Example 5.5.5. *Suppose*

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \quad C = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

It can be directly checked that

$$B * A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \quad C * A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus, $y = xB + S(xA)C$ is a complete mapping permutation on $(\mathbb{F}_2)^4$, for any complete mapping permutation S on $(\mathbb{F}_2)^2$.

In this context we raise the following question:
Given any permutation and complete mapping permutations on $(\mathbb{F}_2)^r$ obtained complete mapping permutation from Theorem 5.5.2 and Corollary 5.5.4 respectively.

We summerized the total counts on complete mapping permutations for $r = 2$ and $n = 4$ as follows:

n	By Theorem 5.5.2		By Corollary 5.5.4	
	r	**Total CMP**	r	**Total CMP**
4	2	**725760**	2	**107520**

Table 5.5: Counts of complete mapping permutation obtained from Theorem 5.5.2 and Corollary 5.5.4

5.6 Huge quasigroups obtained by a chain of generalized XS-circuits

The following proposition is proved by Sade [143].

Proposition 5.6.1. [143, 14] *Let $(Q,+)$ be an admissible group with complete mapping θ. Then $* : Q \times Q \to Q$ is defined as:*

$$x * y = \theta(x - y) + y, \tag{5.6.1}$$

where $x, y \in Q$. Then $(Q, *)$ is a quasigroup.

Note that S is a permutation or complete mapping permutation on $(\mathbb{F}_2)^r$ when $r \geq 2$, so XS-circuits is a complete mapping permutation on $(\mathbb{F}_2)^n$ where $n = 2r$. Define $(A, B, C|S)_{(1)} = (A, B, C|S)$ and let $(A, B, C|S)_{(t)}$, $t \geq 1$, be defined. Then, for some B, A, C be matrices over $\mathbb{F}_2$ of dimension $(t+1) \times (t+1)$, $(t+1) \times r$, $r \times (t+1)$ respectively, define $(A, B, C|S)_{(t+1)}$ to be the generalized XS-circuits created by the permutation or complete mapping permutation $(A, B, C|S)_{(t)}$. Note that $(A, B, C|S)_{(t)}$ is a complete mapping permutations on $(\mathbb{F}_2)^{r2^t}$ for each $t \geq 1$. Hence we have defined inductively a chain of complete mapping permutations $\{(A, B, C|S)_{(t)} | t = 1, 2, 3, \dots\}$ in the corresponding groups. Now we can construct quasigroup of order 2^{r2^t} on the set $(\mathbb{F}_2)^{r2^t}$ for each $n \geq 1$.

A class of huge quasigroups of order 2^{2^k} can be designed as follows. Take $S : (\mathbb{F}_2)^{2^t} \to (\mathbb{F}_2)^{2^t}$, where $t < k$ is a small positive integer ($t = 1, 2, 3$). Choose B, A, C be matrices over $\mathbb{F}_2$ of dimension $2^{t+i} \times 2^{t+i}$, $2^{t+i} \times 2^t$, $2^t \times 2^{t+i}$ respectively, $1 \leq i \leq k - t$, and construct iteratively the complete mapping permutation $(A, B, C|S) = (A, B, C|S)_{k-t} : (\mathbb{F}_2)^{2^k} \to (\mathbb{F}_2)^{2^k}$. Define a quasigroup operation $*$ on the set $(\mathbb{F}_2)^{2^k}$. By Equation (5.6.1) we get

$$x * y = (A, B, C|S)(x + y) + y \qquad \text{for every } x, y \text{ in } (\mathbb{F}_2)^{2^k}.$$

Note that we need only $k - t$ iterations for getting the quasigroups of required order. Construct a quasigroup of order 2^{2^7}, for instance:

Example 5.6.2. *We can use the complete mapping permutation $S : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ for Example 1.8.2. So $t = 1$, we choose B, A, C be matrices over $\mathbb{F}_2$ of dimension $2^{t+i} \times 2^{t+i}$, $2^{t+i} \times 2^t$,*

$2^t \times 2^{t+i}$ *respectively,* $i = 1, 2, \ldots, 6$. *Now we can construct the following complete mapping permutations, where* $x_i, y_i \in (\mathbb{F}_2)^i$, $i = 4, 8, 16, \ldots$:

$S : (\mathbb{F}_2)^2 \to (\mathbb{F}_2)^2$, $(A, B, C|S)_{(1)}$ *as*

$$x_4 \mapsto y_4 = x_4 B_{4\times 4} + S(x_4 A_{4\times 2}) C_{2\times 4}$$

where $B_{4\times 4}$, $A_{4\times 2}$ *and* $C_{2\times 4}$ *satisfied by Theorem 5.5.2 or Corollary 5.5.4.*

$(A, B, C|S)_{(1)} : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4, (A, B, C|S)_{(2)}$ *as*

$$x_8 \mapsto y_8 = x_8 B_{8\times 8} + (A, B, C|S)_{(1)}(x_8 A_{8\times 4}) C_{4\times 8}$$

where $B_{8\times 8}$, $A_{8\times 4}$ *and* $C_{4\times 8}$ *satisfied by Theorem 5.5.2 or Corollary 5.5.4.*

$(A, B, C|S)_{(2)} : (\mathbb{F}_2)^8 \to (\mathbb{F}_2)^8, (A, B, C|S)_{(3)}$ *as*

$$x_{16} \mapsto y_{16} = x_{16} B_{16\times 16} + (A, B, C|S)_{(2)}(x_{16} A_{16\times 8}) C_{8\times 16}$$

where $B_{16\times 16}$, $A_{16\times 8}$ *and* $C_{8\times 16}$ *satisfied by Theorem 5.5.2 or Corollary 5.5.4.*

$(A, B, C|S)_{(3)} : (\mathbb{F}_2)^{16} \to (\mathbb{F}_2)^{16}, (A, B, C|S)_{(4)}$ *as*

$$x_{32} \mapsto y_{32} = x_{32} B_{32\times 32} + (A, B, C|S)_{(3)}(x_{32} A_{32\times 16}) C_{16\times 32}$$

where $B_{32\times 32}, A_{32\times 16}$ *and* $C_{16\times 32}$ *satisfied by Theorem 5.5.2 or Corollary 5.5.4.*

