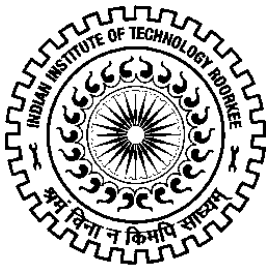
A STUDY OF SOME CRYPTOGRAPHICALLY SIGNIFICANT BOOLEAN FUNCTIONS AND THEIR GENERALIZATIONS

Ph. D. THESIS

by

DEEP SINGH



DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE- 247 667 (INDIA)
JULY, 2014

A STUDY OF SOME CRYPTOGRAPHICALLY SIGNIFICANT BOOLEAN FUNCTIONS AND THEIR GENERALIZATIONS

A THESIS

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

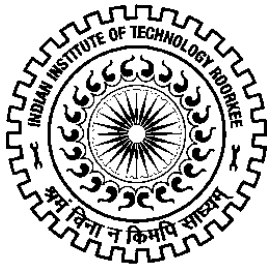
of

DOCTOR OF PHILOSOPHY
in

MATHEMATICS

by

DEEP SINGH



DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE- 247 667 (INDIA)
JULY, 2014

INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis entitled "**A STUDY OF SOME CRYPTOGRAPHICALLY SIGNIFICANT BOOLEAN FUNCTIONS AND THEIR GENERALIZATIONS**" 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 July, 2009 to July, 2014 under the supervision of Dr. Maheshanand, Assistant Professor, Department of Mathematics, 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 Institute.

(DEEP SINGH)

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

(Maheshanand)
Supervisor

Date: July , 2014

The Ph.D. Viva-Voce Examination of **Mr. Deep Singh,** Research Scholar, has been held on……. .

Supervisor Chairman, SRC Signature of External Examiner

Head of the Department/ Chairman ODC

Abstract

This thesis presents an investigation on some cryptographic properties of Boolean functions, q-ary functions due to Kumar et al. (1985) defined from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, and the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. Our aim is to identify and to construct cryptographically significant functions which show good behavior with respect to some important cryptographic criteria including balancedness, resiliency, nonlinearity, crosscorrelation, autocorrelation and global avalanche characteristics (GAC). We identify some classes of Boolean functions with high nonlinearity which show good behavior with respect to second order nonlinearity. We investigate several properties of q-ary functions in terms of their Walsh-Hadamard transform (WHT) and crosscorrelation spectra. The crosscorrelation of a subclass of Maiorana-McFarland (MM) type q-ary bent functions is obtained. Some constructions of q-ary balanced functions which have good GAC measured in terms of the indicators: the sum-of-squares-of-modulus indicator (SSMI) and the modulus indicator (MI), and which satisfy propagation criteria (PC), are presented. We present a new generalization of negabent functions by considering the functions $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. We investigate several properties of generalized negabent functions and provide some examples of such functions.

In 2008 Carlet has introduced a recursive method for the computation of lower bounds of higher order nonlinearities of Boolean functions. Using Carlet's recursive approach we identify some classes of highly nonlinear Boolean functions whose lower bounds on second order nonlinearities are better than some previously known general bounds.

We have considered the problem of computing lower bounds on second order nonlinearities of cubic monomial functions of the form (i) $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$, where $n = 3r,\ 5r$ and $\lambda \in \mathbb{Z}_{2^n} \setminus \{0\}$, (ii) $f(x) = tr_1^n(\lambda x^{2^{2r}+2^r+1})$, where $n = 3r$ and $\lambda \in \mathbb{Z}_{2^r} \setminus \{0\}$. Boolean functions in these classes possess no affine derivatives. The general lower bounds on second

order nonlinearities of the cubic Boolean functions which have no affine derivative have been deduced by Carlet [15]. The bounds obtained by us for the above classes of functions are better than the general bounds obtained by Carlet [15] and the bounds of some other classes of Boolean functions which are recently studied [50, 53, 147]. Further, we obtain lower bounds on second order nonlinearities for some classes of cubic Boolean functions based on secondary constructions.

Gao et al. [52] have provided a method for the construction of plateaued resilient functions with disjoint spectra. Using this approach, we provide some new constructions of highly nonlinear resilient Boolean functions on large number of variables with disjoint spectra by concatenating disjoint spectra resilient functions on small number of variables. In some cases the nonlinearity bounds of the constructed functions are better than the bounds obtained in [52].

Several results on q-ary functions in terms of their WHT and crosscorrelation spectra are presented. We obtain the crosscorrelation of a subclass of Maiorana-McFarland (MM) type q-ary bent functions. A characterization of quaternary (4-ary) bent functions on $n+1$ variables in terms of their subfunctions on n variables is presented. We slightly generalize a result of Tokareva [151] by proving that the direct sum of two q-ary bent functions f_1 and f_2 is a q-ary bent function if and only if f_1 and f_2 both are q-ary bent. Analogous to the indicators, the *sum-of-squares indicator* and the *absolute indicator* in Boolean case, we define two similar indicators: the *sum-of-squares-of-modulus indicator* (SSMI) $\sigma_{f,g}$ and the *modulus indicator* (MI) $\triangle_{f,g}$ to measure the global avalanche characteristics (GAC) of two q-ary functions. We study q-ary functions in terms of these two indicators and derive some lower and upper bounds on these indicators. Also, we provide some constructions of balanced quaternary functions with high nonlinearity under the Lee metric.

Further, we present construction of two classes of q-ary balanced functions which have good GAC measured in terms of two indicators, the SSMI and the MI, and satisfy PC. It is shown that the cryptographic criteria the SSMI, MI, and PC of q-ary functions are invariant under affine transformations. Also, we give a construction of q-ary s-plateaued functions and obtain their SSMI. We provide a relationship between the autocorrelation spectrum of a cubic Boolean function and the dimension of the kernel of the bilinear form associated

with its derivative. Using this result, we identify several classes of cubic semi-bent Boolean functions which have good bounds on their SSMI and MI, and hence show good behavior with respect to the GAC.

We present a method for the construction of ternary functions on $(n+1)$-variables by using decomposition functions f_1, f_2, f_3 on n-variables, and investigate a link between the SSMI of an $(n+1)$-variable ternary function f and the SSMI of their n-variable decomposition functions f_1, f_2, f_3. Also, we provide a construction of ternary functions with low value of SSMI by using pairwise perfectly uncorrelated m-plateaued ternary functions and modified ternary bent functions. A relationship among the indicators, $\sigma_{f,g}$, σ_f (the SSMI of f) and σ_g of two q-ary functions f and g is obtained. Further, we deduce upper bounds to the indicators the SSMI and the MI of two q-ary functions for the case that one of them is s-plateaued q-ary function.

We propose a new generalization of negabent functions by considering the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. We investigate several properties of generalized nega-Hadamard transform (GNHT) and its behavior on various combinations of functions. Some results describing the properties of generalized negabent functions are presented. We have established a connection between the generalized nega-autocorrelation spectra of functions and their GNHT. A characterization of generalized negabent (for $q = 4$) functions on $n+1$ variables in terms of their subfunctions on n-variables is presented. Further, in this setup, we present several examples of generalized negabent functions for different values of q and n.

List of Publications

Journals

1. Singh, D., Bhaintwal, M. and Singh, B.K.: Constructions of q-ary functions with good global avalanche characteristics, International Journal of Computer Mathematics, 2014, DOI:10.1080/00207160.2014.902940

2. Singh, D., Bhaintwal, M. and Singh, B.K.: Some results on q-ary bent functions, International Journal of Computer Mathematics, Vol. 90(9), pp. 1761–1773, 2013.

3. Singh, D.: Second order nonlinearities of some classes of cubic Boolean functions based on secondary constructions, International Journal of Computer Science and Information Technologies, Vol. 2(2), pp. 786–791, 2011.

Conference

1. Singh, D. and Bhaintwal, M.: On the sum-of-squares-modulus indicator of q-ary functions, In Proc. "International Conference on Advances in Computing, Communications and Informatics" (ICACCI-2013), Aug. 22-25, 2013, Mysore, India, pp. 599–603, 2013, DOI: 10.1109/ICACCI.2013.6637240

2. Singh, D. and Bhaintwal, M.: On second order nonlinearities of two classes of cubic Boolean functions, In Proc. "Heterogeneous Networking for Quality, Reliability, Security and Robustness" (QSHINE-2013), Jan. 11-12, 2013, Greater Noida, India, LNICST, Springer-Verlag Berlin Heidelberg, Vol. 115, pp. 560–567, 2013.

3. Singh, D.: Construction of highly nonlinear plateaued resilient functions with disjoint spectra, In Proc. "International Conference on Mathematical Modelling and Scien-

tific Computation" (ICMMSC-2012), March 16-18, 2012, Gandhigram, India, CCIS, Springer-Verlag Berlin Heidelberg, Vol. 283, pp. 522–529, 2012.

Acknowledgement

Foremost, I humbly and politely bow my head to the almighty God who bestowed upon me an opportunity to do this work and gave me comprehension and strength to accomplish this task successfully. I thank Him for His gracious blessings and spiritual support which always help me to withstand and overcome the difficulties in my life.

I convey my deepest gratitude and reverence to my supervisor **Dr. Maheshanand** for his informed guidance and advice. I am highly thankful for his time, attempt and editing skills. His constant support, encouragement and judicious interventions made this thesis to come into the picture. His patience and willingness to discuss the minutiae of the different obstacles I encountered while executing this work were invaluable. I humbly acknowledge a life time's gratitude to him. No words articulate to acknowledge the didactic guidance rendered by him.

I am thankful to Prof. R. C. Mittal and Prof. Rama Bhargava, the present and the former Head, Department of Mathematics, IIT Roorkee, for providing all the necessary facilities and support to carry out the research work.

I extend my gratitude to Dr. Matthew G. Parker for the fruitful discussion on a research problems. I am also extremely indebted to Dr. D. N. Pandey, Dr. Satish Peddoju and Dr. Uaday Singh for their invaluable advices and inspiration. I wish to thank all the faculty members and non-teaching staff of the Department of Mathematics, IIT Roorkee for their cooperation.

The financial support from National Board for Higher Mathematics (DAE), India to complete the present investigations is highly acknowledged.

I gratefully acknowledge the support provided by Central University of Jammu, Jammu to complete this work.

I express my special thanks to Dr. Manoj Kumar and Dr. Brajesh K. Singh for their constant support and encouragement. My sincere thanks are also due to Mr. and Mrs. Rajesh Patel and my friend Mania who were always helpful to me during this work.

I express my heartfelt gratitude to my highly respectable and adorable parents and my other family members for their unconditional love, support, encouragement and blessings.

Last but not the least, I am extremely grateful to all the friends who helped me directly or indirectly during my research work.

With devotion and profound gratitude, I dedicate this thesis to my family.

Roorkee (Deep Singh)

July , 2014

List of Tables

Contents

Chapter 1

Introduction

Cryptography is a key technology in providing secure transmission of information. It is a branch of science which mainly deals with constructing and analyzing protocols which are related to various aspects of secure communication. Now a days cryptography is at the heart of many techniques used for secure transfer of data, such as web based applications, online government services, online banking, mobile phones, wireless local area networks, ATM etc. Thus, cryptography is associated with the security of the piece of the information being transmitted over the insecure channel. Cryptography helps in providing following four necessary security primitives

- Confidentiality
- Authentication
- Integrity
- Non repudiation

Most of the cryptographic security techniques are based on one or more of these security primitives. These cryptographic primitives are used to design very complex algorithms, known as cryptosystems. Cryptosystem is an algorithm required to implement special types of encryptions and decryptions. There are mainly two types of cryptosystems: symmetric key (private key) and asymmetric key (public key) cryptosystems. Further, symmetric key cryptosystems are of two types: block ciphers and stream ciphers.

The study of cryptographic and combinatorial properties of Boolean functions has been an important branch of cryptography. Shannon [137] has established the foundation of modern cryptography and introduced the concept of product ciphers using cryptographic transformations: substitution and permutation. Both these transformations extensively use Boolean functions with desirable cryptographic properties. Boolean functions and S-boxes with certain desirable cryptographic properties have many applications in the design of block ciphers and stream ciphers. In block ciphers the message bits are first divided into the blocks and each block is enciphered using same key. The obtained cipher bits are then transmitted over the channel. Most of the block ciphers use S-boxes as a nonlinear part of the scheme. Matsui [103] have introduced linear cyptanalysis for block ciphers. The security of block ciphers is highly dependent to the strength of the S-boxes. To provide protection against linear cryptanalysis the employed S-boxes should be highly nonlinear.

In stream ciphers (see Figure 1.1) [42, 140, 141] a pseudorandom sequence of bits is generated. In general the length of the generated sequence is same as the length of the message. The message is bitwise XOR-ed with the the generated sequence to get cipher bits, which is then transmitted over the channel. At the receiver end the same pseudorandom

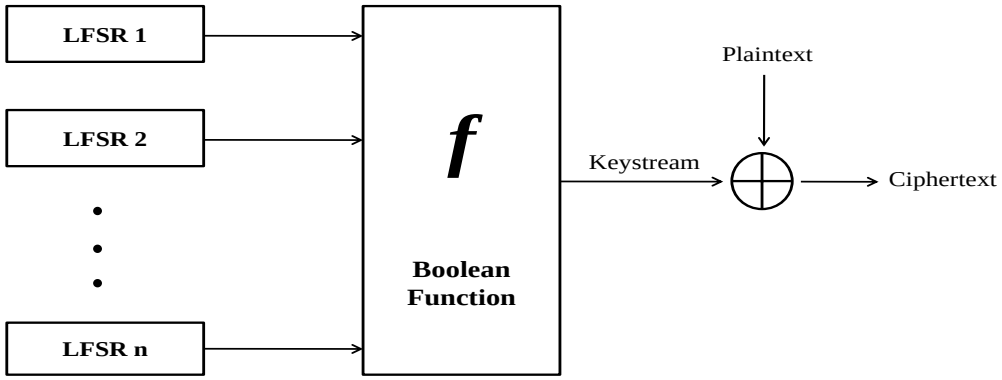


Figure 1.1: LFSR based stream cipher system

sequence is generated using secret key and XOR-ed with cipher bits for deciphering. LFSRs are important building blocks in the stream ciphers. Stream cipher combines the output bits of several LFSRs with the help of a nonlinear Boolean function to get keystream. The Boolean functions to be used as combiner function should possess high nonlinearity.

The study of various properties of combining Boolean function has attracted a lot of attention in the literature. It is considered an important problem to obtain cryptographic functions which are able to provide protection from several known attacks.

In the current age of computers one of the most important objective is to make secure transmission of information through public channels. This can be achieved by using suitable encryption algorithms for generating secure cipher texts.

The basic purpose of the study of Boolean functions, q-ary functions and their properties is to provide necessary tools and resources for the protocols of some important security algorithms. Boolean functions have wide applications in coding theory and cryptography, especially, their use in linear feedback shift registers (LFSRs) as a combiner function and filter function. A proper choice of a Boolean function for a cipher may significantly increase the resistance against different kinds of attacks. In the literature, several attacks have been proposed on stream ciphers and block ciphers [32–34, 56, 57, 60, 104, 105, 109, 116, 117].

Boolean functions used in various cryptosystems must satisfy some desired cryptographic criteria such as *balancedness*, high *nonlinearity*, high *algebraic immunity*, high *correlation immunity*, high *resiliency*, low *crosscorrelation*, *global avalanche characteristics* (GAC). It is impossible to optimize all these cryptographic criteria simultaneously. In other words, if a Boolean function possesses optimal value with respect to one cryptographic criterion it does not imply optimality with respect to all cryptographic criteria. But some tradeoffs can be made among them. These criteria will be discussed in detail in Chapter 2. The thesis presents some constructions and investigations of the cryptographic properties of Boolean functions and q-ary functions, especially highly nonlinear functions, balanced functions, bent functions and the functions satisfying various cryptographic criteria such as resiliency, PC and GAC.