$(A, B, C|S)_{(4)} : (\mathbb{F}_2)^{32} \to (\mathbb{F}_2)^{32}, (A, B, C|S)_{(5)}$ *as*

$$x_{64} \mapsto y_{64} = x_{64} B_{64\times 64} + (A, B, C|S)_{(4)}(x_{64} A_{64\times 32}) C_{32\times 64}$$

where $B_{64\times 64}$, $A_{64\times 32}$ *and* $C_{32\times 64}$ *satisfied by Theorem 5.5.2 or Corollary 5.5.4.*

$(A, B, C|S)_{(5)} : (\mathbb{F}_2)^{64} \to (\mathbb{F}_2)^{64}, (A, B, C|S)_{(6)}$ *as*

$$x_{128} \mapsto y_{128} = x_{128}B_{128\times128} + (A, B, C|S)_{(5)}(x_{128}A_{128\times64})C_{64\times128}$$

where $B_{128\times128}$, $A_{128\times64}$ and $C_{64\times128}$ satisfied by Theorem 5.5.2 or Corollary 5.5.4.

To store a small amount of memory for S, we get the huge quasigroup of order 2^{2^k}. The complexity of this construction is $\mathcal{O}(log(\log n))$, since $n = 2^{2^k}$.

5.7 Associative condition on quasigroups obtained by XS-circuits

In quasigroup $(Q, *)$, it must be shown that knowledge of any two of x, y, z in Q, then

$$x * y = z$$

specifies the third uniquely.
Suppose that $Q = (\mathbb{F}_2^m)^n$, $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$ and $z = (z_1, \ldots, z_n) \in (\mathbb{F}_2^m)^n$. Then the elements of quasigroup (i.e., $* : (\mathbb{F}_2^m)^n \times (\mathbb{F}_2^m)^n \to (\mathbb{F}_2^m)^n$) obtained by XS-circuit $(a, b, c|S)$ as complete mapping permutation is written as:

$$\begin{aligned}(z_1, \ldots, z_n) &= (\sum_{i\in[n]}(x_i + y_i)b_{i1}, \ldots, \sum_{i\in[n]}(x_i + y_i)b_{in}) + (\sum_{i\in[r]} s_i c_{i1}, \ldots, \\ &\sum_{i\in[r]} s_i c_{in}) + (y_1, \ldots, y_n) \\ &= (\sum_{i\in[n]}(x_i + y_i)b_{i1} + \sum_{i\in[r]} s_i c_{i1} + y_1, \ldots, \sum_{i\in[n]}(x_i + y_i)b_{in} + \\ &\sum_{i\in[r]} s_i c_{in} + y_n),\end{aligned}$$

where $(s_1, s_2, \ldots, s_r) = S(\sum_{i\in[n]}(x_i + y_i)a_{i1}, \sum_{i\in[n]}(x_i + y_i)a_{i2}, \ldots, \sum_{i\in[n]}(x_i + y_i)a_{ir})$.

Associative axiom:

$$(x * y) * z = x * (y * z).$$

First, we demostrate the associative condition for L.H.S., let $p = (p_1, \ldots, p_n) \in (\mathbb{F}_2)^n$ be the output of L.H.S.

$$\begin{aligned}(p_1, \ldots, p_n) = (&\sum_{i\in[n]}(x_i + y_i)b_{i1} + \sum_{i\in[r]} s_i c_{i1} + y_1, \ldots, \sum_{i\in[n]}(x_i + y_i)b_{in} + \\ &\sum_{i\in[r]} s_i c_{in} + y_n) * (z_1, \ldots, z_n)\end{aligned}$$

$$\begin{aligned}i.e., \quad (p_1, \ldots, p_n) = (&\sum_{i\in[n]}(u_i + z_i)b_{i1} + \sum_{i\in[r]} s_i^{(1)} c_{i1} + z_1, \ldots, \sum_{i\in[n]}(u_i + z_i)b_{in} + \\ &\sum_{i\in[r]} s_i^{(1)} c_{in} + u_n),\end{aligned}$$

where $(u_1, u_2, \ldots, u_r) = (\sum_{i\in[n]}(x_i + y_i)b_{i1} + \sum_{i\in[r]} s_i c_{i1} + y_1, \ldots, \sum_{i\in[n]}(x_i + y_i)b_{in} + \sum_{i\in[r]} s_i c_{in} + y_n)$ and $(s_1^{(1)}, s_2^{(1)}, \ldots, s_r^{(1)}) = S(\sum_{i\in[n]}(u_i + z_i)a_{i1}, \sum_{i\in[n]}(u_i + z_i)a_{i2}, \ldots, \sum_{i\in[n]}(u_i + z_i)a_{ir})$. Similarly, we demostrate the associative condition for R.H.S., let $q = (q_1, \ldots, q_n) \in (\mathbb{F}_2)^n$ be the output of R.H.S.

$$\begin{aligned}(q_1, \ldots, q_n) = (x_1, \ldots, x_n) * (&\sum_{i\in[n]}(y_i + z_i)b_{i1} + \sum_{i\in[r]} s_i^{(2)} c_{i1} + z_1, \ldots, \sum_{i\in[n]}(y_i + z_i)b_{in} + \\ &\sum_{i\in[r]} s_i^{(2)} c_{in} + z_n)\end{aligned}$$

$$\begin{aligned}i.e., \quad (q_1, \ldots, q_n) = (&\sum_{i\in[n]}(x_i + v_i)b_{i1} + \sum_{i\in[r]} s_i^{(3)} c_{i1} + v_1, \ldots, \sum_{i\in[n]}(x_i + v_i)b_{in} + \\ &\sum_{i\in[r]} s_i^{(3)} c_{in} + v_n).\end{aligned}$$

where $(s_1^{(2)}, s_2^{(2)}, \ldots, s_r^{(2)}) = S(\sum_{i\in[n]}(y_i + z_i)a_{i1}, \sum_{i\in[n]}(y_i + z_i)a_{i2}, \ldots, \sum_{i\in[n]}(y_i + z_i)a_{ir})$, $(v_1, v_2, \ldots, v_r) = (\sum_{i\in[n]}(y_i + z_i)b_{i1} + \sum_{i\in[r]} s_i^{(2)} c_{i1} + y_1, \ldots, \sum_{i\in[n]}(y_i + z_i)b_{in} + \sum_{i\in[r]} s_i^{(2)} c_{in} + y_n)$ and $(s_1^{(3)}, s_2^{(3)}, \ldots, s_r^{(3)}) = S(\sum_{i\in[n]}(y_i + z_i)a_{i1}, \sum_{i\in[n]}(y_i + z_i)a_{i2}, \ldots, \sum_{i\in[n]}(y_i + z_i)a_{ir})$. It can be checked that the quasigroup $(Q, *)$ is associative if and only if the following equality is satisfied in $((\mathbb{F}_2^m)^n, \oplus_n)$

$$(p_1, \ldots, p_n) = (q_1, \ldots, q_n). \tag{5.7.1}$$

This equation shows that the obtained quasigroups is highly non-associative, since by Theorems 5.3.1 and 5.3.3, Corollaries 5.3.5 and 5.3.7 function S on $\mathbb{F}_2^m$ and a, c in $\mathbb{F}_2^n$ can hardly

satisfies the Equation (5.7.1) for given elements x, y, z in Q. Among those quasigroups which one have minimum associative triples for particular S, a and c to be estimated by Equation (5.7.1). In Chapter 3, we solved similar equations for diiferent kinds of permutations, i.e., linear permutations, quadratic permutations, APN permutations, Differentially 4-uniform permutations and Differentially δ-uniform permutations and get the counts of associative triples.

Chapter 6

Conclusions

6.1 Conclusion

In this thesis, we have studied quasigroups with minimum number of associative triples and find associative index of some implemented quasigroups which are derived from Feistel function and permutation over finite fields. We futher evolved quasigroups with low associative triples by Genetic algorithms. Quasigroups are represented as vectorial Boolean function, since each coordinate function of a vectorial Boolean function is a Boolean function. We also evolved balanced Boolean function by simulated annealing with profile (n, d, nl, ac), i.e., n variables Boolean function with algebraic degree d, nonlinearity nl and autocorrelation ac.

We evolve balanced Boolean function with profile $(8, 7, 114, 32)$ which is equivalent to random plus hill-climb algorithm result [31] and Kavut and Yücel's result [73]. Using Genetic algorithm, we further evolve isotopic quasigroups with small order, 4, 5, ..., 10 and also with large order 2^4, 2^5, ..., 2^8 whose associative indeces are relatively less than the square of their order. We propose a new cost function for this evolving.

Markovski and Mileva [104] proved that if $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is bijective then the Feistel network

$$\begin{aligned} F &: \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n \\ F(l, r) &= (r, l + f(r)) \qquad \forall\ (l, r) \in \mathbb{F}_2^n \times \mathbb{F}_2^n\ . \end{aligned}$$

is a complete mapping permutation. They indentified that Feistel network based quasigroup is highly non-associative with respective to the governing equations obtained from

the associativity condition. We solve these equations for linear permutation, quadratic permutation, APN (almost perfect nonlinear) permutations and differentially δ-uniform permutations over $\mathbb{F}_2^n$ and get the counts of associative triples. We see that linear permutations, APN permutations, differentially 4-uniform permutations and differentially δ-uniform permutations over $\mathbb{F}_2^n$ provide the associative index which is equal to the square of quasigroup's order. For quadratic permutation, we get the lower bound is $2|Q|^2$, where $|Q|$ is the order of quasigroup. Later we identify the relation between the cryptographic characteristics, i.e., nonlinearity, differential uniformity and Strict Avalanche Criteria (SAC), of bijective mapping and Feistel network based quasigroup.

Kotzig and Reischer [87] proposed the construction of quasigroups by finite commutative, but not necessarily associative or unitary, ring. We implement this construction by two different permutations over $\mathbb{F}_{2^n}$ and get the counts of associative triples by using linear permutations, affine permutations, quadratic permutations and linear complete mapping permutations over $\mathbb{F}_{2^n}$ which are satisfy the best known upper bound. We further also examine how the cryptographic characteristics, i.e., nonlinearity and differential uniformity, affect the quasigroups and using permutations.

The theory of XS-circuits is proposed by Agievich [2]. Construction of complete mapping permutations by using Feistel network has been proposed by Markovski and Mileva [104] which they used to construct huge quasigroups. We construct complete mapping permutations from functions over finite fields by using XS-circuits and give the counts for particular order. We also construct $\mathcal{K}$-complete mapping permutation which can be used to define uniformly distributed sequences. We also find a recursive constrictions that extend a complete mapping of dimension r to a complete mapping of dimension n, where $r \leq n$.

6.2 Some open problems

There are many open questions of Quasigroups and Boolean function apart from the results given in this thesis. We summarize below some open problems which immediately arise from our study.

- Up to now there has been described no infinite series of quasigroups $(Q, *)$ with order n for which the value of $a(Q)$ would be linear in $|Q| = n$.

- There has been described only one infinite series of quasigroups $(Q, *)$ with order n for which $a(Q) < n^2$, and that was done by Kotzig and Reischer [87]. The other algebraic construction of quasigroups $(Q, *)$ with order n for which $a(Q) < n^2$, is a challenge for us.

- Drápal and Valent [48] analysed that each quasigroup Q that is isotopic to an abelian group G there exist transformations or permutations α, β, γ of G such that

$$\alpha + \beta + \gamma = 0 \text{ and } a(Q) = |\{(x, y, z) \in G^3 : \alpha(x) + \beta(y) + \gamma(z) = 0\}|.$$

  To find the minimum value of $a(Q)$ is an open problem. On the heuristic search point of view it is more suitable for further research.

- Specifically we focus on an open problem for $n = 8$ balanced Boolean function with profile $(8, 5, 118, 16)$.

Bibliography

[1] S. Agievich, *EHE: nonce misuse-resistant message authentication*, IACR Cryptology ePrint Archive, Report 2017: 231.

[2] S. Agievich, *XS-circuits in Block Ciphers*, IACR Cryptology ePrint Archive, Report 2018: 512.