Preneel et al. [122] have remarked that all the security schemes framed by combining permutations and substitutions are strongly dependent on the characteristics of the S-boxes used. To design S-boxes for various cryptosystems, it is strongly recommended to use highly nonlinear functions. It is to be noted that high nonlinearity alone is not sufficient for cryptographic purposes, for example, *bent* functions [124] possessing maximum possible nonlinearity are not of direct use, but they are used as starting point in the

construction of highly nonlinear functions which satisfy some other cryptographic criteria. In [43], Dobbertin has provided a well-known example of construction of highly nonlinear balanced Boolean functions.

The nonlinearity of Boolean functions is one of the important cryptographic criteria. It is the minimum Hamming distance of the function from the class of affine functions. The nonlinearity of a Boolean function f protects the system against linear cryptanalysis [103], best affine approximation attacks [56] and fast correlation attacks [106,116], when f is used as a combiner function or a filter function in stream ciphers. The relationship between nonlinearity and an explicit attack on symmetric cipher was discovered by Matsui [103]. The nonlinearity is related to the Walsh-Hadamard transform of the function and can be computed by using fast Walsh-Hadamard transform algorithm [36, 96]. Nonlinearity of Boolean functions has been studied in theoretical analysis as well as in algorithm implementation. The Boolean functions possessing maximum possible nonlinearity are called bent function and exists only for even n [124]. Bent functions are of special interest in cryptography [38, 88, 107, 113, 114] and coding theory [96, 103], and they have practical applications in spread spectrum communication [115]. In case of odd n, to obtain maximal value of nonlinearity of Boolean functions is still an open problem. During last few years a lot of work has been reported to construction of functions with good nonlinearity bounds. For more details on the functions with high nonlinearity we refer to [15, 17, 127, 135].

Another useful class of Boolean functions is *semi-bent* Boolean functions [9, 81]. The WHT of semi-bent Boolean functions takes only values $0, \pm 2^{\frac{n+1}{2}}$. Semi-bent Boolean functions are important in cryptography because they have low WHT which provides protection against linear cryptanalysis [103] and best affine approximation attacks [56]. Further, they usually satisfy other cryptographic criteria like high algebraic degree, low additive autocorrelation, resiliency, propagation criteria etc. Recently, many constructions of semi-bent functions have been proposed in the literature. The first family, Gold-like semi-bent functions with low values of autocorrelation spectrum has been introduced by Gold [55]. Khoo et al. [81] have proposed some new classes of quadratic semi-bent Boolean functions with multiple trace terms. There are several known classes of semi-bent Boolean functions. For further study on semi-bent functions we refer [23, 29, 55, 64, 65, 68, 81, 108, 111].

1.1 Higher order nonlinearities of Boolean functions

The higher order nonlinearities of Boolean functions is a natural generalization of the concept of the nonlinearity. The r-th order nonlinearity of $f \in \mathcal{B}_n$ is the minimum Hamming distance of f from the set of all functions of degree at most r. The r-th order nonlinearity of a Boolean function plays an important role against different kinds of attacks such as *best affine approximation* attacks [56] and *higher order approximation* attacks [32] on block ciphers and stream ciphers. Also, it plays a role in coding theory, since it is related to the covering radii of Reed-Muller codes. For $r = 1$, the $nl_1(f) = nl(f)$ is called first order nonlinearity (or simply the nonlinearity) of f. The sequence $\{nl_1(f), nl_2(f), ..., nl_{n-1}(f)\}$ is known as the *nonlinearity profile* of f. The r-th order nonlinearity of a Boolean fucntion measures the resistance of the function against various lower and higher order approximation attacks [35, 57, 77, 104, 109, 116], and has been extensively used in cryptanalysis [2, 33, 56, 74, 76, 84, 109, 114, 117, 138]. The Boolean functions used to design a secure cryptosystem should have high r-th order nonlinearities, so that it will not be possible to approximate them efficiently by low degree functions.

Unlike first order nonlinearity, there is no efficient algorithm to compute rth order nonlinearity of a Boolean function. Forquet and Tavernier [47] have provided an efficient algorithm for the computation of second order nonlinearity of Boolean functions for $n \leq 11$ and, up to $n = 13$ for some functions. Therefore, we require theoretically obtained lower bounds on higher order nonlinearities of functions which work for all values of n. The best known asymptotic upper bound on nl_r, obtained by Carlet and Mesnager [22], is

$$nl_r(f) \leq 2^{n-1} - \frac{\sqrt{15}}{2} \cdot (1+\sqrt{2})^{r-2} \cdot 2^{\frac{n}{2}} + O(n^{r-2}).$$

Carlet [14] has shown that for every real number c, with $c^2 \log_2 e \geq 1$, there exist a Boolean function f for which $nl_r(f) \geq 2^{n-1} - c\sqrt{\sum_{k=0}^{r} \binom{n}{k}} 2^{\frac{n-1}{2}}$, where e is the base of natural logarithm. Iwata and Kurosawa [74] have introduced notion of *higher order bent functions* and constructed Boolean functions whose lower bound on r-th order nonlinearities is $2^{n-r-3}(r+5)$.

Carlet [15] has provided a technique for systematic study of r-th order nonlinearities and nonlinearity profile of Boolean functions. He developed a recursive approach to compute the lower bounds on r-th order nonlinearities of a function f using the $(r-1)$-th order nonlinearities of its derivative. Using this approach he has derived lower bounds on nonlinearity profiles of several classes of functions including inverse functions, Welch functions, Kasami functions, functions in Maiorana-McFarland bent class, and in [16] for Dillon bent functions. Using Carlet's recursive approach several authors have obtained lower bounds on second order nonlinearities of some highly nonlinear Boolean functions [15,50,51,53,54,85,146,147].

1.2 Resiliency of Boolean functions

Resiliency of a Boolean function is an important cryptographic criterion and plays a crucial role when used as a combiner function in stream cipher systems. High resiliency provides protection against correlation attack [141], while high nonlinearity offers protection against linear approximation attack [103]. From cryptographic viewpoint it is important to construct resilient Boolean functions satisfying multiple cryptographic criteria. During last few years a lot of work has been done to construct highly nonlinear resilient functions with optimal algebraic immunity [59, 105, 126, 161].

Camion et al. [11] have constructed nonlinear resilient functions after modification in the Maiorana-McFarland (MM) type bent functions by concatenating small affine functions. Carlet [13] extended this technique by replacing affine concatenation to the quadratic concatenation. Xiao and Massey [158] have provided Spectra Characterization theorem of correlation immune Boolean functions. Sarkar and Maitra [126, 127] have generalized this result by proving that the Walsh-Hadamard spectrum m-resilient functions is divisible by 2^{m+2}. They have established a relationship between nonlinearity and the order of resiliency of Boolean functions. Recently, Gao et al. [52] have provided a technique to construct plateaued resilient Boolean functions having disjoint spectra. By using this technique, they have constructed plateaued resilient Boolean functions with disjoint spectra having good nonlinearity. For more results on resilient Boolean function having good nonlinearity we refer to [43, 100, 102, 125, 134, 161].

1.3 Crosscorrelation and autocorrelation of Boolean functions

Among the cryptographic criteria, the crosscorrelation and the autocorrelation of Boolean functions play central role in design and crytptanalysis of symmetric key cryptosystems. Analysis of crosscorrelation and autocorrelation of sequences has received a lot of attention in literature [49, 59, 128, 162, 166]. It follows from Shannon's basic design principles: *confusion* and *diffusion*, that it is good if the constituent functions of a secret key cryptosystem possess small correlation between them. The low crosscorrelation between two functions indicates that they are very different from each other, and such functions when used in a cryptosystem provide best confusion [128]. A lot of work has been reported in this direction and many important results have been obtained [59, 128, 162, 166, 167]. Boolean functions are of great interest in both block ciphers and stream ciphers, and various types of correlation analyses between them have found many applications in cryptography.

The functions with low correlation are central objects in various code division multiple access (CDMA) communication systems. In particular, the functions with low crosscorrelation are used to distinguish various users and to minimize interference due to other users in a common channel of CDMA system at the same time, whereas, the functions with low autocorrelation are important to have accurate phase information at the receiver end. Furthermore, by assigning a large number of functions with low correlation one can increase the capacity of CDMA communication systems. For more results on constructions of functions with low correlation we refer to [3,28,55,78,83,86,112,139,153,157]. Evaluation of crosscorrelation between two non binary (q-ary) functions has been studied by various researchers (for special values of q) [45, 64, 73, 110, 136, 152].

Gong and Youssef [61] have investigated autocorrelation and crosscorrelation properties of Welch-Gong transformation sequences. Sarkar and Maitra [128] have used crosscorrelation as a fundamental tool for analysis of cryptographic criteria for Boolean functions, and established the Crosscorrelation Theorem for n-variable Boolean functions. Moreover, they have provided a new characterization of Boolean bent function in terms of

autocorrelation and crosscorrelation of its subfunctions. Gangopadhyay and Maitra [49] have investigated crosscorrelation and autocorrelation spectra of Dillon type and Patterson-Wiedemann type functions. They have shown that the crosscorrelation spectrum of Dillon type functions is at most 5-valued, and in case of Dillon type bent functions at most 3-valued. Gong and Khoo [59] have computed the additive autocorrelation of some exiting classes of *resilient preferred functions* with the help of their dual functions. Due to huge cryptographic importance, the study of the crosscorrelation and the autocorrelation of Boolean functions has become a topic of great interest over more than 40 years. Several important relationships among these two criteria and other cryptographic criteria have been reported in the literature. For a detailed study on the topic we suggest the articles [61, 63, 97, 122, 128, 143, 155, 156, 162, 166, 168].

Webster and Tavares [155, 156] have introduced the concept of *strict avalanche criteria* (SAC) for Boolean functions. A Boolean function f on n variables is said to satisfy the SAC if complementing a single bit results in the output of f being complemented with a probability 1/2. Preneel et al. [122] have generalized this concept by introducing the concept of propagation criteion (PC). The concept of PC is very important for design of the one-way hash function and the encryption algorithm [143]. A function f is said to satisfy the PC with respect to a vector $\mathbf{u}$ of $\mathbb{Z}_2^n$ if the the value of autocorrelation coefficient vanishes at $\mathbf{u}$. It is to be noted that SAC and PC describe only local characteristics of a Boolean function. To analyze the global behavior of the functions, Zhang and Zheng [162] have introduced another criterion to measure the global avalanche characteristics (GAC) of one Boolean function. They have proposed two indicators: *sum-of-squares indicator* σ_f and *absolute indicator* $\triangle_f$ related to the GAC of one Boolean function, and obtained lower and upper bounds on these indicators. Zhou et al. [166] have generalized this concept for two functions and defined two new indicators: *sum-of-squares indicator* $\sigma_{f,g}$, and *absolute indicator* $\triangle_{f,g}$ of crosscorrelation between two functions, and provided lower and upper bounds on these two indicators. Since the smaller values of $\sigma_{f,g}$ and $\triangle_{f,g}$ correspond to low correlation between f and g, it may be important to construct cryptographic functions which possess smaller values of these indicators as well as optimal values of other cryptographic criteria. In the literature, several constructions of Boolean functions with optimal values of $\sigma_{f,g}$ and $\triangle_{f,g}$,

and satisfying some other important cryptographic criteria like balancedness, SAC and PC are reported. For a detailed study on these indicators we refer to [143,148,162,164,166,167].

On the other hand, Parker and Riera have extended the concept of bent functions to some generalized bent criteria for Boolean functions by analyzing Boolean functions having flat spectrum with respect to one or more unitary transforms [118, 123]. The set of transforms chosen by Riera and Parker [123] is motivated by a choice of local unitary transforms that have central role in the structural analysis of pure n-qubit stabilizer quantum state. Riera and Parker [123] have chosen the transforms formed by n-fold tensor product of the identity mapping I, the Walsh-Hadamard matrix H, and the *nega-Hadamard matrix* N, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{and } N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}, \text{ with } i = \sqrt{-1}.$$

Riera and Parker [123] have discussed the spectral properties of Boolean functions with respect to the transform set $\{I, H, N\}^3$ formed by tensor product of I, H and N, and established various results about the generalized bent properties of Boolean functions.

The nega-Hadamard transform (NHT) of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is a complex valued function on $\mathbb{Z}_2^n$ defined as

$$N_f(\mathbf{u}) = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + <\mathbf{x},\mathbf{u}>} i^{w_H(\mathbf{x})}.$$

A function $f \in \mathcal{B}_{n,2}$ is negabent if $|N_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$ i.e., if nega-Hadamard spectrum of f is flat. The Boolean functions which are simultaneously bent and negabent are of recent interest and referred to as *bent-negabent* functions. Parker and Pott [119] have provided a necessary and sufficient condition for a quadratic Boolean function to be bent-negabent. They have provided a necessary and sufficient condition for a Boolean function on even number of variables to be bent-negabent.

It is well known that the maximum possible degree of an n variable negabent functions is $\lceil \frac{n}{2} \rceil$ [144]. Schmidt et al. [132] have presented transformations which leave bent-negabent property invariant. They have constructed infinitely many bent-negabent functions in $2mn$-variables (with $m \not\equiv 1 \mod 3$) with algebraic degree at most n. These functions form a subclass of Maiorana-McFarland (MM) type bent functions. Further, they have shown that

the algebraic degree of a bent-negabent function on even number of variables in MM bent class is at most $\frac{n}{2} - 1$.

Stănică et al. [144] have investigated several properties of nega-Hadamard transform. They have provided a method to construct bent-negabent functions using complete mapping polynomials. Further, they have shown that for every $r \geq 2$, there exist bent-negabent functions on $n = 12r$-variables with algebraic degree $\frac{n}{4} + 1 = r + 1$.

Recently, Su et al. [145] have presented a necessary and sufficient conditions for n variable Boolean functions to be negabent for both the cases n even and n odd by investigating a direct link between the NHT and the WHT of Boolean functions. They have obtained the nega-Hadamard spectrum distribution of negabent Boolean functions. Further, they have constructed bent-negabent functions of maximum algebraic degree.

For the results on nega-Hadamard transform and bent-negabent functions we refer to [119, 123, 132, 144, 145].

1.4 q-ary functions

In recent years, many generalizations of Boolean functions have been proposed by several authors [1, 41, 70, 87, 123, 131]. They have established various analogous properties of the functions in the generalized setup. Kumar et al. [87] have provided a natural generalization of Boolean bent functions [124]. They have generalized the notion of Boolean bent functions by considering functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, where $q \geq 2$ and n a positive integer, and $\mathbb{Z}_q$ is the ring of integers modulo q. T A function f from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ is referred to as a *q-ary function*.

The Walsh-Hadamard transform (WHT) of a q-ary function f is a complex valued function on $\mathbb{Z}_q^n$ defined as

$$\mathcal{W}_f(\mathbf{u}) = \frac{1}{q^{\frac{n}{2}}} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{f(\mathbf{x}) + \langle \mathbf{x}, \mathbf{u} \rangle},$$

where $\xi = e^{\frac{2\pi i}{q}}$ is the complex q-th primitive root of unity, and $\langle \mathbf{x},\ \mathbf{u} \rangle$ is the usual inner product of $\mathbf{x}$ and $\mathbf{u}$ in $\mathbb{Z}_q^n$. A function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is said to be *q-ary bent* if $|\mathcal{W}_f(\mathbf{u})| = 1$ for every $\mathbf{u} \in \mathbb{Z}_q^n$ i.e., if f has flat spectra with respect to the Walsh-Hadamard transform. We recall that binary bent functions exist only for even number of inputs. Kumar et al. [87]

have provided constructions of q-ary bent functions for all values of q and n (except the case when n is odd and $q \equiv 2 \mod 4$). They have investigated several properties of q-ary functions and provided an analogue of binary Maiorana-McFarland type bent functions in the q-ary setup. They have remarked that, to establish and analyze the analogous properties of q-ary functions are seems to be more difficult than Boolean bent functions [87]. It can be noted that q-ary bent functions have applications in Code-Division Multiple-Access (CDMA) communications systems [131]. For an excellent survey on q-ary bent functions we refer to [20, 70–72, 81, 82, 90, 93, 95, 160].