[3] J. A. Álvarez-Cubero and P. J. Zufiria, *Cryptographic criteria on vector boolean functions*, Cryptography and Security in Computing, Dr. Jaydip Sen (Ed.), ISBN: 978-953-51-0179-6, InTech, 2012. `https://www.intechopen.com/books/cryptography-and-security-in-computing/cryptographic-criteria-on-vector-boolean-functions`

[4] J. Andress and S. Winterfeld, *Cyber warfare: techniques, tactics and tools for security practitioners*, Elsevier, 2013.

[5] V. A. Artamonov, S. Chakrabarti, S. Gangopadhyay and S. K. Pal, *On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts*, Quasigroups And Related Systems, vol. 21(2), pp. 117–130, 2013.

[6] R. Asthana, N. Verma and R. Ratan, *Generation of Boolean functions using Genetic Algorithm for cryptographic applications*, In Advance Computing Conference (IACC), 2014 IEEE International, pp. 1361–1366, 2014.

[7] V. Bakeva, V. Dimitrova and M. Kostadinoski, *Pseudo Random Sequence Generators Based on the Parastrophic Quasigroup Transformation*, In ICT Innovations 2014, Springer, Cham, pp. 125–134, 2015.

[8] L. A. Bassalygo and V. A. Zinoviev. *Permutation and complete permutation polynomials*, Finite Fields and Their Applications, vol. 33, pp. 198–211, 2015.

[9] J. C. Bean, *Genetic algorithms and random keys for sequencing and optimization*, Journal on Computing, vol. 6, pp. 154–160, 1994.

[10] V. D. Belousov, *Fundamentals of the Theory of Quasigroups and Loops*, Nauka Moskva, 1967.

[11] T. P. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, *On Almost Perfect Nonlinear Functions Over* $\mathbb{F}_2^n$, IEEE Transactions on Information Theory, vol. 52(9), pp. 4160–4170, 2006.

[12] E. R. Berlekamp and L. R. Welch, *Weight distributions of the cosets of the* $(32, 6)$ *Reed-Muller code*, IEEE Transactions on Information Theory, vol. 18(1), pp. 203–207, 1972.

[13] R. H. Bruck, *Some results in the theory of quasigroups*, Transactions of the American Mathematical Society, vol. 55, pp. 19–52, 1944.

[14] L. Burnett, *Heuristic optimization of Boolean functions and substitution boxes for cryptography*, PhD Dissertation, Queensland University of Technology, 2005.

[15] E. Byres and J. Lowe, *The myths and facts behind cyber security risks for industrial control systems*, In Proceedings of the VDE Kongress, vol. 116, pp. 213–218, 2004.

[16] A. Canteaut, *Lectures Notes on Cryptographic Boolean functions*, Inria, Paris, France, version: March 10, 2016.

[17] A. Canteaut, S. Duval and G. Leurent, *Construction of Lightweight S-Boxes using Feistel and MISTY structures (Full Version)*, Cryptology ePrint Archive, Report 2015/711, 2015.

[18] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes, in Boolean Methods and Models*, Y. Crama and P. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press [Online]. Available: http://www.math.univ-paris13.fr/ carlet/chap-fcts-Bool-corr.pdf, to be published.

[19] C. Carlet, *Vectorial Boolean functions for cryptography*, Boolean models and methods in mathematics, computer science, and engineering, vol. 134, pp. 398–469, 2010.

[20] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes, in Boolean Methods and Models*, Capter of the monograph: Boolean models and methods in mathematics, computer science, and engineering, Yves Crama and Peter L. Hammer (eds.), pp. 257–397, 2010.

[21] C. Carlet, P. Charpin and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Designs Codes Cryptography, vol. 15(2), pp. 125-156, 1998.

[22] C. Carlet, D. K. Dalai, K. C. Gupta and S. Maitra *Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction*, IEEE Transactions Information Theory, vol. 52(7), pp. 3105–3121, 2006.

[23] C. Carlet and S. Mesnager, *A note on Semi-Bent Boolean Functions*, IACR Cryptology ePrint Archive, Report 2010: 436.

[24] G. Carter, E. Dawson and L. Nielsen, *A latin square version of DES*, Proc. Workshop of Selected Areas in Cryptography, Ottawa, Canada, 1995.

[25] A. Cayley, *Desiderata and suggestions: No. 2. the theory of groups: graphical representation*, American Journal of Mathematics, vol. 1(2), pp. 174–176, 1878.

[26] A. Cayley, *On latin squares*, Messenger of Math, vol. 19, pp. 135–137, 1890.

[27] S. Chakrabarti, S. K. Pal and S. Gangopadhyay, *An improved 3–quasigroup based encryption scheme*, `http://proceedings.ictinnovations.org/attachment/paper/53/an-improved-3-quasigroup-based-encryption-scheme.pdf`, pp. 173–184, 2012.

[28] P. Charpin, A. Tietäväinen and V. A. Zinoviev, *On binary cyclic codes with minimum distance $d = 3$*, Problemy Peredachi Informatsii, vol. 33(4), pp. 3–14, 1997.

[29] J. A. Clark and J. L. Jacob, *Two-stage optimisation in the design of Boolean functions*, Australian Conference on Information Security and Privacy (ACISP), pp. 242–254, 2000.

[30] J. A. Clark, J. L. Jacob and S. Stepney, *The design of S-boxes by simulated annealing*, New Generation Computing, vol. 23(3), pp. 219–231, 2005.

[31] J. A. Clark, J. L. Jacob, S. Stepney, S. Maitra and W. Millan, *Evolving Boolean functions satisfying multiple criteria*, INDOCRYPT, vol. 2, pp. 246–259, 2002.

[32] J. Cooper, D. Donovan and J. Seberry, *Secret sharing schemes arising from Latin squares*, Bulletin of the Institute of Combinatorics and its Applications, vol. 4, pp. 33–43, 1994.

[33] T. W. Cusick and P. Stănică, *Cryptograhic Boolean Functions and Applications*, Book, Academic Press, (1^{st} Edition), 2009.

[34] Z. D. Dai, S. W. Golomb and G. Gong, *Generating all linear orthomorphism without repetition*, Discrete Mathematics, vol. 205, pp. 47–55, 1999.

[35] D. K. Dalai, *On 3-to-1 and Power APN S-Boxes*, SETA, pp. 377–389, 2008.

[36] D. K. Dalai and S. Maitra, *Balanced Boolean Functions with (more than) Maximum Algebraic Immunity*, IACR Cryptology ePrint Archive, Report 2006: 434.

[37] J. Dénes and T. Dénes, *Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack*, Quasigroups And Related Systems, vol. 8, pp. 7–14, 2001.

[38] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Akadémiai Kiado, Budapest, 1974.

[39] J. Dénes and P. Petroczki, *Digitális titkosító kommunikációs rend-szer, (A Digital Encrypting Communication System)*, Hungarian patent No. 201437 A.

[40] V. Dimitrova, *Quasigroup processed strings, their Boolean presentation and application in cryptography and coding theory*, Doctoral dissertation, University Sts. Cyril and Methodius, Skopje, 2010.

[41] C. Ding, G. Xiao and W. Shan, *The Stability Theory of Stream Ciphers*, Springer Science & Business Media, vol. 561, 1991.

[42] H. Dobbertin, *Construction of bent functions and balanced functions with hign non-linearity*, In Fast Software Encryption, 1994 Leuven Workshop, Lecture Notes in Computer Science, Springer-Verlag, Berlin, vol. 1008, pp. 61–74, 1994.

[43] H. Dobbertin, *Almost perfect nonlinear power functions on GF(2^n): A new class of n is divisible by* 5, In Proc. Finite Fields and Applications $Fq5$. Springer, Berlin, Verlag, pp. 113–121, 2000.

[44] A. Drápal, *On quasigroup rich in associative triples*, Discrete Mathematics, vol. 44(3), pp. 251–265, 1983.

[45] A. Drápal, J. Ježek and T. Kepka, *Groupoids and the associative law IX. (Associative triples in some classes of groupoids)*, Acta Universitatis Carolinae. Mathematica et Physica, vol. 38(1), pp. 39–52, 1997.

[46] A. Drápel and T. Kepka, *A note on the number of associative triples in quasigroups isotopic to groups*, Commentationes Mathematicae Universitatis Carolinae, vol. 22(4), pp. 735–743, 1981.

[47] A. Drápal and T. Kepka , *Sets of Associative Triples*, European Journal of Combinatorics, vol. 6(3), pp. 227–231, 1985.

[48] A. Drápal and V. Valent, *Few associative triples, isotopisms and groups*, Designs Codes Cryptography, vol. 86(3), pp. 555–568, 2018.

[49] J. Dvorsky, E. Ochodkova and V. Snašel, *Hash function based on quasigroups*, (Czech), Proc. of Mikulášska kryptobesídká, Praha, pp. 27–36, 2001.

[50] J. Dvorsky, E. Ochodkova and V. Snašel, *Hash function based on large quasigroups*, (Czech), Proc. of Velikonocní i kryptologie, Brno, pp. 1–8, 2002.

[51] L. Euler, *Recherches sur une nouvel le especе de quarres magiques*, Zeeuwsch Genootschao, 1782.

[52] L. Euler, *De quadratis magicis*, Commentationes arithmeticae, vol. 2, pp. 593-602, 1849.

[53] L. Euler, *On magic squares*, arXiv preprint math/0408230, (Translated by Jordan Bell in 2004).

[54] J. C. Faugere, R. S. Ødegård, L. Perret and D. Gligoroski, *Analysis of the MQQ public key cryptosystem*, International Conference on Cryptology and Network Security (CANS), vol. 6467, pp. 169–183, 2010.

[55] H. Feistel, *Cryptography and computer privacy*, Scientific American, vol. 228(5), pp. 15–23, 1973.

[56] É. Galois and P. M. Neumann, *The mathematical writings of Évariste Galois*, European mathematical society, vol. 6, 2011.

[57] S. Gangopadhyay, A. Joshi, G. Leander and R. K. Sharma, *A new construction of bent functions based on $\mathbb{Z}$-bent functions*, Designs Codes Cryptography, vol. 66(1-3), pp. 243–256, 2013.

[58] S. Gangopadhyay, E. Pasalic and P. Stănică, *A Note on Generalized Bent Criteria for Boolean Functions*, IEEE Transactions on Information Theory, vol. 59, pp. 3233–3236, 2013.

[59] S. Gangopadhyay, E. Pasalic, P. Stănică and S. Datta, *A note on non-splitting Z-bent functions*, Information Processing Letters, vol. 121, pp. 1–5, 2017.

[60] S. Gangopadhyay, B. Singh and V. Vetrivel, *Investigations on cubic rotation symmetric bent functions*, Electronic Notes in Discrete Mathematics, vol. 56, pp. 15–19, 2016.

[61] D. Gligoroski, V. Dimitrova and S. Markovski, *Quasigroups as Boolean functions, their equation systems and Gröbner bases*, Gröbner Bases, Coding, and Cryptography, pp. 415–420, 2009.

[62] D. Gligoroski and M. E. G. Moe, *On deviations of the AES S-box when represented as vector valued Boolean function*, International Journal of Computer Science and Network Security, vol. 7(4), pp. 156–163, 2007.

[63] F. Gologlu, *Almost Bent and Almost Perfect Nonlinear Functions, Exponential Sums, Geometries ans Sequences*, PhD Dissertation, University of Magdeburg, 2009.

[64] O. Grošek and P. Horák, *On quasigroups with few associative triples*, Designs Codes Cryptography, vol. 64(1), pp. 221–227, 2012.

[65] M. Hall and L. J. Paige, *Complete mappings of finite groups*, Pacific Journal of Mathematics, vol. 5(4), pp. 541–549, 1955.

[66] D. Hermawanto, *Genetic algorithm for solving simple mathematical equality problem*, arXiv preprint arXiv:1308.4675, 2013.

[67] I. N. Herstein, *Topics in Algebra*, Book, Wiley, (2^{rd} Edition), 1975.

[68] X. D. Hou, *On the Norm and Covering Radius of First-Order Reed-Muller Codes*, IEEE Transactions on Information Theory, vol. 43(3), pp. 1025–1027, 1997.

[69] S. G. Ibragimov, *On forgotten works of Ernst Schr oder lying between algebra and logic (Russian)*, Istoriko-Matematicheskie Issledovaniya, vol. 17, pp. 247–258, 1966.