Ambrosimov [1] has investigated all quadratic q-ary bent functions over a finite field and calculated their number. Hou [70] has provided some constructions of q-ary bent functions over chain rings. Solé and Tokareva [142] have provided a systematic link among Boolean bent functions, quaternary (4-ary) bent functions [75, 87], and generalized bent Boolean functions (due to Schmidt [131]) [142]. Recently, Jadda and Parraud [75] have investigated quaternary (for $q = 4$) functions and have characterized completely the $\mathbb{Z}_4$-nonlinearity and the balancedness for quaternary functions. Budaghyan et al. [5, 6] have provided a relationship among the known infinite classes of q-ary bent functions and class of Maiorana-McFarland type bent functions. Helleseth et al. [69] have shown that the Niho type crosscorrelation spectrum between two m-sequences, which differs by a decimation $d \equiv 1(\mod q-1)$, is at least 4-valued. The results concerning the analysis and computation of lower bounds of crosscorrelation of q-ary functions (for special values of q) can be found in [45, 64, 73, 110, 136, 152].

A q-ary function f is called *s-plateaued* if $|\mathcal{W}_f(\mathbf{a})| \in \{0, q^{\frac{s}{2}}\}$ for every $\mathbf{a} \in \mathbb{Z}_q^n$ [24]. Recently, Çeşmelioğlu and Meidl [24, 25] have presented a technique to construct p-ary (p a prime integer) bent functions using plateaued functions. In particular, for $p = 3, 5$ they have constructed bent functions achieving upper bounds of algebraic degree [24]. Çeşmelioğlu et al. [26, 27] have presented several properties and constructions of p-ary bent functions.

In this thesis we investigate several cryptographic properties of Boolean functions, q-ary functions introduced by Kumar et al. (1985), and the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. We identify some classes of Boolean functions with high nonlinearity which show good behavior with respect to second order nonlinearity. We investigate several properties of q-ary functions in

terms of their Walsh-Hadamard transforms (WHT) and crosscorrelation spectra. We compute the crosscorrelation of a subclass of Maiorana-McFarland type q-ary bent functions. Several primary as well as secondary constructions of q-ary functions are presented. We provide some constructions of balanced q-ary functions which have good GAC measured in terms of the indicators: the sum-of-squares-of-modulus indicator (SSMI) and the modulus indicator (MI), and which satisfy propagation criteria (PC). We present a new generalization of negabent functions by considering the functions $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. We investigate several properties of generalized negabent functions and provide some examples of such functions.

1.5 Thesis Plan

The chapter wise description of the thesis is as follows:

In **Chapter 1** we present some introductory matter on some important cryptographic criteria such as higher order nonlinearity, resiliency, crosscorrelation, autocorrelation, GACs of Boolean functions, negabent functions and q-ary functions, which gives motivation to the thesis.

Chapter 2 provides most of the preliminaries required for the thesis. We provide some basic definitions, notations and cryptographic properties of Boolean functions and q-ary functions. A brief summary of some basic results on finite fields and linearized polynomials is given. We discuss some existing results on higher order nonlinearities, bent functions, semi-bent functions, resilient Boolean functions, crosscorrelation, autocorrelation, GAC and negabent functions. Also, we discuss some recent results on q-ary functions.

In **Chapter** 3 we consider the problem of computing lower bounds on second order nonlinearities of cubic monomial functions of the form

1. $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$, where $n = 3r,\ 5r$ and $\lambda \in \mathbb{Z}_{2^n} \setminus \{0\}$,
2. $f(x) = tr_1^n(\lambda x^{2^{2r}+2^r+1})$, where $n = 3r$ and $\lambda \in \mathbb{Z}_{2^r} \setminus \{0\}$.

Boolean functions in the above classes possess no affine derivative. It is observed that the lower bounds obtained by us for the above classes of functions are better than the general bounds obtained by Carlet [15] and the bounds of some other classes of Boolean functions

which are recently studied [50, 53, 147]. Further, we obtain lower bounds on second-order nonlinearities for some classes of cubic Boolean functions based on secondary constructions.

Gao et al. [52] have provided a method for the construction of plateaued resilient functions with disjoint spectra. In **Chapter 4** using this technique, we provide some new constructions of highly nonlinear resilient Boolean functions on large number of variables with disjoint spectra by concatenating disjoint spectra functions on small number of variables. We observe that in some cases the nonlinearity bounds of the constructed functions are better than the bounds obtained by Gao et al. [52].

Chapter 5 through Chapter 7 are devoted to the study of various cryptographic properties and constructions of q-ary functions.

In **Chapter 5** we compute the crosscorrelation of a subclass of Maiorana-McFarland (MM) type q-ary bent functions. We provide a characterization of quaternary (4-ary) bent functions on $(n+1)$-variables in terms of their subfunctions on n-variables. We slightly generalize a result of Tokerava [151] by proving that the direct sum of two q-ary bent functions f_1 and f_2 is q-ary bent if and only if f_1 and f_2 both are q-ary bent. We present several results on q-ary functions in terms of their WHTs and crosscorrelations. Analogous to the indicators sum-of-squares indicator and absolute indicator in Boolean case, we define two similar indicators: the *sum-of-squares-of-modulus indicator* (SSMI) $\sigma_{f,g}$ and the *modulus indicator* (MI) $\triangle_{f,g}$ to measure the global avalanche characteristic (GAC) of two q-ary functions. We study q-ary functions in terms of these two indicators and derive some lower and upper bounds on these indicators. Also, we provide some constructions of balanced quaternary functions with high nonlinearity under the Lee metric.

In **Chapter 6** we present construction of two classes of q-ary *balanced* functions which have good GAC measured in terms of two indicators SSMI and MI, and *propagation criterion* (PC). We show that the cryptographic criteria the SSMI, MI, and PC of q-ary functions are invariant under affine transformations. Also, we give a construction of q-ary s-plateaued functions and obtain their SSMI. We provide a relationship between the autocorrelation spectrum of a cubic Boolean function and the dimension of the kernel of the bilinear form associated with the derivative of the function. Using this result, we identify several classes of cubic semi-bent Boolean functions which have good bounds on their SSMI

and MI, and hence show good behavior with respect to the GAC.

In **Chapter 7**, we study some further properties of q-ary functions and provide some constructions for ternary ($q = 3$) functions. We provide a method for the construction of ternary functions on $(n + 1)$ variables by using decomposition functions f_1, f_2, f_3 on n-variables, and investigate a link between the SSMI of a $(n + 1)$-variable ternary function f and the SSMI of their n-variable decomposition functions f_1, f_2, f_3. Also, we provide a construction of ternary functions with low value of SSMI by using pairwise perfectly uncorrelated m-plateaued ternary functions and modified ternary bent functions. We investigate a relationship among the indicators, $\sigma_{f,g}$, σ_f (the SSMI of f) and σ_g (the SSMI of g) of two q-ary functions f and g. Further, we deduce upper bounds to the indicators the SSMI and the MI of two q-ary functions for the case that one of them is s-plateaued q-ary function.

In **Chapter 8** we propose a new generalization of negabent functions by considering the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. We investigate several properties of generalized nega-Hadamard transform (GNHT) and its behavior on various combinations of functions. We have obtained some results describing the properties of generalized negabent functions. We generalize a result of Schmidt et al. [132, Lemma 1] (obtained for binary case) to $\mathbb{Z}_q$. We have established a connection between the generalized nega-autocorrelation of functions and their GNHT. Further, we present a characterization of generalized negabent (for $q = 4$) functions on $n + 1$ variables in terms of their subfunctions on n-variables. Further, in the new setup we have proposed, we present several interesting examples of generalized negabent functions for various values of q and n.

Chapter 9 is the conclusion.

Chapter 2

Background

In this chapter, we present a brief overview of the most important and essential aspects of Boolean functions, desired cryptographic criteria, and q-ary functions. First, we describe some notations and symbols that will be used throughout the thesis. We present various representations of Boolean functions which are frequently used in cryptography. Important definitions and existing results on Boolean functions and q-ary functions are provided. Next, we discuss some important tools like Walsh-Hadamard transform (WHT), nega-Hadamard transform (NHT), autocorrelation etc. that are extensively used in the analysis of cryptographic properties of Boolean functions and q-ary functions. Further, we present some important relations which provide some well-known bounds and several tradeoffs among various cryptographic properties.

2.1 Notation

Let $\mathbb{F}_2 = \{0, 1\}$ be the binary field and $\mathbb{F}_2^n$ the linear space of all n-tuples over $\mathbb{F}_2$. Let $\mathbb{F}_{2^n}$ be the field of cardinality 2^n. For a fixed basis of $\mathbb{F}_{2^n}$, every element $\mathbf{x} = (x_n, \ldots, x_1) \in \mathbb{F}_2^n$ can uniquely be associated to an element $a \in \mathbb{F}_{2^n}$. Let $\{u_n, \ldots, u_1\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then a relation between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ can be defined as

$$\phi : \mathbb{F}_2^n \to \mathbb{F}_{2^n} \text{ such that } \phi(\mathbf{x}) = a = \sum_{i=0}^{n-1} u_i x_i.$$

Thus, $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ are isomorphic as $\mathbb{F}_2$-vector spaces. According to the convenience we will use $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ interchangeably. Let $\mathbb{Z}_q$ denotes the ring of integers modulo q. For q a prime, $\mathbb{Z}_q$ is a field. In particular, for $q = 2$, we use both notations $\mathbb{F}_2$ and $\mathbb{Z}_2$. Let $\mathbb{R}$ and $\mathbb{C}$ denote the fields of real and complex numbers respectively, and $\mathbb{Z}$ the ring of integers. $\mathbb{N}$ denotes the set of positive integers. The addition in $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_q$ is denoted by $+$ and is clear from the context. Let $z = (x + iy) \in \mathbb{C}$, $i^2 = -1$, $x, y \in \mathbb{R}$, then $\overline{z} = x - iy$ denotes the complex conjugate of z in $\mathbb{C}$. The absolute value of z is defined as $|z| = \sqrt{x^2 + y^2}$. We denote the cardinality of a set A by $|A|$.

Let $q \geq 2$ be a positive integer. The usual inner product of two elements $\mathbf{x} = (x_n, \ldots, x_1)$, $\mathbf{y} = (y_n, ..., y_1) \in \mathbb{Z}_q^n$ is defined as $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$. For $q = 2$ it becomes the usual inner product on $\mathbb{F}_2^n$.

2.2 Boolean functions

A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called a Boolean function on n variables. Since $\mathbb{F}_2^n$ is isomorphic to $\mathbb{F}_{2^n}$ as an $\mathbb{F}_2$-space, therefore, a Boolean function can also be assumed to be a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$. Let $\mathcal{B}_n$ denote the set of all n-variable Boolean functions. The cardinality of $\mathcal{B}_n$ is 2^{2^n}.

Now, we present some important representations of Boolean functions used in the study of Boolean functions in the context of coding theory and cryptography.

2.2.1 Truth-table and bipolar representation

A Boolean function on n variables can uniquely be represented by a truth table, which is a vector $(f(0, ..., 0), f(0, ..., 1), ..., f(1, ..., 1))$ consists of its 2^n functional values in the lexicographical increasing order. Since, the order of each functional value in truth table representation is fixed, therefore, the truth table of a Boolean function can be represented by a binary string

$$f = (f(0, ..., 0) f(0, ..., 1) ... f(1, ..., 1))$$

of length 2^n. Recall that for every element $a \in \mathbb{F}_{2^n}$ there exists a unique vector $\mathbf{x} = (x_n, ..., x_1)$ in $\mathbb{F}_2^n$ such that $a = \sum_i x_i 2^{i-1}$. Thus, the truth table of f can also be represented as $f = (f(0)f(1)...f(2^n - 1))$. The truth table representation of a Boolean function f is an important representation as it can directly verify some properties of f such as weight, support, and distance. The distance between two Boolean functions f and g is computed by considering the distance between their corresponding truth tables.

A function $(-1)^f = 1 - 2f$ is called Sign function of f. The functional values of $(-1)^f$ belong to the set $\{1, -1\}$. The string of length 2^n

$$(-1)^f = ((-1)^{f(0)}(-1)^{f(1)}(-1)^{f(2)}...(-1)^{f(2^n-1)})$$

corresponding to the function value of $(-1)^f$ is known as polarity truth table (or bipolar representation) of f. The bipolar representation can directly be obtained by replacing 0 and 1 by 1 and -1, respectively in the truth table representation.

In Table 2.1, we present an example of truth table representation of a 3-variable Boolean function f. First three columns of the table represent the input variables and last column represents the function values of f corresponding to the inputs. Thus, f is represented by the binary vector $f = (10100011)$.

Table 2.1: Truth table representation of a 3 variable Boolean function

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

The function $f = (10100011)$ in Table 2.1 is the sum of the atomic functions f_1, f_2, f_3 and f_4. The truth tables of these atomic functions are given in Table 2.2.

Now, we discuss some important definitions which are closely related to the truth table

Table 2.2: Truth table of atomic functions of a 3 variable Boolean function

x_3	x_2	x_1	f_1	f_2	f_3	f_4	f
0	0	0	1	0	0	0	1
0	0	1	0	0	0	0	0
0	1	0	0	1	0	0	1
0	1	1	0	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	0	0	0	1	0	1
1	1	1	0	0	0	1	1

representation of a Boolean function.

Definition 2.2.1. *The support* $supp(\mathbf{x})$ *of a vector* $\mathbf{x} \in \mathbb{F}_2^n$ *is defined as the set containing non-zero positions of* $\mathbf{x}$*, i.e.,* $supp(\mathbf{x}) = \{i : \ x_i \neq 0\}$, $i = 1, 2, ..., n$*. In the same way, the support of a function* $f \in \mathcal{B}_n$ *is defined as* $supp(f) = \{\mathbf{x} \in \mathbb{F}_2^n : \ f(\mathbf{x}) \neq \mathbf{0}\}$.

Definition 2.2.2. *The Hamming weight* $w_H(\mathbf{x})$ *of an element* $\mathbf{x} \in \mathbb{F}_2^n$ *is defined as the number of non-zero positions in* $\mathbf{x}$*, i.e.,* $w_H(\mathbf{x}) = |\{i : \ x_i \neq 0, \ i = 1, 2, ..., n\}| = \sum_i x_i$ $= |supp(\mathbf{x})|$*. Similarly, the Hamming weight* $w_H(f)$ *of* $f \in \mathcal{B}_n$ *is defined as* $w_H(f) = |\{\mathbf{x} \in \mathbb{F}_2^n : \ f(\mathbf{x}) \neq \mathbf{0}\}| = |supp(f)|$.

Definition 2.2.3. *The Hamming distance* $d_H(\mathbf{x}, \mathbf{y})$ *between two vectors* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ *is the number of positions where they do not match, i.e.,* $d_H(\mathbf{x}, \mathbf{y}) = |\{i : \ x_i \neq y_i, \ i = 1, 2, ..., n\}| = w_H(\mathbf{x} + \mathbf{y})$*. In the same way, the Hamming distance between* $f, g \in \mathcal{B}_n$ *is given by* $d_H(f, g) = |\{\mathbf{x} \in \mathbb{F}_2^n : \ f(\mathbf{x}) \neq g(\mathbf{x})\}| = w_H(f + g)$.

Definition 2.2.4. *A Boolean function* f *is called balanced if the output column of its truth table has equal number of* 0*'s and* 1*'s. That is, if the Hamming weight of* $f \in \mathcal{B}_n$ *is* $w_H(f) = 2^{n-1}$.

Example 2.2.5. *Let* f *and* g *be* 3*-variable Boolean functions with their truth table representation as* $f = (11010010)$ *and* $g = (10011101)$*. Then, we have* $w_H(f) = 4, w_H(f) = 5$*, and* $d_H(f, g) = w_H(f + g) = w_H(01001111) = 5$.