[70] L. Janczewski, *Cyber warfare and cyber terrorism*, IGI Global, 2007.

[71] J. Ježek and T. Kepka, *Notes on the number of associative triples*, Acta Universitatis Carolinae. Mathematica et Physica, vol. 31(1), pp. 15–19, 1990.

[72] S. Kavut, S. Maitra, S. Sarkar and M. D. Yücel, *Enumeration of–9 variable rotation symmetric Boolean functions having nonlinearity ¿ 240*, In: Proceedings of the INDOCRYPT'06, LNCS, Springer, vol. 4329, pp. 266–279, 2006.

[73] S. Kavut and M. D. Yücel, *Improved cost function in the design of Boolean functions satisfying multiple criteria*, In International Conference on Cryptology in India, pp. 121–134, 2003.

[74] S. Kavut and M. D. Yücel, *Generalized Rotation Symmetric and Dihedral Symmetric Boolean Functions–9 variable Boolean Functions with Nonlinearity 242*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp. 321–329, 2007.

[75] A. D. Keedwell, *Some applications of non-associative algebraic systems in cryptology*, Pure Mathematics and Applications, vol. 12(2), pp. 147–195, 2001.

[76] A. D. Keedwell and J. Dénes, *Latin squares and their applications*, Book, North Holland, (2^{nd} Edition), 2015.

[77] T. Kepka, *A note on associative triples of elements in cancellation groupoids*, Commentationes Mathematicae Universitatis Carolinae, vol. 21(3), pp. 479–487, 1980.

[78] T. Kepka, *Notes on associative triples of elements in commutative groupoids*, Acta Universitatis Carolinae, Mathematica et Physica, vol. 22(2), pp. 39–47, 1981.

[79] T. Kepka, *A note on the number of associative triples in finite commutative Moufang loops*, Commentationes Mathematicae Universitatis Carolinae, vol. 22(4), pp. 745–753, 1981.

[80] T. Kepka and J. Kratochvíl, *Graphs and associative triples in quasitrivial groupoids*, Commentationes Mathematicae Universitatis Carolinae, vol. 25(4), pp. 679–687, 1984.

[81] T. Kepka and M. Trch, *Groupoids and the associative law I. (Associative triples)*, Acta Universitatis Carolinae. Mathematica et Physica, vol. 33(1), pp. 69–86, 1992.

[82] T. Kepka and M. Trch, *Groupoids and the associative law II. (Groupoids with small semigroup distance)*, Acta Universitatis Carolinae. Mathematica et Physica, vol. 34(1), pp. 67–83, 1993.

[83] K. Kim, T. Matsumoto and H. Imai, *A recursive construction method of S-boxes satisfying strict avalanche criterion*, In Conference on the Theory and Application of Cryptography, Springer, Berlin, Heidelberg, pp. 565–574, 1990.

[84] S. Kirkpatrick, C. D. Gelatt and M. P. Vecchi, *Optimization by simulated annealing*, Science, vol. 220(4598), pp. 671–680, 1983.

[85] M. Kontak and J. Szmidt, *Nonlinearity of Round Function*, Control and Cybernatics, vol. 36(4), pp. 1037–1044, 2007.

[86] C. Kościelny, *Generating quasigroups for cryptograhic applications*, International Journal of Applied Mathematics and Computer Science, vol. 12(4), pp. 559–570, 2002.

[87] A. Kotzig and C. Reischer, *Associativity index of finite quasigroup*, Glasnik Matematički, vol. 18(38), pp. 243–253, 1983.

[88] M. Krancer, *The Biggest Cybersecurity Threat: The Energy Sector*, 2015. `http://www.forbes.com/sites/michaelkrancer/2015/11/04/the-biggest-cybersecurity-threat-the-energy-sector/`

[89] A. Krapež, *An application of quasigroups in cryptology*, Mathematica Macedonica, vol. 8, pp. 47–52, 2010.

[90] Y. Kumar, P. R. Mishra, N. R. Pillai and R. K. Sharma, *Affine equivalence and non-linearity of permutations over* $\mathbb{Z}_n$, Applicable Algebra in Engineering, Communication and Computing, vol. 28(3), pp. 257–279, 2017.

[91] M. Kumar, S. K. Pal and A. Panigrahi, *On the Security of Extended Generalized Feistel Networks*, IACR Cryptology ePrint Archive, Report 2015: 734.

[92] Y. Laigle-Chapuy, *A Note on a Class of Quadratic Permutations over* $\mathbb{F}_{2^n}$, In International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, pp. 130–137, 2007.

[93] Y. Laigle-Chapuy, *Polynômes de permutation et application en cryptographie - Cryptanalyse de registres combinés. HAL Id: tel-00438765. https://tel.archives-ouvertes.fr/tel-00438765.*

[94] G. Leander and A. Poschmann, *On the classification of 4 bit S-boxes*, Arithmetic of Finite Fields, pp. 159–176, 2007.

[95] Y. Li and M. Wang, *Constructing S-boxes for lightweight cryptography with Feistel structure*, In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 127–146, 2014.

[96] R. Lidl and H. Niederreiter, *Finite Fields (Encyclopedia Of Mathematics And Its Applications)*, Book, Addision - Wesley Publication, (2^{nd} Edition), 2008.

[97] C. H. Lim, *CRYPTON: A new 128-bit block cipher*, AES submission, 1998.

[98] S. Maitra, *Highly nonlinear balanced Boolean functions with very good autocorrelation property*, In Workshop on Coding and Cryptography - WCC 2001, Paris, 2001. Electronic Notes in Discrete Mathematics, vol. 6, Elesvier Science, 2001.

[99] B. Mandal, B. Singh, S. Maitra, S. Gangopadhyay and V. Vetrivel, *On non-existence of bent-negabent rotation symmetric Boolean functions*, Discrete Applied Mathematics, vol. 236, pp. 1–6, 2018.

[100] M. S. Mandi, *Almost Perfect Nonlinear functions and related combinatorial structures*, A Thesis, 2005.

[101] S. Markovski, *Quasigroup string processing and applications in cryptography*, Proceedings of the Conference MII 2003, Thessaloniki, Greece, pp. 278–290, 2003.

[102] S. Markovski, *Design of crypto primitives based on quasigroups*, Quasigroups And Related Systems, vol. 23(1), pp. 41–90, 2015.

[103] S. Markovski, D. Gligoroski and V. Bakeva, *Quasigroup and hash functions*, Proc. of the 6th ICDMA, Bansko, pp. 43–50, 2001.

[104] S. Markovski and A. Mileva, *Generating huge quasigroups from small non-linear bijections via extended Feistel function*, Quasigroups And Related Systems, vol. 17(1), pp. 91–106, 2009.

[105] J. L. Massey, *Shift-register synthesis and BCH decoding*, IEEE Transactions on Information Theory, vol. 15(1), pp. 122-127, 1969.

[106] M. Matsui, *Linear cryptanalysis method for DES cipher*, In: Proceedings of the EUROCRYPT'93, LNCS, Springer, vol. 765, pp. 386–397, 1994.

[107] M. Matsui, *New structure of block ciphers with provable security against differential and linear cryptanalysis*, In Fast Software Encryption, Springer, Berlin, Heidelberg, pp. 205–218, 1996.

[108] R. Mattews, *Permutation properties of the polynomials* $1 + x + x^2 + \ldots + x^k$ *over a finite field*, Proceedings of the American Mathematical Society, vol. 120(1), pp. 47–51, 1994.

[109] W. Meier and O. Staffelbach, *Fast correlation attacks on stream ciphers*, Journal of Cryptology, vol. 1(3), pp. 159–176, 1989.

[110] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Crptography*, Book, CRC Press, 2001.

[111] S. Mesnager, *Bent Functions, Fundamentals and Results*, Springer, 2016.

[112] K. A. Meyer, *A new message authentication code based on the non-associativity of quasigroups*, PhD Thesis, Lowa State University, 2006.

[113] H. Mihajloska and D. Gligoroski, *Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4*, The Sixth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE, 2012.

[114] M. J. Mihaljevič, S. Gangopadhyay, G. Paul and H. Imai, *Internal state recovery of keystream generator LILI-128 based on a novel weakness of the employed Boolean function*, Information Processing Letters, vol. 112, pp. 805–810, 2012.

[115] M. J. Mihaljevič, S. Gangopadhyay, G. Paul and H. Imai, *Generic cryptographic weakness of k-normal Boolean functions in certain stream ciphers and cryptanalysis of grain-128*, Periodica Mathematica Hungarica, vol. 65(2), pp. 205–227, 2012.

[116] A. Mileva, *Cryptographic Primitives with Quasigroup Transformations*, PhD Dissertation, University Sts. Cyril and Methodius, Skopje, 2010.

[117] A. Mileva, *Analysis of some Quasigroup transformations as Boolean Functions*, Mathematica Balkanica, vol. 26(3-4), pp. 359–368, 2012.

[118] A. Mileva and S. Markovski, *Shapeless quasigroups derived by Feistel orthomorphisms*, Glasnik Mathematički, vol. 47(2), pp. 333–349, 2012.

[119] A. Mileva and S. Markovski, *Quasigroup representation of some feistel and generalized feistel ciphers*, In ICT Innovations 2012, Springer, Berlin, Heidelberg, pp. 161–171, 2013.

[120] W. Millan, A. Clark and E. Dawson, *Smart hill climbing finds better boolean functions*, Workshop on Selected Areas in Cryptology, Workshop Record, pp. 50–63, 1997.

[121] W. Millan, A. Clark and E. Dawson, *An effective genetic algorithm for finding highly nonlinear Boolean functions*, International Conference on Information and Communications Security, vol. 1334, pp. 149–158, 1997.

[122] W. Millan, A. Clark and E. Dawson, *Heuristic Design of Cryptographically Strong Balanced Boolean Functions*, In Advances in Cryptology EUROCRYPT'98, Lecture Notes in Computer Science, Springer-Verlag, vol. 1403, pp. 489–499, 1998.

[123] L. Mittenthal, *Block Substitutions Using Orthomorphic Mappings*, Advances in Applied Mathematics, vol. 16, pp. 59–71, 1995.

[124] R. A. Mollin and C. Small, *On permutation polynomials over finite field*, International Journal of Mathematics and Mathematical Sciences, vol. 10(3), pp. 535–543, 1987.

[125] R. Moufang, *Zur struktur von alternativk ŏrpern*, Mathematische Annalen, vol. 110(1), pp. 416–430, 1935.

[126] M. Niemenmaa and T. Kepka, *On a general associative law in groupoids*, Monatshefte für Mathematik, vol. 113, pp. 51–57, 1992.

[127] D. A. Norton, *A note on associativity*, Pacific Journal Of Mathematics, vol. 10(2), pp. 591–595, 1960.

[128] K. Nyberg, *Perfect nonlinear S-boxes*, Advances in Cryptology EUROCRYPT-91, Springer, Berlin, Heidelberg, pp. 378–386, 1991.

[129] K. Nyberg, *Differentially uniform mappings for cryptography*, Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, pp. 55–64, 1993.

[130] K. Nyberg, *S-boxes and Round Functions with Controlled Linearity and Diffrential Uniformity*, International Workshop on Fast Software Encryption, FSE-1994, pp. 111–130, 1994.

[131] K. Nyberg and L. R. Knudsen, *Provable security against a differential attack*, Journal of Cryptology, vol. 8(1), pp. 27–37, 1995.

[132] S. K. Pal, D. Bhardwaj, R. Kumar and V. Bhatia, *A New Cryptographic Hash Function based on Latin Squares and Non-linear Transformations*, IEEE International Advance Computing Conference (IACC 2009), pp. 882–867, 2009.

[133] S. K. Pal and Sumitra, *Development of Efficient Algorithms for Quasigroup Generation & Encryption*, IEEE International Advance Computing Conference (IACC 2009), pp. 940–945, 2009.

[134] E. Pasalic, A. Muratovič-Ribič, S. Hodzič and S. Gangopadhyay, *On derivatives of polynomials over finite fields through integration*, Discrete Applied Mathematics, vol. 217, pp. 294–303, 2017.