2.2.2 Algebraic normal form (ANF)

Algebraic normal form (ANF) is another way to represent Boolean functions. This representation of Boolean functions has been extensively used in coding theory and cryptography. Every Boolean function f has its unique ANF. Let $f \in \mathcal{B}_n$, then the ANF of f is defined as an n variable polynomial in $\mathbb{F}_2[x_n, \ldots, x_2, x_1]/(x_n^2 - x_n, \ldots, x_2^2 - x_2, x_n^2 - x_1)$ as

$$f(x_n, \ldots, x_2, x_1) = \bigoplus_{\mathbf{a}=(a_n,\ldots,a_2,a_1)\in\mathbb{F}_2^n} \lambda_{\mathbf{a}} \left(\prod_{i=1}^{n} x_i^{a_i} \right), \quad \lambda_{\mathbf{a}} \in \mathbb{F}_2,$$

where $\lambda_{\mathbf{a}} \in \mathbb{F}_2$ is the coefficient of the monomial $\prod_{i=1}^{n} x_i^{a_i}$. The algebraic degree of a function $f \in \mathcal{B}_n$ is the highest degree of the monomials present in the ANF of f for which $\lambda_{\mathbf{a}} \neq 0$, i.e., $deg(f) := \max\{w_H(\mathbf{a}) : \ \mathbf{a} \in \mathbb{F}_2^n, \lambda_{\mathbf{a}} \neq 0\}$. A function $f \in \mathcal{B}_n$ is called *homogeneous* Boolean function if all the terms in the ANF of f are of same degree.

Let $\mathbf{a}, \mathbf{x} \in \mathbb{F}_2^n$, then an affine Boolean function on n variables is defined as

$$\begin{aligned} \phi_{\mathbf{a},b}(\mathbf{x}) &= \langle \mathbf{a}, \mathbf{x} \rangle + b \\ &= l_{\mathbf{a}}(\mathbf{x}) + b, \ b \in \mathbb{F}_2, \end{aligned}$$

where $l_{\mathbf{a}}(\mathbf{x}) = \langle \mathbf{a}, \mathbf{x} \rangle = \sum_{i=1}^{n} a_i x_i$ denotes a linear function in $\mathbb{F}_2^n$. The affine functions are the simplest functions from ANF point of view [17]. Affine functions are either balanced or constant. The set $\mathcal{A}_n$ of all affine Boolean functions over $\mathbb{F}_2^n$ is defined as

$$\mathcal{A}_n = \{l_{\mathbf{a}} + b, \ \mathbf{a} \in \mathbb{F}_2^n, b \in \mathbb{F}_2\}.$$

Definition 2.2.6. *Two Boolean functions f and g are called* affine equivalent *if there exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{a}, \mathbf{c}, \mathbf{x} \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2$ such that $f(\mathbf{x}) = g(A\mathbf{x} + \mathbf{c}) + \langle \mathbf{a}, \mathbf{x} \rangle + b$, where $GL(n, \mathbb{F}_2)$ is group of all $n \times n$ invertible matrices over $\mathbb{F}_2$.*

It is to be noted that the two representations of Boolean functions: the truth table representation and the ANF representation are closely related to each other, as one can be obtained directly from the other.

Example 2.2.7. *Consider f the function as defined in Table 2.2. The value of the function*

f_1 is 1 if and only if $1+x_1=1$, $1+x_2=1$, and $1+x_3=1$, i.e., if and only if $(1+x_1)(1+x_2)(1+x_3)=1$. The ANF of f_1 is defined as $f_1=(1+x_1)(1+x_2)(1+x_3)$. In the same way, we obtain the ANF's $f_2=(1+x_1)x_2(1+x_3)$, $f_3=(1+x_1)x_2x_3$, and $f_4=x_1x_2x_3$. Therefore, the ANF of f is given by $f=(1+x_1)(1+x_2)(1+x_3)+(1+x_1)x_2(1+x_3)+(1+x_1)x_2x_3+x_1x_2x_3$.

2.2.3 Trace representation

The trace representation is very useful in defining and analyzing various properties of Boolean functions. Also, it is useful in the study of sequence theory. Let m and n be two positive integers such that $m|n$. The trace function tr_m^n [96] is a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ defined as

$$tr_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{m(\frac{n}{m}-1)}}, \quad x \in \mathbb{F}_{2^n}.$$

In particular, for $m=1$, a Boolean function can be viewed as a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ defined as

$$tr_1^n(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}} = \sum_{i=0}^{n-1} x^{2^i}.$$

The function $\langle x, y\rangle = tr_1^n(xy)$ denotes the inner product in $\mathbb{F}_{2^n}$. Further, every linear Boolean function can be expressed as $tr_1^n(ax)$ for some element $a \in \mathbb{F}_{2^n}$.

Definition 2.2.8. *Let $\mathbb{F}_{2^n}^*$ denote the multiplicative group of units of $\mathbb{F}_{2^n}$. An element $\alpha \in \mathbb{F}_{2^n}$ is called a primitive element of $\mathbb{F}_{2^n}$ if it is a generator of $\mathbb{F}_{2^n}^*$, which is a cyclic group. A cyclotomic coset modulo (2^n-1) [96, page 104-105] of s is given as $C_s = \{s, 2s, 2^2s, ..., 2^{n_s-1}s\}$, where n_s is the smallest positive integer satisfying $s \equiv s2^{n_s} \mod (2^n-1)$ and represents the size of the cyclotomic coset C_s. If s is the smallest member in the coset C_s then it is known as coset leader of C_s.*

The following are two important facts about cyclotomic cosets

- The cyclotomic cosets are either disjoint or identical.
- The cardinality of the cyclotomic coset $|C_s|$ is either n or non-trivial devisor of n.

Example 2.2.9. *[96, page 104-105] The cyclotomic cosets* mod 15 *are presented in Table 2.3.*

Table 2.3: The cyclotomic cosets modulo 15

Coset representatives	Cyclotomic cosets modulo 15
C_0	$\{0\}$
C_1	$\{1, 2, 4, 8\}$
C_3	$\{3, 6, 12, 9\}$
C_5	$\{5, 10\}$
C_7	$\{7, 14, 13, 11\}$

The following properties of trace functions are useful in the study of Boolean functions and sequence theory [94, 96].

Theorem 2.2.10. *The trace function tr_1^n satisfies the following properties:*

- *Trace tr_1^n is a linear function, i.e.,*

$$tr_1^n(ax + by) = atr_1^n(x) + btr_1^n(y), \quad x, y \in \mathbb{F}_{2^n},\ a \in \mathbb{F}_2.$$

- *$tr_1^n(x)$ takes every value in $\mathbb{F}_{2^n}$ equally often, i.e., $tr_1^n(x)$ is a balanced function.*
- *$tr_1^n(x)$ is not identically zero.*
- *$tr_1^n(x^{2^i}) = (tr_1^n(x))^{2^i} = tr_1^n(x)$.*
- *$tr_1^n(a) = an \ (mod\ 2)$, for every $a \in \mathbb{F}_2$.*
- *$tr_1^n(x)$ represents a polynomial $\sum_{i=0}^{n-1} x^{2^i}$.*
- *Let C be the set of coset leaders of cyclotomic cosets modulo $(2^n - 1)$ of all r which appear as the power of x in $tr_1^n(c_r x^r)$. Then, we have*

$$\textstyle\sum_{r \in C} tr_1^n(c_r x^r) = 0\ \forall x \in \mathbb{F}_{2^n} \text{ if and only if } tr_1^n(c_r x^r) = 0\ \forall r \in C.$$

For the proof of the above results, we refer to [94, 96].

The Boolean functions over $\mathbb{F}_{2^n}$ can also be represented by an univariate polynomial

$$f(x) = \sum_{i=0}^{2^n-1} c_i x^i, \tag{2.2.1}$$

where $c_0, c_{2^n-1} \in \mathbb{F}_2$, and for $1 \leq i \leq 2^n - 1$ $c_i \in \mathbb{F}_2$ with $c_i^2 = c_{2i}$ where $2i$ is taken mod $(2^n - 1)$. The algebraic degree of $f \in \mathcal{B}_n$ in (2.2.1) is defined as $\deg(f) = \max_{c_i \neq 0}\{w_H(i) : 0 \leq i \leq 2^n - 1\}$ [21].

Let $n \in \mathbb{N}$. Then every integer $0 \leq d \leq 2^n - 1$ can uniquely be expressed as

$$d = d_{n-1}2^{n-1} + d_{n-2}2^{n-2} + \ldots + d_1 2 + d_0, \tag{2.2.2}$$

where $d_{n-1}, \ldots, d_0 \in \mathbb{F}_2$. Once the order in which the exponents of 2 appear in (2.2.2) is fixed, the finite sequence $d_{n-1}d_{n-2}\ldots d_0$ is referred to as binary representation of d. The Hamming weight of d is $w_H(d) = \sum_{i=0}^{n-1} d_i$, where the sum is taken over $\mathbb{Z}$.

In the following result, we discuss the trace representation of any non-zero Boolean function.

Lemma 2.2.11. *[58, page 178] Any non-zero function $f \in \mathcal{B}_n$ can be represented as*

$$f(x) = \sum_{i \in \Gamma(n)} tr_1^n(\beta_i x^i) + \beta_{2^n-1} x^{2^n-1}, \text{ for all } x \in \mathbb{F}_{2^n}, \tag{2.2.3}$$

where $\Gamma(n)$ is the set of coset leaders modulo $2^n - 1$ and $\beta_i \in \mathbb{F}_{2^{nt_i}}$, $\beta_{2^n-1} \in \mathbb{F}_2$ for every $i \in \Gamma(n)$.

A Boolean function is known as *monomial trace function* if if its trace representation has single trace term. For more results on trace functions we refer to [94, 96].

2.3 Linearized polynomials

A special class of polynomials that is important for both in theory and in applications is discussed in this section.

Definition 2.3.1. *Let q be a prime power. Then the polynomial $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$ having its coefficients in $\mathbb{F}_{q^m}$, an extension field of $\mathbb{F}_q$, is called a q-polynomial over the field $\mathbb{F}_{q^m}$. For a fixed value of q, these polynomials are referred to as linearized polynomials.*

Now we list some results regarding linearized polynomials over $\mathbb{F}_{q^m}$, which are useful in the study of cryptographic properties of Boolean functions.

Lemma 2.3.2. *[94, Theorem 3.50] If $L(x)$ is a non-zero linearized polynomial over field $\mathbb{F}_{q^m}$ and the extension field $F = \mathbb{F}_{q^s}$ of $\mathbb{F}_{q^m}$ contains all the zeros of $L(x)$. Then*

(*i*) *The function $L : \lambda \in F \to L(\lambda) \in F$ is an $\mathbb{F}_q$-linear operator on F and the zeros of $L(x)$ form an $\mathbb{F}_q$-subspace of F.*

(*ii*) *Every zero of $L(x)$ has the same multiplicity which is either 1 or a power of q.*

Proof. (*i*) Suppose $x, y \in F$, then we have

$$L(x+y) = \sum_{i=0}^{n} \alpha_i (x+y)^{q^i} = \sum_{i=0}^{n} \alpha_i x^{q^i} + \sum_{i=0}^{n} \alpha_i y^{q^i} = L(x) + L(y).$$

and for every $c \in \mathbb{F}_q$, we get

$$L(x) = \sum_{i=0}^{n} \alpha_i (cx)^{q^i} = \sum_{i=0}^{n} \alpha_i (cx)^{q^i} = cL(x) \ \ (\text{ as } \ c^{q^i} = c).$$

Thus, L induces an $\mathbb{F}_q$-linear operator to the field F. Now, it follows that if x, y are zeroes of $L(x)$, then so is, $ax + by$ for all $a, b \in \mathbb{F}_q$. Hence, the set of zeroes of $L(x)$ forms an $\mathbb{F}_q$-subspace of F.

(*ii*) For $\sum_{i=0}^{n} \alpha_i x^{q^i}$, $L'(x) = \alpha_0$, where $L'(x)$ is the derivative of $L(x)$. An element $\gamma \in F$ is a repeated root of $L(x)$ if an only if it is a common root of L and L'. Thus, $L(x)$ has simple roots for $\alpha_o \neq 0$. Otherwise, if $\alpha_0 = \alpha_1 = ... = \alpha_{j-1} = 0$ and $\alpha_j \neq 0$ for some $j \geq 1$, then

$$L(x) = \sum_{i=j}^{n} \alpha_i x^{q^i} = \sum_{i=j}^{n} \alpha_i^{q^{m_j}} x^{q^i} = \left(\sum_{i=j}^{n} \alpha_i^{q^{(m-1)j}} x^{q^i} \right)^{q^j},$$

and $L'(x) = \alpha_j^{q^{(m-1)j}} \neq 0$, which implies that $L(x)$ is the $q^j th$ power of a linearized polynomial having only simple zeros. Thus, each zero of $L(x)$ has same multiplicity q^j. ∎

Lemma 2.3.3. *[94] Let $L(x)$ be a linearized polynomial over the field $\mathbb{F}_{q^m}$ and $F = \mathbb{F}_{q^s}$ an extension of $\mathbb{F}_{q^m}$. Then $L(x)$ has q^{s-r} number of zeroes in F, where r is the rank of the matrix representation of $\mathbb{F}_q$-linear operator L on F.*

The following is an important property of linearized polynomials, which is used in computation of some results in this thesis.

Proposition 2.3.4. *[4, Corollary1] Let* $L(x) = \sum_{i=0}^{h} a_i x^{2^{ik}}$, *where* h *and* k *are integers and* $gcd(n,k) = 1$. *Then there are at most* 2^h *zeros of* $L(x)$ *in* $\mathbb{F}_{2^n}$.

Proposition 2.3.5. *[94, 96] Let* $L_k, k \in \mathbb{N}$, *be a linearized polynomial over* $\mathbb{F}_{2^n}$ *such that*

$$L_k(x) = a_0^k x + a_1^k x^2 + ... + a_0^k x^{2^{n-1}}.$$

Then $L_k(x)$ *will have same number of zeros in* $\mathbb{F}_{2^n}$ *corresponding to all the elements* k *where* k *belongs to the same cyclotomic coset modulo* $2^n - 1$.

For detailed study on linearized polynomials we refer to [94, 96].

2.4 Walsh-Hadamard transform

The Walsh-Hadamard transform (WHT) is an important tool by which almost all cryptographic criteria of Boolean functions can be characterized. The WHT of $f \in \mathcal{B}_n$ is an integer valued function from $\mathbb{F}_2^n$ to $[-2^n, 2^n]$ defined as

$$W_f(\mathbf{a}) = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) + \langle \mathbf{a}, \mathbf{x} \rangle} \quad \text{for every } \mathbf{a} \in \mathbb{F}_2^n,$$

where $\langle \mathbf{a}, \mathbf{x} \rangle = a_1 x_1 + \cdots + a_n x_n$ is usual inner product of $\mathbf{a}$ and $\mathbf{x}$ in $\mathbb{F}_2^n$. In case of finite fields, for $a, x \in \mathbb{F}_{2^n}$ the inner product of a and x is defined as $a \cdot x = tr_1^n(ax)$. From the definition, it follows that the $W_f(\mathbf{a})$ is equal to the number of 0's minus number of 1's in the truth table representation of the function $f + l_{\mathbf{a}}$, where $l_{\mathbf{a}}(\mathbf{x}) = \langle \mathbf{a}, \mathbf{x} \rangle = a_1 x_1 + \cdots + a_n x_n$ is a linear Boolean function. The multiset $\{W_f(\mathbf{a}) : \mathbf{a} \in \mathbb{F}_2^n\}$ is called Walsh-Hadamard spectrum (WHS) of the function f.

The sum

$$W_f(\mathbf{a}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) + \langle \mathbf{a}, \mathbf{x} \rangle}$$

for every $\mathbf{a} \in \mathbb{F}_2^n$ is called the *non-normalized* WHT of $f \in \mathcal{B}_n$.