[135] N. J. Patterson and D. H. Wiedemann, *The covering radius of the* $(2^15, 16)$ *Reed-Muller code is at least 16276*, IEEE Transactions on Information Theory, IT-29(3), pp. 354–356, 1983 (see correction IT-36(2), pp. 443, 1990).

[136] J. Pieprzyk and C. X. Qu, *Fast hashing and rotation-symmetric functions*, Journal of Universal Computer Science, vol. 5(1), pp. 20–31, 1999.

[137] K. Pommerening, *Fourier Analysis of Boolean Maps*, A Tutorial, J. Gutenberg University, 2005.

[138] B. Preneel, *The state of cryptographic hash functions*, In School organized by the European Educational Forum, Springer, Berlin, Heidelberg, pp. 158–182, 1998.

[139] B. Preneel, *Analysis and Design of Cryptographic Hash Functions*, A Thesis, 2003.

[140] R. L. Rivest, *Permutation polynomials modulo* 2^w, Finite Fields and Their Applications, vol. 7(2), pp. 287–292, 2001.

[141] S. Rønjom and T. Hellseeth, *A new attack on filter generator*, IEEE Transactions on Information Theory, vol. 53(5), pp. 1752-1758, 2007.

[142] O. S. Rothaus, *On bent functions*, Journal of Combinatorial Theory, Series A, vol. 20(3), pp. 300–305, 1976.

[143] A. Sade, *Quasigroups automorphes par le groupe cylique*, Canadian Journal of Mathematics, vol. 9, pp. 321–335, 1957.

[144] P. Sarkar and S. Maitra, *Construction of nonlinear Boolean functions with important cryptographic properties*, In: Proceedings of the EUROCRYPT'00, LNCS, Springer, vol. 1870, pp. 485–506, 2000.

[145] P. Sarkar and S. Maitra, *Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes*, Theory of Computing Systems, vol. 35(1), pp. 39–57, 2002.

[146] M. V. K. Satti, *Quasi Group based Crypto-System*, Master Thesis, Louisiana State University, 2007.

[147] M. V. K. Satti, *A Quasigroup Based Cryptographic System*, A Thesis, 2007.

[148] V. A. Shcherbacov, *Elements of Quasigroup Theory and Applications*, Book, ChapMan & Hall/CRC Press, 2017.

[149] R. P. Singh and S. Maity, *Permutation Polynomials modulo p^n*, Cryptology ePrint Archive, 2009/393, 2009.

[150] I. Slaminková and M. Vojvoda, *Cryptanalysis of a hash function based on isotopy of quasigroups*, Tatra Mountains Mathematical Publications, vol. 45(1), pp. 137–149, 2010.

[151] J. D. H. Smith, *An Introduction to Quasigroups and Their Representations*, Book, ChapMan & Hall/CRC Press, (1^{st} Edition), 2006.

[152] V. Snášel, A. Abraham and J. Dvorský, *Searching for quasigroups for hash functions with genetic algorithms*, Nature & Biologically Inspired Computing, NaBIC 2009. World Congress on IEEE, pp. 367–372, 2009.

[153] V. Snášel, A. Abraham, J. Dvorsky, P. Krőmer and J. Platoš, *Hash function based on large quasigroups*, Computational Science–ICCS, pp. 521–529, 2009.

[154] V. Snášel, J. Dvorský, E. Ochodková, P. Krömer, J. Platoš and A. Abraham, *Evolving quasigroups by genetic algorithms*, In proceedings of the DATESO 2010 workshop, pp. 108–117, 2010.

[155] L. V. Snyder and M. S. Daskin, *A random-key genetic algorithm for the generalized traveling salesman problem*, European Journal of Operational Research, vol. 174(1), pp. 38–53, 2006.

[156] W. M. Spears and K. A. De Jong, *On the virtues of parameterized uniform crossover*, Naval Research Lab Washington DC, 1991.

[157] P. Stănică, S. Maitra and J. A. Clark, *Results on rotation symmetric bent and correlation immune Boolean function*, In International Workshop on Fast Software Encryption, pp. 161–177, 2004.

[158] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. Kar-Gangopadhyay and S. Maitra, *Investigations on Bent Negabent Functions via the Nega-Hadamard Transform*, IEEE Transactions on Information Theory, vol. 58(6), pp. 4064–4072, 2012.

[159] D. R. Stinson, *Cryptography: Theory and Practice*, Book, ChapMan & Hall/CRC Press, (3^{rd} Edition), 2006.

[160] M. Sýs, *Latin squares in cryptography*, PhD Dissertation, 2009.

[161] Y. Tan, G. Gong and B. Zhu, *Enhanced criteria on differential uniformity and nonlinearity of cryptographically significant functions*, Cryptography and Communications, vol. 8(2), pp. 291–311, 2016.

[162] Z. Tu, X. Zeng and L. Hu, *Several classes of complete permutation polynomials*, Finite Fields and Their Applications, vol. 25, pp. 182–193, 2014.

[163] V. Valent, *Quasigroups with few associative triples*, Bachelor Thesis, 2016.

[164] M. Vojvoda, *Cryptanalysis of one hash function based on quasigroup*, Tatra Mountains Mathematical Publications, vol. 29(173), pp. 173–181, 2004.

[165] United States Department of Energy, *Cybersecurity*, 2016. `http://www.energy.gov/oe/services/cybersecurity`.

[166] A. Wagner, *On the associative law of groups*, Rend. Mat. e Appl., vol. 21, pp. 60–76, 1962.

[167] A. Winterhof, *Generalizations of complete mappings of finite fields and some applications*, Journal of Symbolic Computation, vol. 64, pp. 42–52, 2014.

[168] Y. Yu, M. Wang and Y. Li, *Constructing differential 4-uniform permutations from know ones*, Chinese Journal of Electronics, vol. 22(3), pp. 495–499, 2013.

[169] K. Zetter, *The Biggest Security Threats Well Face in 2016*, 2016. `http://www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/`

[170] Y. Zheng and X. M. Zhang, *Improved upper bound on the nonlinearity of high order correlation immune functions*, In Selected Areas in Cryptography - SAC 2000, Lecture Notes in Computer Science, Springer-Verlag, vol. 2012, pp. 264–274, 2000.