The properties of WHT describing its various characteristics will be discussed in the later sections. The conservation law for the WHS values of $f \in \mathcal{B}_n$ is known as Parsavel's identity, which states that the sum of squares of WHT values is constant. In the following result, we provide the proof outline for the Parseval's identity.

Theorem 2.4.1. *Let $f \in \mathcal{B}_n$, then* $\sum_{\mathbf{a}\in\mathbb{F}_2^n} W_f^2(\mathbf{a}) = 2^n$.

Proof. We compute

$$\begin{aligned}
\sum_{\mathbf{a}\in\mathbb{F}_2^n} W_f^2(\mathbf{a}) &= \frac{1}{2^n} \sum_{\mathbf{a}\in\mathbb{F}_2^n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})+\langle \mathbf{a},\mathbf{x}\rangle} \sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{y})+\langle \mathbf{a},\mathbf{y}\rangle} \\
&= \frac{1}{2^n} \sum_{\mathbf{a}\in\mathbb{F}_2^n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})+f(\mathbf{y})+\langle \mathbf{a},\mathbf{x}+\mathbf{y}\rangle} \\
&= \frac{1}{2^n} \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})+f(\mathbf{y})} \sum_{\mathbf{a}\in\mathbb{F}_2^n} (-1)^{\langle \mathbf{a},\mathbf{x}+\mathbf{y}\rangle} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})+f(\mathbf{x})} \\
&= 2^n.
\end{aligned}$$

■

Theorem 2.4.2. *The inverse of WHT of a function $f \in \mathcal{B}_n$ is given by*

$$(-1)^{f(\mathbf{x})} = \frac{1}{2^{n/2}} \sum_{\mathbf{a}\in\mathbb{F}_2^n} W_f(\mathbf{a})(-1)^{\langle \mathbf{a},\mathbf{x}\rangle}.$$

Proof. The proof direct follows from the definition of WHT. ■

Now, we provide some important definitions in terms of the WHT of Boolean functions.

Definition 2.4.3. *A function $f \in \mathcal{B}_n$ is called Plateaued if its WHS consists of only* 0 *and* $\pm 2^k$, *where k is a positive integer and is known as the amplitude of f.*

Definition 2.4.4. *Two Boolean functions f and g are called disjoint spectra functions if* $W_f(\mathbf{w})W_g(\mathbf{w}) = 0$ *for every* $\mathbf{w} \in \mathbb{F}_2^n$.

A function $f \in \mathcal{B}_n$ is called *balanced* if $W_f(0) = 0$, and in this case, we have $w_H(f) = 2^{n-1}$.

Derivative of a Boolean function

Let $f \in \mathcal{B}_n$, then the derivative $D_a f$ of f at $a \in \mathbb{F}_{2^n}$ is defined as $D_a f = f(x) + f(x+a)$, for every $x \in \mathbb{F}_{2^n}$. Applying the derivation several times to the function f gives higher order derivatives.

Definition 2.4.5. *Suppose V is a r-dimensional subspace of $\mathbb{F}_{2^n}$ generated by elements $a_1, \ldots, a_r$. The r-th order derivative of $f \in \mathcal{B}_n$ with respect to V is defined as*

$$D_V f(x) = D_{a_1} \cdots D_{a_r} f(x) \text{ for every } x \in \mathbb{F}_{2^n}.$$

Clearly, an r-th order derivative of f depends only on the choice of the r-dimensional subspace V and is independent of the choice of the basis of V .

2.5 Quadratic Boolean functions

Let V be an n-dimensional vector space over $\mathbb{F}_q$, the field of characteristic 2. Then a mapping $S : V \to \mathbb{F}_q$ is called a quadratic form [10] on V if

1. $S(ax) = a^2 S(x)$, for every $x \in V$ and $a \in \mathbb{F}_q$.

2. $B(x, y) = S(0) + S(x) + S(y) + S(x + y)$ is bilinear on V.

Proposition 2.5.1. *[10, Proposition 1] Suppose V is a vector space over $\mathbb{F}_q$, the field of characteristics 2, and S is a quadratic form on V. Then the dimension of the space V and the dimension of the kernel of bilinear form $B(x, y)$ have same parity.*

Let $f \in \mathcal{B}_n$ be a quadratic Boolean function, then the bilinear form of f is given as $B(x, y) = f(0) + f(x) + f(y) + f(x+y)$. Also, the kernel of $B(x, y)$ [10,96] forms a subspace of the field $\mathbb{F}_{2^n}$ and defined as

$$\varepsilon_f = \{x \in \mathbb{F}_{2^n} : B(x, y) = 0, \ \forall\, y \in \mathbb{F}_{2^n}\}.$$

Lemma 2.5.2. *[10, Lemma 1] If $f \in \mathcal{B}_n$ is a quadratic function, then the kernel ε_f of f is a subspace of $\mathbb{F}_{2^n}$ and can be expressed as*

$$\varepsilon_f = \{a \in \mathbb{F}_{2^n} : D_a f = consatnt\}.$$

The elements of ε_f are known as linear structure of f. The derivative $D_a f$ of a quadratic Boolean function f is obviously an affine function and hence either balanced or constant. It may be noted that the WHS of quadratic Boolean functions is completely characterized in terms of the dimension of the kernel of the bilinear form associated with them, as the following result shows.

Proposition 2.5.3. *[96, page 441] The weight distribution of WHS of a quadratic function $f \in \mathcal{B}_n$ depends only on the dimension k of the kernel ε_f of bilinear form and is given in the Table 2.4.*

Table 2.4: Weight distribution of the WHS of a quadratic Boolean function

$W_f(\alpha)$	number of α
0	$2^n - 2^{n-k}$
$2^{(n+k)/2}$	$2^{n-k-1} + (-1)^{f(0)}2^{(n-k-2)/2}$
$-2^{(n+k)/2}$	$2^{n-k-1} - (-1)^{f(0)}2^{(n-k-2)/2}$

Some desirable cryptographic criteria

A function is said to be of cryptographic importance if it satisfies some desirable cryptographic criteria such as balancedness, nonlinearity, higher order nonlinearity, resiliency, correlation immunity, crosscorrelation, propogation criteria (PC) and global avalanche characteristics (GAC). It is not possible to optimize all the criteria simultaneously, therefore some tradeoffs among them are necessary. In the following sections, we discuss some important cryptographic criteria of Boolean functions.

2.6 Balancedness

A Boolean function is said to be *balanced* if the output column of the truth table contains equal number of 0's and 1's. That is, if the Hamming weight of $f \in \mathcal{B}_n$ is $w_H(f) = 2^{n-1}$. From the definition of WHT, it follows that $f \in \mathcal{B}_n$ is balanced if $W_f(0) = 0$.

From cryptographic point of view, balanced functions are very important. In case of an unbalanced function, the input and output variables have considerable dependence on each other, which may cause susceptible cryptanalysis attacks. Balanced functions have direct applications in various cryptosystems as combiner functions and filter functions. Due to their extensive applications in cryptography, it is considered an important problem to construct and analyze balanced functions. Many constructions of balanced functions are available in the literature [43, 134]. Zhang and Zheng [162] have presented construction of balanced Boolean functions for both even and odd number of inputs. For further study on balanced functions we refer to [43, 133–135, 162].

2.7 Nonlinearity

The Nonlinearity of Boolean functions is an important cryptographic criterion to be satisfied by the functions used in various cryptosystems. Boolean functions with high nonlinearity provide protection against different kind of attacks [57, 103, 107]. It is the minimum Hamming distance of $f \in \mathcal{B}_n$ to the set $\mathcal{A}_n$ of all affine functions.

$$nl(f) = \min\{d_H(f, g) : g \in \mathcal{A}_n\}.$$

The nonlinearity of f can also be measured in terms of its WHT as

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

For more results on Boolean functions possessing high nonlinearity we refer to [15, 17, 79, 80, 124, 126, 127, 135].

2.7.1 Bent functions

Bent functions are defined as a class of Boolean functions with maximum possible nonlinearity. Bent functions were introduced by Rathous [124], and exist only for even number of input variables. Due to their minimum correlation with affine functions, bent functions are optimally resistent toward best affine approximation attacks [56].

Definition 2.7.1. *A function* $f \in \mathcal{B}_n, n =$ *even, is called bent if its WHT values are* $W_f(\mathbf{a}) = \pm 1$ *for every* $\mathbf{a} \in \mathbb{F}_2^n$.

Although, the structure of bent functions is considered to be quit complicated, however, due to their applications in coding theory and cryptography, the work on bent functions has got special attention in the literature and an extensive research has been carried out on bent functions [8, 12, 38, 39]. There are several known classes of bent functions. The main constructions of bent functions have been given by Rathous [124], Dillon [40], Dobbertin [43], Canteaunt and Charpin [8], and Carlet [12].

Rathous [124] proposed two classes of bent functions. One of the classes of classical bent functions due to Rathous is defined as follows.

Rathous Construction: Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m, n = 2m$ and $g \in \mathcal{B}_m$. Then the function defined by

$$f(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \mathbf{y} \rangle + g(\mathbf{y}),$$

is bent.

Maiorana and McFarland [87, as cited in]have presented a generalization of above class of bent functions by replacing $\langle \mathbf{x}, \pi(\mathbf{y}) \rangle$ for $\langle \mathbf{x}, \mathbf{y} \rangle$, where $\pi(\mathbf{y})$ denotes a permutation of $\mathbf{y}$ in $\mathbb{F}_2^m$.

Maiorana-McFarland Construction: Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^m, n = 2m$ and $g(\mathbf{y}) \in \mathcal{B}_m$, then the function

$$f(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \pi(\mathbf{y}) \rangle + g(\mathbf{y}),$$

where $\pi(\mathbf{y})$ is permutation of $\mathbf{y}$ in $\mathbb{F}_2^m$, is bent.

For a detailed study on several constructions of bent functions, we refer to [8, 12, 40, 43, 124].

In the following results, we present some important properties of bent functions.

Theorem 2.7.2. *[87] The affine or linear translate of a bent function is again bent function. Symbolically, if $f(\mathbf{x})$ is a bent function, then*

$$F(\mathbf{x}) = f(\mathbf{x}) + \langle \mathbf{a}, \mathbf{x} \rangle + b, \quad \mathbf{a}, \mathbf{x} \in \mathbb{F}_2^m, \ b \in \mathbb{F}_2,$$

is also a bent function.

Theorem 2.7.3. *[87] If $f \in \mathcal{B}_m, g \in \mathcal{B}_n$ are any two bent functions, then the function*

$$h(x_{m+n}, \ldots, x_{m+1}, x_m, \ldots, x_1) = f(x_m, \ldots, x_1) + g(x_{m+n}, \ldots, x_{m+1}),$$

is a bent function on $m+n$ variables.

Theorem 2.7.4. *[39, Theorem 4.3] A function $f \in \mathcal{B}_n$ is bent if and only if its autocorrelation $C_f(\mathbf{a}) = 0$ for every non-zero $\mathbf{a} \in \mathbb{F}_2^n$.*

Theorem 2.7.5. *[39, Theorem 4.5] Let $f \in \mathcal{B}_n$ be a bent function. Then for $n > 2$, the degree of f is at most $\frac{n}{2}$.*

2.7.2 Semi-bent functions

In this section, we discuss another important class of cryptographic functions known as *semi-bent* functions. Semi-bent functions were introduced by Chee et. al. [30]. These functions exist for both even and odd number of input variables and defined as follows.

Definition 2.7.6. *[30] A function $f \in \mathcal{B}_n$ is called semi-bent if for every $a \in \mathbb{F}_{2^n}$, $W_f(a) \in \{0, \pm\sqrt{2}\}$, for n odd, and $W_f(a) \in \{0, \pm 2\}$, for n even.*

In the literature, semi-bent Boolean functions are also referred as plateaued functions [163] and 3-valued almost optimal functions [7]. It can be noted that well known Kasami functions given by $f(x) = tr_1^n(x^{2^{2r}-2^r+1})$ are semi-bent functions if $\gcd(n, r) = \gcd(n, 2r)$ [44, 78] . These functions are balanced up to the addition of linear functions.

It is important to note that semi-bent functions satisfy several cryptographic criteria simultaneously. Usually, semi-bent functions are balanced, resilient, having low autocorrelation values and satisfy PC. Semi-bent functions possess low WHT and have been extensively studied in cryptography. These functions when employed in any cryptosystem provide protection against fast correlation attacks [106], best affine approximation attacks [56] and linear cryptanalysis [103]. In the following results, we present some well known classes of semi-bent functions.

Theorem 2.7.7. *[55] Let $f \in \mathcal{B}_n$, n odd. Then $f(x) = tr_1^n(x^{2^i}+1)$ is semi-bent if and only if $gcd(i,n) = 1$.*

Theorem 2.7.8. *[3] Let $f \in \mathcal{B}_n$, n odd. Then $f(x) = \sum_{i=1}^{\frac{n-1}{2}} tr_1^n(x^{2^i}+1)$ is semi-bent if and only if $gcd(i,n) = 1$.*

Theorem 2.7.9. *[81] Let $f \in \mathcal{B}_n$, n odd, and $a_i \in \mathbb{F}_2$ for $1 \leq i \leq (n-1)/2$. Then $f(x) = \sum_{i=1}^{\frac{n-1}{2}} a_i tr_1^n(x^{2^i}+1)$ is semi-bent if and only if $gcd(a(x), x^n+1) = x+1$, where $a(x) = \sum_{i=1}^{\frac{n-1}{2}} a_i(x^i + x^{n-i})$.*

Khoo et al. [81] have further generalized the above result to the q-ary setup for q an odd prime, and obtained both q-ary bent and q-ary semi-bent functions. For more results on semi-bent functions we refer [23, 29, 55, 64, 65, 68, 108, 111].

2.8 Some known results on higher order nonlinearities

The notion of nonlinearity has been generalized to the higher order nonlinearities and nonlinearity profile. For every positive integer $r < n$, the r-th order nonlinearity $nl_r(f)$ of $f \in \mathcal{B}_n$ is the minimum Hamming distance of f to the set of all functions of degree at most r. The sequence $\{nl_r(f)\}_{1 \leq r \leq n-1}$ is called *nonlinearity profile* of f.

The r-th order nonlinearity of $f \in \mathcal{B}_n$ remains invariant under the addition of an n-variable Boolean function of algebraic degree at most r.

Lemma 2.8.1. *[74] Suppose $f, h \in \mathcal{B}_n$ and $r < n$. If $\deg(f) > r$ and $deg(h) \leq r$, then*

$$nl_r(f) = nl_r(f+h).$$

Proof. By definition of r-th order nonlinearity, we have

$$nl_r(f+h) = \min_{g\in\mathcal{R}(r,n)} d(f+h,g) = \min_{g\in\mathcal{R}(r,n)} d(f,g+h) = \min_{g\in\mathcal{R}(r,n)} d(f,g) = nl_r(f).$$

■

Iwata and Kurosawa [74] have introduced the *probabilistic higher order differential attack*. In order to provide protection against their proposed attack they have introduced the concepts of *higher order nonlinearity* and *higher order bent* functions.

Definition 2.8.2. *[74] A function $f \in \mathcal{B}_n$ is called r-th order bent if*

$$nl_r(f) \geq \begin{cases} 2^{n-r-3}(r+4), & \text{if } r \text{ is even,} \\ 2^{n-r-3}(r+5), & \text{if } r \text{ is odd,} \end{cases} \qquad \text{for } 0 \leq r \leq n-3.$$

They have pointed out that a bent function is a 1-st order bent function, but the converse is not true.

2.8.1 Recursive lower bounds on the nonlinearity profile

Carlet [15] has systematically studied the nonlinearity profile of Boolean functions. He introduced some techniques which lead to a recursive way of obtaining the lower bounds on the r-th order nonlinearity of a Boolean function in the case lower bounds exist for the $(r-1)$-th order nonlinearities of its derivatives. Carlet's lower bounds are useful in computing the lower bounds on r-th order nonlinearities of Boolean functions and are dependent on the nonlinearities of their derivatives.

The following results due to Carlet [15] are extensively used in determining the lower bounds of the r-th order nonlinearities of Boolean functions.

Proposition 2.8.3. *[15, Proposition 2] Let $f \in \mathcal{B}_n$ and r be a positive integer smaller than n. Then the r-th order nonlinearity of f satisfies the relation*

$$nl_r(f) \geq \frac{1}{2} \max_{a\in\mathbb{F}_{2^n}} nl_{r-1}(D_a f).$$

In terms of higher order derivatives

$$nl_r(f) \geq \frac{1}{2^i} \max_{a_1,a_2,\ldots,a_i \in \mathbb{F}_{2^n}} nl_{r-i}(D_{a_1} D_{a_2} \ldots D_{a_i} f)$$

for every positive integer $i < r$.

If the lower bound on the $(r-1)$-th order nonlinearity is known for all the derivatives (in non-zero directions) of the function, then we use the following proposition to determine the lower bounds on r-th order nonlinearity.

Proposition 2.8.4. *[15, Proposition 3] Let $f \in \mathcal{B}_n$ and r be a positive integer smaller than n. Then, we have*

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2 \sum_{a \in \mathbb{F}_{2^n}} nl_{r-1}(D_a f)}.$$

Applying Proposition 2.8.4 i times, we obtain the lower bound on $nl_r(f)$ in terms of i-th order derivatives of f as follows.

Corollary 2.8.5. *[15] Let $f \in \mathcal{B}_n$ and r be a positive integer smaller than n. Then*

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{\sum_{a_1 \in \mathbb{F}_{2^n}} \sqrt{\sum_{a_2 \in \mathbb{F}_{2^n}} \cdots \sqrt{2^{2n} - 2 \sum_{a_i \in \mathbb{F}_{2^n}} nl_{r-1}(D_{a_1} \cdots D_{a_i} f)}}},$$

where i is a positive integer smaller than r.

Remark 2.8.6. *In [15], Carlet remarked that, in general, the lower bounds given in Proposition 2.8.4 are potentially better than the bounds given in Proposition 2.8.3.*

Corollary 2.8.7. *[15, Corollary 2] Let $f \in \mathcal{B}_n$ and $r < n$. If for some non-negative integers m and M, $nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m$ for all non-zero $a \in \mathbb{F}_{2^n}$. Then*

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^{n-1})M2^{m+1} + 2^n}$$

$$\approx 2^{n-1} - \sqrt{M}2^{\frac{n+m-1}{2}}.$$

The Proposition 2.8.3, 2.8.4 and Corollary 2.8.7 are used for computation of the second order nonlinearity of Boolean functions. This is because of the fact, we have mentioned earlier, that the algebraic degree of the first derivative of a cubic Boolean function is at most 2, and the WHS of a quadratic Boolean function is completely characterized by the dimension of the kernel of the bilinear form associated with it.

Lemma 2.8.8. *[15, Remark] Let $f \in \mathcal{B}_n$ be a cubic function, then the second order nonlinearity $nl_2(f)$ of f satisfies $nl_2(f) \geq 2^{n-3}$. Further, if f has no affine derivative in non-zero directions, then*

$$nl_2(f) \geq 2^{n-1} - 2^{n-3/2}.$$

Proof. Given that f is a cubic Boolean function, so, there exists at least one element $a \in \mathbb{F}_{2^n}$ such that $D_a f$ is quadratic. Therefore, the WHS of $D_a f$ is $\{0, \pm 2^{\frac{n+k}{2}}\}$, where k is the dimension of the kernel $\varepsilon_{D_a f}$. By Proposition 2.5.1, we have $k \leq n-2$. Therefore, the nonlinearity of $D_a f$ is $nl(D_a f) = 2^{n-1} - \frac{1}{2}2^{\frac{n+k}{2}} \geq 2^{n-2}$. By Proposition 2.8.3, we have

$$nl_2(f) \geq 2^{n-3}. \tag{2.8.1}$$

If all the derivatives $D_a(f)$ for every $a \neq 0$ have algebraic degree exactly 2, then on comparing (2.8.1) and Corollary 2.8.7, we get $M = 1$ and $m = n-2$. Therefore, by Corollary 2.8.7, we obtain

$$nl_2(f) \geq 2^{n-1} - 2^{n-3/2}.$$

■

The following result is used to improve the bounds of the rth-order nonlinearities of Boolean functions and known as McEliece's theorem.

Proposition 2.8.9. *[96, Chapter 15] If $\lfloor a \rfloor$ denotes the integer part of a and $\lceil a \rceil$ the smallest integer $\geq a$, then the rth-order nonlinearity $nl_r(f)$ of $f \in \mathcal{B}_n$ with algebraic degree d is divisible by $2^{\lceil \frac{n}{d} \rceil - 1} = 2^{\lfloor \frac{n-1}{d} \rfloor}$.*

2.8.2 Second order nonlinearities of some classes of cubic Boolean functions

Sun and Wu [146, Theorem 1, 2 and 3] have deduced the lower bounds on second order nonlinearities of some classes of highly nonlinear cubic Boolean functions of the form $tr_1^n(x^k)$ for different values of k. These are summarized in the following result.

Lemma 2.8.10. *[146] Let $f \in \mathcal{B}_n$ be a cubic function such that*

$$f(x) = tr_1^n(x^k), \text{ for all } x \in \mathbb{F}_{2^n},$$

where

(i) $k = 2^{m+1} + 3$, $n = 2m$ and m is odd. Then

$$nl_2(f) \geq 2^{2m-1} - \frac{1}{2}\sqrt{2^{5m/2+1} + 2^{3m+1} - 2^{2m} - 2^{3m/2+1}}.$$

(ii) $k = 2^m + 2^{\frac{m+1}{2}} + 3$, $n = 2m$ and m is odd. Then

$$nl_2(f) \geq 2^{2m-1} - \frac{1}{2}\sqrt{2^{5m/2+1} + 2^{3m+1} - 2^{2m} - 2^{3m/2+1}}.$$

(iii) $k = 2^{2r} + 2^{r+1} + 1$, $n = 4r$. Then

$$nl_2(f) \geq 2^{4r-1} - \frac{1}{2}\sqrt{2^{5r+1} + 2^{6r+2} - 2^{3r+1} - 3.2^{4r}}.$$

It is to be noted that the WHS of the functions defined above in first two cases (case (i) and case (ii)) is three valued multiset with values from the set $\{0, \pm 2^{m+1}\}$ [35,146], and hence these functions are semi-bent, whereas, the functions in case (iii) are bent [89].

In [147], Sun and Wu have investigated a class of highly nonlinear cubic Boolean functions of the form $Tr_1^n(\lambda x^{2^{2r}+2^r+1})$, $\lambda \in \mathbb{F}_{2^r}^*$ with $n = 4r$. The following lemma describes the lower bound on second-order nonlinearities of these functions.

Lemma 2.8.11. *[147, Theorem 1] Let $f \in \mathcal{B}_n$ be defined as $f(x) = Tr_1^n(\lambda x^{2^{2r}+2^r+1})$, for all $x \in \mathbb{F}_{2^n}$, where $\lambda \in \mathbb{F}_{2^r}^*$ and $n = 4r$. Then*

$$nl_2(f) \geq 2^{4r-1} - 2^{2r-1}\sqrt{2^{3r} + 2^r - 1}.$$

Gangopadhyay et al. [50, Theorem 2] have obtained the lower bound on second order nonlinearities of a class of cubic bent functions in MM class. These bounds are provided in the following result.

Lemma 2.8.12. *[50, Theorem 2] If $f(x, y) = Tr_1^p(xy^{2^i+1})$ for all $x, y \in \mathbb{F}_{2^p}$, where $n = 2p$, $n \geq 6$ and i is a positive integer such that $1 \leq i < p, \gcd(2^p-1, 2^i+1) = 1$ and $\gcd(i, p) = e$, then*

$$nl_2(f) \geq 2^{2p-1} - \frac{1}{2}\sqrt{2^{3p+e} - 2^{\frac{3p+e}{2}} + 2^{2p}(2^{\frac{p+e}{2}} - 2^e + 1)}. \tag{2.8.2}$$

For $n = 10$, these functions reach the maximum known bound of second order nonlinearity ($nl_2(f) = 400$).

Gode and Gangopadhyay [53] have provided the lower bounds on second order nonlinearities of more general classes of cubic Boolean functions. Li et al. [91] have deduced the lower bounds of second order nonlinearities of more general classes of cubic Boolean functions with multiple trace terms.

2.9 Correlation immunity and resiliency

The correlation immune functions were introduced by Siegenthaler [140].

Definition 2.9.1. *An n-variable Boolean function f is said to be correlation immune of order r if $W_f(\mathbf{a}) = 0$ for every $\mathbf{a} \in \mathbb{F}_2^n$ with $1 \leq w_H(\mathbf{a}) \leq r$. A balanced correlation immune function of order r is known as r-resilient function.*

The functions used in various LFSR based stream ciphers as a combiner function or filter function are required to satisfy multiple cryptographic criteria, among them are balancedness, correlation immunity and nonlinearity. However, all these criteria can not be

optimized together. Perhaps bent functions are the most suitable example. Bent functions possess maximum possible nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1}$ and are able to prevent linear attacks [103]. But they are improper for direct cryptographic applications as they are neither balanced nor correlation immune. Therefore, it is important to obtain functions which are highly nonlinear as well as resilient. A lot of work has been reported in this direction [11,13,31,98,121,125,130,140,149,158,161]. Recently, Gao et al. [52] have constructed plateaued resilient Boolean functions with disjoint spectra having good nonlinearity.

For detailed study on resilient functions we refer to [11, 13, 31, 46, 98–100, 121, 126, 127, 129, 130, 134, 140, 149, 158, 161].

2.10 Algebraic immunity

Algebraic immunity $AI(f)$ of a Boolean function is the measure of resistance against various algebraic attacks [33, 34, 62]. High algebraic immunity is a necessary condition for Boolean functions used in various cryptosystems to resist algebraic attacks [19, 37].

Definition 2.10.1. *Let $f \in \mathcal{B}_n$. Then $g \in \mathcal{B}_n$ is called an annihilator of f if g is not identically zero and $g(\mathbf{x})f(\mathbf{x}) = 0$ for every $\mathbf{x} \in \mathbb{F}_2^n$. The algebraic immunity of $f \in \mathcal{B}_n$ is defined by*

$$AI(f) = \min\{\deg(g) : g \in AN(f) \cup AN(f+1)\}$$

where, $AN(f) = \{g \in \mathcal{B}_n : gf = 0, g \neq 0\}$ is the set of annihilators of f.

The higher order nonlinearity and algebraic immunity of a Boolean function are closely related. In connection with this, we provide following two results.

Lemma 2.10.2. *[19, Theorem 2] Let $f \in \mathcal{B}_n$ and r be a positive integer smaller than n. If $nl(f) \leq \sum_{i=0}^{d} \binom{n}{i}$, then $AI(f) \leq d+1$. More generally if $nl_r(f) \leq \sum_{i=0}^{d} \binom{n}{i}$, then $AI(f) \leq d + r$. In other words $nl_r(f) \geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i}$.*

Lemma 2.10.3. *[14, Theorem 1] Let $f \in \mathcal{B}_n$ and $r < n$. If $AI(f) \leq r$ and f is a balanced function, then $nl_r(f) \leq 2^{n-1} - 2^{n-r}$.*

2.11 Crosscorrelation and autocorrelation

The crosscorrelation is one of the important cryptographic criteria. From cryptographic point of view, it is good if the component functions of a secret key cryptosystem have low crosscorrelation or low autocorrelation. To estimate the correlation between two arbitrary Boolean functions, crosscorrelation plays an important role [128]. The crosscorrelation $C_{f,g}(\mathbf{u})$ between two Boolean functions f and g at $\mathbf{u} \in \mathbb{Z}_2^n$ is defined as

$$C_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{x})+g(\mathbf{x}+\mathbf{u})}.$$

For $f = g$, $C_{f,f}(\mathbf{u}) = C_f(\mathbf{u})$ is called autocorrelation of f at $\mathbf{u}$ and defined as

$$C_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{x})+f(\mathbf{x}+\mathbf{u})}.$$

Since the function $D_{\mathbf{u}}(f,g) = f(\mathbf{x})+g(\mathbf{x}+\mathbf{u})$ represents the derivative of f and g at $\mathbf{u} \in \mathbb{Z}_2^n$, the crosscorrelation between f and g can also be defined in terms of derivative $D_{\mathbf{u}}(f,g)$ of f and g as

$$C_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{D_{\mathbf{u}}(f,g)}.$$

During last few decades the crosscorrelation and the autocorrelation of cryptographic functions have attracted a lot of research and have been studied in various forms. Sarkar and Maitra [128] have studied crosscorrelation of Boolean functions and proved the Crosscorrelation Theorem, which provides an important relationships between the crosscorrelation spectrum and the WHS of Boolean functions. The next result states the Crosscorrelation Theorem [128].

Lemma 2.11.1. *[128, Theorem 3.1] Let $f, g \in \mathcal{B}_n$, then*

$$[C_{f,g}(0), \ldots, C_{f,g}(2^n-1)]H_n = [W_f(0)W_g(0), \ldots, W_f(2^n-1)W_f(2^n-1)],$$

where H_n is the Hadamard matrix of order 2^n such that $H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $H_n = H_1 \otimes H_{n-1}$,

and $\otimes$ represents the Kronecker product of matrices.

Also, they have provided a new characterization of bent functions in terms of the cross-correlation and the autocorrelation of its subfunctions [128].

In [102], Maitra and Sarkar have provided modifications of Patterson-Wiedemann (PW) type functions and observed that the autocorrelation spectra of these functions are very useful for cryptographic applications. In [49] Gangopadhyay and Maitra have investigated the crosscorrelation spectrum of Dillon and Patterson-Wiedemann type functions and used the results to obtain the autocorrelation spectrum of these functions. They have also justified why the maximum absolute values in the autocorrelation spectra of PW type functions are low.

2.12 Strict avalanche criteria and propagation criteria

Webster and Tavares [156] have introduced the concept of *strict avalanche criteria* (SAC). A function $f \in \mathcal{B}_n$ is said to satisfy SAC if on changing any one bit of the input vector $x \in \mathbb{F}_{2^n}$ results in the output of the function changed for exactly half of the vectors. A function $f \in \mathcal{B}_n$ satisfying SAC implies a slight change in the input of the function provides a large change in the output, i.e., an avalanche effect. Also, it has been observed that the large change in output is of uniform kind and hence the name strict avalanche criterion. This property of the functions is useful for their cryptographic applications [63, 156].

Lemma 2.12.1. *[156] The function $f \in \mathcal{B}_n$ satisfies the SAC if and only if its derivative $D_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x}) + f(\mathbf{x}+\mathbf{a})$ is balanced for every $\mathbf{a} \in \mathbb{F}_2^n$ with $w_H(\mathbf{a}) = 1$.*

It is well known that the autocorrelation of an affine function $f \in \mathcal{B}_n$ is either 0 or 2^n. Therefore, the following result follows from Lemma 2.12.1.

Lemma 2.12.2. *[36, Lemma 3.9] A function $f \in \mathcal{B}_n$ satisfies SAC if and only if the autocorrelation $C_f(\mathbf{a})$ is equal to 2^{n-1} for every $\mathbf{a} \in \mathbb{F}_2^n$ with $w_H(\mathbf{a}) = 1$.*

Preneel et al. [122] have generalized the concept of SAC to the *propagation criterion* (PC). A function $f \in \mathcal{B}_n$ is said to satisfy the PC with respect to $\mathbf{a} \in \mathbb{F}_2^n$ if $f(\mathbf{x}) =$

$f(\mathbf{x}) + f(\mathbf{x} + \mathbf{a})$ is balanced, and to satisfy PC of degree k, PC(k), if it satisfies the PC with respect to all non-zero vectors of Hamming weight at most k. In other words, $f \in \mathcal{B}_n$ satisfies PC(k) if on complementing k or less bits in the input vectors, the output of f is changed for exactly half of 2^n vectors. Therefore, PC(1) is identical to SAC and the functions satisfying PC of degree n coincide with bent functions. Thus, the SAC and the PC describe the behavior of the cryptographic function when the coordinates of the input vectors are complemented. Observe that the SAC and its generalization PC both are measured in terms of the properties of the derivative of the function and hence are closely related with the autocorrelation of the function.

Lemma 2.12.3. *[36, Lemma 3.24] A function $f \in \mathcal{B}_n$ satisfies PC(k) if and only if all the values of the autocorrelation function*

$$C_f(\mathbf{a}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x})+f(\mathbf{x}+\mathbf{a})}, \;\; 1 \leq w_H(\mathbf{a}) \leq k$$

are equal to 2^{n-1}.

2.13 Global avalanche characteristics (GAC)

Zhang and Zheng [162] have introduced the concept of *global avalanche characteristics* (GAC) and mentioned that a function is said to have good avalanche characteristics if it does not possess non-zero linear structure and satisfies PC with respect to the majority of the vectors. They have observed that although the PC is a generalization of SAC, however it is also another cryptographic criterion which describes the local properties of a cryptographic function. They remark that there is a need to search a new cryptographic criterion for the functions that should overcome the shortcomings of SAC and PC. The new criterion should be able to forecast and explain the overall avalanche characteristics of a function.

Zhang and Zheng [162] have proposed two indicators: the *sum-of-square indicator* σ_f and the *absolute indicator* $\triangle_f$ related to the autocorrelation of a Boolean function f that forecast the GAC of a cryptographic function.

Definition 2.13.1. *[162] Let $f \in \mathcal{B}_n$. Then the sum-of-squares indicator of f is defined as $\sigma_f = \sum_{\mathbf{x}\in\mathbb{F}_2^n} C_f^2(\mathbf{x})$, and the absolute indicator of f is defined as $\triangle_f = \max_{\mathbf{x}\in\mathbb{F}_2^n} |C_f(\mathbf{x})|$.*

They have constructed some cryptographic functions which satisfy overall avalanche characteristics.

Zhou et. al [166] have generalized this concept and proposed two new indicators *sum-of-squares indicator* and *absolute indicator* related to the crosscorrelation of two Boolean functions to study the global behavior of the functions.

Definition 2.13.2. *[166] Let $f, g \in \mathcal{B}_n$. Then the sum-of-squares indicator [166] for f and g is defined as $\sigma_{f,g} = \sum_{\mathbf{x}\in\mathbb{F}_2^n} C_{f,g}^2(\mathbf{x})$, and the absolute indicator for f and g is defined as $\triangle_{f,g} = \max_{\mathbf{x}\in\mathbb{F}_2^n} |C_{f,g}(\mathbf{x})|$.*

They have provided some interesting results regarding lower and upper bounds of these indicators. These bounds are listed in the following results.

Theorem 2.13.3. *[166, Theorem 5] If $f, g \in \mathcal{B}_n$, then $(C_{f,g}(\mathbf{0}))^2 \leq \sigma_{f,g} \leq 2^{3n}$. Moreover, $\sigma_{f,g} = 2^{3n}$ if and only if f and g are affine functions, and $\sigma_{f,g} = (C_{f,g}(\mathbf{0}))^2$ if and only if f and g are perfectly uncorrelated or f and g are bent functions.*

Theorem 2.13.4. *[166, Theorem 4] If $f, g \in \mathcal{B}_n$, then $0 \leq \triangle_{f,g} \leq 2^n$. Moreover, $\triangle_{f,g} = 0$ if and only if $f(\mathbf{x}) + g(\mathbf{x} + \mathbf{a})$ is a balanced function for every $\mathbf{a} \in \mathbb{F}_2^n$, and $\triangle_{f,g} = 2^n$ if and only if $f(\mathbf{x}) = g(\mathbf{x} + \mathbf{a}) + b$ for some $\mathbf{a} \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$.*

For $f = g$, the above two results regarding upper and lower bounds on two indicators, coincide with the results due to Zhang and Zheng [162].

Further, Zhou et al. [166] have established some relationship among these indicators and higher order nonlinearities, these are listed in the following theorem.

Theorem 2.13.5. *[166, Theorem 7 and 8] Let $f, g \in \mathcal{B}_n$ such that $deg(g) \leq r$. Then*

1. $\triangle_{f,g} \leq 2^n - 2nl_r(f)$.
2. $\triangle_{f,g} \leq \sqrt{2^{2n} - 2\sum_{\mathbf{a}\in\mathbb{F}_2^n} nl_{r-1}(D_{\mathbf{a}}(f))}$.

3. $\sigma_{f,g} \leq 2^{3n} - 2^{2n+2} nl_r(f) + 2^{n+2} nl_r^2(f)$.

4. $\sigma_{f,g} \leq 2^{3n} - 2^{n+1} \sum_{\mathbf{a} \in \mathbb{F}_2^n} nl_{r-1}(D_{\mathbf{a}}(f))$.

In [162], Zhang and Zheng have given the following conjecture for balanced Boolean functions with algebraic degree at least 3.

Conjecture 2.13.6. *Let $f \in \mathcal{B}_n$, n odd, be a balanced function with algebraic degree ≥ 3. Then $\triangle_f \geq 2^{\frac{n+1}{2}}$.*

The conjecture was disproved in 2002 by Maitra and Sarkar [102] by introducing suitable modifications in Patterson-Wiedmann type functions. They have shown that a balanced Boolean function f on $n = 15$ can be constructed with $\triangle_f = 216 < 2^{\frac{15+1}{2}}$. Later on in 2006 the conjecture was again disproved in [48] for $n = 21$.

2.14 Nega-bent functions

Parker and Riera have extended the concept of bentness to some generalized bent criteria by analyzing Boolean functions having flat spectrum with respect to one or more unitary transforms [118, 123]. The transforms they have chosen are n-fold tensor product of the identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the Walsh-Hadamard matrix $W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and the nega-Hadamard matrix $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, $i^2 = -1$.

The *nega-Hadamard transform* (NHT), $N_f : \mathbb{Z}_2^n \to \mathbb{C}$ of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is defined as

$$N_f(\mathbf{u}) = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + \langle \mathbf{x}, \mathbf{u} \rangle} i^{w_H(\mathbf{x})}.$$

A function $f \in \mathcal{B}_n$ is *negabent* if $|N_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. The multiset $\{N_f(\mathbf{u}) : \mathbf{u} \in \mathbb{Z}_2^n\}$ is called the *nega-Hadamard spectrum* of f.

Let $f, g \in \mathcal{B}_n$. Then the sum

$$C_{f,g}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + g(\mathbf{x}+\mathbf{u})} (-1)^{\langle \mathbf{x}, \mathbf{u} \rangle}$$

is called the *nega-crosscorrelation* between f and g at $\mathbf{u} \in \mathbb{Z}_2^n$. For $f = g$, $C_f(\mathbf{u}) = C_{f,f}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{x})+f(\mathbf{x}+\mathbf{u})}(-1)^{\langle \mathbf{x},\mathbf{u}\rangle}$ is called the *nega-autocorrelation* of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{Z}_2^n$.

The functions which are both bent and negabent are called bent-negabent functions and are of recent interest [144, 145]. Parker and Pott [119] have provided a necessary and sufficient condition for a quadratic Boolean function to be bent-negabent. The maximum possible degree of an n variable negabent functions is $\lceil \frac{n}{2} \rceil$ [144]. Schmidt et al. [132] have shown that the algebraic degree of a bent-negabent function on even number of variables in MM bent class is at most $\frac{n}{2} - 1$.

The following results are due to Schmidt et al. [132].

Theorem 2.14.1. *[132, Theorem 2] Let $f, g \in \mathcal{B}_n$. Suppose*

$$g(\mathbf{x}) = f(A\mathbf{x} + \mathbf{b}) + \langle \mathbf{c}, \mathbf{x}\rangle + d,$$

where $\mathbf{b}, \mathbf{c} \in \mathbb{Z}_2^n, d \in \mathbb{Z}_2$ and A is any matrix from orthogonal group of $n \times n$ matrices over $\mathbb{Z}_2$. Then, g is a bent-negabent function if f is bent-negabent.

Theorem 2.14.2. *[132, Theorem 10] Let $n = 2m$ and $g \in \mathcal{B}_m$. Suppose that the function $f : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2$ defined as*

$$f(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \pi(\mathbf{y})\rangle + g(\mathbf{y})$$

is negabent. Then for $n > 3$, the degree of f is at most $m - 1$.

Stănică et al. [144] have provided a method to construct bent-negabent functions using complete mapping polynomials. Further, they have shown that for every $r \geq 2$, there exist bent-negabent functions on $n = 12r$-variables with algebraic degree $\frac{n}{4} + 1 = r + 1$.

Theorem 2.14.3. *[144, Theorem 17] Let $n = 2m$. Then for $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n$ and $g \in \mathcal{B}_m$ the function*

$$f(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \pi(\mathbf{y})\rangle + g(\mathbf{y}),$$

where π is a permutation such that $w_H(\mathbf{x}+\mathbf{y}) = w_H(\pi(\mathbf{x})+\pi(\mathbf{y}))$, is bent-negabent function if and only if g is bent function.

Recently, Su et al. [145] have presented a necessary and sufficient conditions for n variable Boolean functions to be negabent for both the cases n even and n odd. They have constructed bent-negabent functions of maximum algebraic degree.

Theorem 2.14.4. *[145, Theorem 5] Let $f \in \mathcal{B}_n$ be a function defined as*

$$f(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \pi(\mathbf{y}) \rangle + g(\mathbf{y}), \quad \mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^m$$

such that $\pi(\mathbf{y})$ and $\pi(\mathbf{y}) + \mathbf{y}$ are permutations on $\mathbb{Z}_2^m$ and $g \in \mathcal{B}_m$. Then the function

$$f^{'}(\mathbf{x}, \mathbf{y}) = f((\mathbf{x}, \mathbf{y}) \cdot OA + \mathbf{a}) + \langle \mathbf{b}, \mathbf{x} \rangle + c$$

is a bent-negabent with $deg(f) = deg(f^{'})$, for every $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^m, c \in \mathbb{Z}_2$, and every $A \in GL(n, \mathbb{Z}_2)$, and $n \times n$ orthogonal matrix O over $\mathbb{Z}_2$.

For more results related to the several properties of nega-Hadamard transform and constructions of bent-negabent functions we refer to [119, 123, 132, 144, 145].

2.15 q-ary functions

Recently, many generalizations of Boolean bent functions have been proposed by several authors [70, 87, 131]. Many analogous properties of these functions have been studied in the generalized set up. A natural generalization of Boolean bent functions was presented by Kumar et al. [87]. They have considered the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, where $\mathbb{Z}_q$ is the ring of integers modulo q. These functions are called q-ary functions. Let $\mathcal{B}_{n,q}$ be the set of all such q-ary functions.

The Walsh Hadamard transform (WHT) $\mathcal{W}_f : \mathbb{Z}_q^n \to \mathbb{C}$ of $f \in \mathcal{B}_{n,q}$ at $\mathbf{u} \in \mathbb{Z}_q^n$ is defined as

$$\mathcal{W}_f(\mathbf{u}) = \frac{1}{q^{n/2}} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{f(\mathbf{x}) + \langle \mathbf{u}, \mathbf{x} \rangle},$$

where $\xi = e^{\frac{2\pi i}{q}}$ is the complex q-th primitive root of unity. A function $f \in \mathcal{B}_{n,q}$ is called *q-ary bent* if $|\mathcal{W}_f(\mathbf{u}) = 1|$ for all $\mathbf{u} \in \mathbb{Z}_q^n$. Kumar et al. [87] have generalized Maiorana-McFarland

(MM) type Boolean bent functions to the q-ary set up as follows.

Let $n = 2m$. Then the function

$$f(\mathbf{x}) = g(\mathbf{x}) + \langle \pi(\mathbf{x}), \mathbf{y} \rangle,$$

where $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^m$ and $g : \mathbb{Z}_q^m \to \mathbb{Z}_q$, and π is a permutation of the elements of $\mathbb{Z}_q^m$, is q-ary bent. This class of q-ary bent functions is known as generalized Maiorana-McFarland (GMM) type q-ary bent functions.

Let $f, g \in \mathcal{B}_{n,q}$. The sum

$$\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{f(\mathbf{x}) - g(\mathbf{x}+\mathbf{u})},$$

is called the crosscorrelation between the functions f and g at $\mathbf{u} \in \mathbb{Z}_q^n$. Further, for $f = g$, the sum $\mathcal{C}_{f,f}(\mathbf{u}) = \mathcal{C}_f(\mathbf{u})$ is called the autocorrelation of f at $\mathbf{u}$.

An $n \times n$ matrix $\mathcal{A}$ with entries as integral powers of a complex primitive n-th root of unity ξ, is called *generalized Hadamard matrix* [151] if

$$\mathcal{A}\mathcal{A}^* = nI_n,$$

where I_n denotes identity matrix and $\mathcal{A}^*$ the transpose of conjugate matrix of $\mathcal{A}$.

Theorem 2.15.1. *[151, Theorem 2] The following statements are equivalent:*

1. *a q-ary function f is bent,*
2. *the matrix $\mathcal{A} = (a_{i,j})$ with $a_{i,j} = \xi^{i+j}$ is a generalized Hadamard matrix.*

For $q = 2$ the concept of q-ary bent functions coincides with the concept of classical Boolean bent functions [87, 124, 151].

Let $f \in \mathcal{B}_{n,q}$ and $b \in \mathbb{Z}_q$. Then the function F defined as

$$F(\mathbf{x}) = f(\mathbf{x}) + \langle \mathbf{a}, \mathbf{x} \rangle + b, \ \mathbf{x} \in \mathbb{Z}_q^n$$

is called an affine traslate of f if $b \neq 0$, and a linear translate of f if $b = 0$ and $a \neq 0$.

The following results are due to Kumar et al. [87] in which they have established several properties of q-ary bent functions.

Theorem 2.15.2. *[87] The q-ary functions satisfy the following properties.*

1. *Every linear or affine translate of a q-ary bent function is a q-ary bent.*
2. *The property of q-ary bentness is invariant under an affine or linear translate of coordinates.*
3. *Let $f \in \mathcal{B}_{m,q}$ and $g \in \mathcal{B}_{n,q}$ are two q-ary bent functions, then the function defined as*

$$h(x_{m+n}, ..., x_1) = f(x_m, ..., x_1) + g(x_{m+n}, ..., x_{m+1})$$

is also q-ary bent.

In the following result Kumar et al. [87] have presented an important characterization of q-ary bent functions in terms of their autocorrelation spectrum.

Lemma 2.15.3. *[87] A function $f \in \mathcal{B}_{n,q}$ is q-ary bent if and only if autocorrelation $\mathcal{C}_f(\mathbf{u})$ is identically zero for every non-zero value of $\mathbf{u}$, i.e., if and only if*

$$\mathcal{C}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{f(\mathbf{x}) - f(\mathbf{x}+\mathbf{u})} = \begin{cases} 0 & \text{if } \mathbf{u} \neq 0, \\ q^n & \text{if } \mathbf{u} = 0. \end{cases}$$

They have identified values of q for which q-ary bent functions do not exist.

Theorem 2.15.4. *[87, Property 6] Let n be an odd integer and $q \equiv 2 \mod 4$. Further if $q = 2$ or $q \neq 2$ and there exists an integer a such that $2^a \equiv -1 \mod (\frac{q}{2})$, then there do not exist bent functions over $\mathbb{Z}_q^n$.*

Hou [70] has extended the study of q-ary bent functions to the chain rings. A chain ring is defined as a finite local principal ideal ring. He has provided construction of q-ary bent functions over chain rings and observed that these functions are free $\mathbb{Z}_q$-modules.

Helleseth and Kholosha [67] have considered quadratic p-ary ($p \geq 3$ prime) functions of the form $f(x) = tr_1^n(ax^{p^i+1}), a \in \mathbb{Z}_{p^n}$, and deduced a criterion on a for which f is a

p-ary bent function. They have shown that all the existing monomial quadratic p-ary bent functions are contained in this class of p-ary bent functions.

Recently, Youssef [159] has generalized the concept of binary hyperbent functions to the q-ary setup and proved that p-ary ($p \geq 3$ prime) hyperbent functions are quadratic. He has provided a necessary and sufficient conditions for a function to be a hyperbent functions as follows:

Suppose $T_{i_1}(A)$ is the matrix obtained after deleting i_1th row and i_1th column of A, $T_{i_2 i_1}(A)$ is the matrix obtained after deleting i_2th row and i_2th column of $T_{i_1}A$ and so on.

Theorem 2.15.5. *[159, Theorem 1] Let A be the coefficient matrix of the quadratic form of f defined as*

$$f(x) = \sum_{i,j=1}^{n} C_{ij} x_i x_j.$$

Let $g(x)$ be an arbitrary affine function over $\mathbb{Z}_p$. Then the function $h(x) = f(x) + g(x)$ is a p-ary hyperbent if and only if $rank(A) = n$ and $rank(T_{i_m \ldots i_1}(A)) = n - m, 1 \leq m \leq n-1,\ 1 \leq i_j \leq n - j + 1$.

In [72], Hou has presented p-ary and q-ary ($q = p^n, p =$ prime) versions of some important results of binary bent functions and binary resilient functions by using non-normalized version of WHT. In particular, by using the Teichmüller character and Gauss sums, he has presented a characterization of some q-ary resilient functions in terms of their coefficients. He has studied p-ary bent functions and obtained tight upper bounds on their degrees.

Theorem 2.15.6. *[72, Proposition 4.4] Let $f \in \mathcal{B}_{n,p}$ be a bent function. Then*

$$\deg f \leq \frac{(p-1)n}{2} + 1.$$

In 2006, Khoo et al [81], have obtained a new characterization of quadratic bent and semi-bent functions on $\mathbb{Z}_p$. The functions of the form $tr_1^n(x^{p^i} + 1)$ are called Gold functions. Using polynomial GCD computation, they have shown whether a $\mathbb{Z}_p$-linear combination of functions $tr_1^n(x^{p^i} + 1)$ is p-ary bent or semi-bent.

Solé and Tokerava [142] have provided a systematic link among Boolean bent functions, generalized Boolean bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_4$ due to Schmidt [131], and quaternary

(4-ary) bent functions. Let $\mathcal{GB}_n^q$ denotes the set of all generalized Boolean functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$ due to Schmidt [131]. Let $f \in \mathcal{GB}_{2n}^4$ defined as $f(\mathbf{x},\mathbf{y}) = a(\mathbf{x},\mathbf{y}) + 2b(\mathbf{x},\mathbf{y})$, where $a, b \in \mathcal{B}_{2n}$ and $\mathbf{x},\mathbf{y} \in \mathbb{Z}_2^n$. Let $g \in \mathcal{B}_{n,4}$ be such that $g(\mathbf{x}+2\mathbf{y}) = f(\mathbf{x},\mathbf{y})$. Solé and Tokareva have investigated the relationship among bentness criteria by using non-normalized WHT for these functions defined in three different contexts. Some of their results are listed in Theorem 2.15.7 and Theorem 2.15.8 below.

Theorem 2.15.7. *[142, Theorem 32] Let $f(\mathbf{x},\mathbf{y}) = a(\mathbf{x},\mathbf{y}) + 2b(\mathbf{x},\mathbf{y})$, where $a, b \in \mathcal{B}_{2n}$ and $\mathbf{x},\mathbf{y} \in \mathbb{Z}_2^n$. Then the following two statements are equivalent:*

1. *f is generalized Boolean bent function.*
2. *Both $a+b$ and b are Boolean bent functions.*

Theorem 2.15.8. *[142, Theorem 34] Let $g(\mathbf{x}+2\mathbf{y}) = f(\mathbf{x},\mathbf{y})$, where $f(\mathbf{x},\mathbf{y})$ is as defined in Theorem 2.15.7. Then the following two statements are equivalent:*

1. *$g \in \mathcal{B}_{n,4}$ is quaternary bent function.*
2. *$b, a+b \in \mathcal{B}_{2n}$ are bent correlated.*

The following results are due to Jadda and Parraud [75] derived by using non-normalized form of WHT of the functions.

Definition 2.15.9. *[75] Let $\eta_i(f) = |supp_i(f)| = |\{\mathbf{x} \in \mathbb{Z}_4^n : f(\mathbf{x}) = i\}|$, $\forall\ i \in \mathbb{Z}_4$. Then $f \in \mathcal{B}_{n,4}$ is called balanced if and only if $\eta_i(f) = 4^{n-1}$, for every $i \in \mathbb{Z}_4$.*

Theorem 2.15.10. *[75, Proposition 1] Let f be a quaternary function then f is balanced if and only if $\mathcal{W}_f(0) = \mathcal{W}_f^2(0) = 0$, where $\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_4^n} i^{f(\mathbf{x})+\langle \mathbf{u},\mathbf{x}\rangle}$ and $\mathcal{W}_f^2(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_4^n} i^{f(\mathbf{x})+\langle \mathbf{u},\mathbf{x}\rangle}$.*

A function $f \in \mathcal{B}_{n,q}$ is said to be *balanced* if $|\{\mathbf{x} :\ f(\mathbf{x}) = k\}| = q^{n-1}$ for all $k \in \mathbb{Z}_q$.

In the same paper [75], they have introduced the concept of $\mathbb{Z}_4$-nonlinearity and obtained separate expressions for $\mathbb{Z}_4$-nonlinearity of quaternary functions under the Hamming metric and the Lee metric. Similar to binary case, the $\mathbb{Z}_4$-nonlinearities $nl_4^H(f)$ and $nl_4^L(f)$ of

$f \in \mathcal{B}_{n,4}$ are the minimum Hamming distance and minimum Lee distance, respectively from the set of all affine functions.

Çeşmelioğlu et al. [27] have constructed self-dual non-quadratic p-ary bent functions for $p \equiv 1 \mod 4$, and presented some results regarding self-dual p-ary bent functions with $p \equiv 3 \mod 4$. In [26], Çeşmelioğlu et al. have analyzed a class containing p-ary bent functions, which includes MM q-ary bent class as a special case. This class contains several types of p-ary bent functions such as regular bent functions, weakly regular bent functions and not weakly regular bent functions.

Recall that a function with minimum absolute WHT values is called q-ary bent, i.e., $f \in \mathcal{B}_{n,q}$ is q-ary bent if $|\mathcal{W}_f(\mathbf{u})| = 1$ for every $\mathbf{u} \in \mathbb{Z}_q^n$ [87, 124, 151]. A function $f \in \mathcal{B}_{n,q}$ is called *s-plateaued* if $|\mathcal{W}_f(\mathbf{u})| \in \{0, q^{\frac{s}{2}}\}$ for all $\mathbf{u} \in \mathbb{Z}_q^n$ [24, 25]. The case $s = 0$ (respectively $s = 1, 2$) corresponds to q-ary bent (respectively semi-bent) functions and $s = n$ to affine or constant functions. [24, 25]. Çeşmelioğlu and Meidl [25] have presented a method for the construction of p-ary bent functions by using s-plateaued functions.

Theorem 2.15.11. *[25, Theorem 2] Let $f_{\mathbf{u}} \in \mathcal{B}_{n,p}$, $\mathbf{u} = (u_s, \ldots, u_1) \in \mathbb{Z}_p^s$, be an s-plateaued function. If $supp(\mathcal{W}_{f_{\mathbf{u}}}) \cap supp(\mathcal{W}_{f_{\mathbf{v}}}) = \emptyset$ for $\mathbf{u} \neq \mathbf{v}, \mathbf{u}, \mathbf{v} \in \mathbb{Z}_p^s$, then the function $g(\mathbf{x}, y_s, \ldots, y_1) \in \mathcal{B}_{n+s,p}$ defined as*

$$g(\mathbf{x}, y_s, \ldots, y_1) = \sum_{\mathbf{u} \in \mathbb{Z}_p^n} \frac{(-1)^s \prod_{i=1}^{s} y_i(y_i - 1) \cdots (y_i - (p-1)) f_{\mathbf{u}}(\mathbf{x})}{(y_1 - u_1) \cdots (y_s - u_s)},$$

is p-ary bent.

Further, they have described a method to construct a set of s-plateaued functions having pairwise disjoint support of their WHT from given s-plateaued functions.

Theorem 2.15.12. *[25, Lemma 1] Let $f \in \mathcal{B}_{n-s,p}, s < n$ an integer and $\mathbf{u} = (u_n, \ldots, u_{n-s+1}) \in \mathbb{Z}_p^s$. Then the function*

$$f_{\mathbf{u}}(x_n, \ldots, x_1) = f(x_{n-s}, \ldots, x_1) + \sum_{i=n-s+1}^{n} u_i x_i,$$

is s-plateaued with $supp(\mathcal{W}_{f_{\mathbf{u}}}) = \{(u_n, \ldots, b_{n-s+1}, b_{n-s}, \ldots, b_1) : b_i \in \mathbb{Z}_p, 1 \leq i \leq n-s\}$.

Chapter 3

Second order nonlinearities of some classes of cubic Boolean functions

3.1 Introduction

The second order nonlinearity of a function $f \in \mathcal{B}_n$ is the minimum Hamming distance of f to the set of all Boolean functions of degree at most 2. The concept of higher order nonlinearity has been used in cryptanalysis by several authors [32,56,74,114], which provide motivation to identify and construct Boolean functions with good nonlinearity profile. In general, it is a tough task, to compute r-th order nonlinearity $nl_r(f)$ (even for $r = 2$) of a Boolean function f. It may be noted that even second order nonlinearity is known only for a few classes of Boolean functions. Although, there are some algorithms to compute r-th order nonlinearity of Boolean functions, they give significant results for $n \leq 11$ and in some cases for $n \leq 13$ [47]. Thus, there is a need to determine theoretical bounds on second order nonlinearities of Boolean functions which are valid for all values of n.

Iwata-Kurosawa [74] have introduced r-th order bent functions and derived lower bounds on r-th order nonlinearity Boolean functions. Carlet [15] has presented a systematic study of r-th order nonlinearities of Boolean functions. He has developed a recursive approach for the computation of lower bounds on r-th order nonlinearities of Boolean functions. Further, he has obtained lower bounds on r-th order nonlinearity of several classes of Boolean functions

including the *inverse functions* $tr_1^n(x^{2^n-2})$, functions in Maiorana-McFarland bent class, and the *Welch functions* $tr_1^n(2^r)$, where (i) $n = 2r+1$ and n odd, or (ii) $n = 2r-1$ and n odd.

Carlet [15] has derived the lower bounds on r-th order nonlinearity of $f \in \mathcal{B}_n$ in terms of $(r-1)$th order nonlinearity of its derivative $D_a f$. It is well known that the WHS of an affine or a quadratic function is completely characterized [96, Chapter 15] by the dimension of the kernel of bilinear form associated with it and hence the nonlinearity. Obviously, the derivative of a cubic function is at most quadratic. Thus, in case of cubic Boolean functions Carlet's [15] recursive results are directly applicable for computation of lower bounds on r-th order nonlinearities. These results have been extensively used to investigate the lower bounds on second order nonlinearities of several classes of Boolean functions [50,53,146,147].

Sun and Wu [146] have obtained lower bounds on second order nonlinearity of three classes of highly nonlinear cubic Boolean functions of the form $tr_1^n(x^d)$, where (i) $d = 2^{r+1}+3$ and $n = 2r$, (ii) $d = 2^r + 2^{\frac{r+1}{2}} + 1$, $n = 2r$ and r is odd, and (iii) $d = 2^{2r} + 2^{r+1} + 1$ and $n = 4r$. In [53], Gode and Gangopadhyay have obtained lower bounds on second order nonlinearities of cubic monomial functions of the form $tr_1^n(\lambda x^{2^i+2^j+1})$, where $\lambda \in \mathbb{F}_{2^n}$ and $i > j$. Recently, Sun and Wu [147] have obtained lower bounds on second order nonlinearity of highly nonlinear cubic Boolean functions of the form $tr_1^n(\lambda x^d)$, where $d = 2^{2r} + 2^r + 1$, where $n = 4r$ and $\lambda \in \mathbb{F}_{2^r} \setminus \{0\}$. The lower bounds on second order nonlinearity have been further studied in [15, 50, 54, 85, 91].

In this chapter, we consider the problem of computing the lower bounds on second order nonlinearities of some classes of Boolean functions. We obtain the lower bounds on second order nonlinearities of some classes of highly nonlinear cubic Boolean functions of the form $tr_1^n(\lambda x^d)$, where

(i) $d = 2^{2r} + 2^r + 1$, where $n = 3r$ and $\lambda \in \mathbb{F}_{2^r} \setminus \{0\}$,

(ii) $d = 2^{2r} + 2^{r+1} + 1$, where $n = 3r$, $n = 5r$ and $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$.

We compare our results with some existing lower bounds. Further, we obtain lower bounds on second order nonlinearities of some classes of cubic Boolean functions based on secondary constructions.

3.2 Main results

In this section, we deduce some lower bounds on the second order nonlinearity of some classes of cubic Boolean functions by investigating the lower bounds of the first order nonlinearity of their derivatives.

Theorem 3.2.1. *Suppose* $f \in \mathcal{B}_n$ *such that* $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1}) \ \forall \ x \in \mathbb{F}_{2^n}$, *with* $n = 3r$ *and* $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$. *Then the second order nonlinearity of* f *satisfies the relation*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n+r+2}{2}} + 2^n}.$$

Proof. The derivative of $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$, where $n = 3r$ and $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$, with respect to $a \in \mathbb{F}_{2^n} \setminus \{0\}$ is

$$\begin{aligned}
D_a f(x) = f(x) + f(x+a) &= tr_1^n\left(\lambda(x+a)^{2^{2r}+2^{r+1}+1}\right) + tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1}) \\
&= tr_1^n\left(\lambda\left(x^{2^{2r}+2^{r+1}} + x^{2^{2r}}a^{2^{r+1}} + x^{2^{r+1}}a^{2^{2r}} + a^{2^{2r}+2^{r+1}}\right)(x+a)\right. \\
&\qquad \left. + \lambda x^{2^{2r}+2^{r+1}+1}\right) \\
&= tr_1^n\left(\lambda\left(x^{2^{2r}+2^{r+1}}a + x^{2^{2r}+1}a^{2^{r+1}} + x^{2^{r+1}+1}a^{2^{2r}}\right)\right) + l(x),
\end{aligned}$$

where $l(x)$ is an affine function. Let $a \neq b \in \mathbb{F}_{2^n} \setminus \{0\}$, then

$$\begin{aligned}
D_b D_a f(x) &= tr_1^n\left(\lambda\left((x+b)^{2^{2r}+2^{r+1}}a + (x+b)^{2^{2r}+1}a^{2^{r+1}} + (x+b)^{2^{r+1}+1}a^{2^{2r}}\right)\right) \\
&\quad + tr_1^n\left(\lambda(x^{2^{2r}+2^{r+1}}a + x^{2^{2r}+1}a^{2^{r+1}} + x^{2^{r+1}+1}a^{2^{2r}})\right) + constant \\
&= tr_1^n\left(x^{2^{2r}}(\lambda b a^{2^{r+1}} + \lambda a b^{2^{r+1}}) + x^{2^{r+1}}(\lambda b a^{2^{2r}} + \lambda a b^{2^{2r}})\right. \\
&\qquad \left. + x(\lambda a^{2^{r+1}} b^{2^{2r}} + \lambda a^{2^{2r}} b^{2^{r+1}})\right) + constant \\
&= tr_1^n\left(x\left((\lambda b a^{2^{r+1}} + \lambda a b^{2^{r+1}})^{2^r} + (\lambda b a^{2^{2r}} + \lambda a b^{2^{2r}})^{2^{2r-1}}\right.\right. \\
&\qquad \left.\left. + (\lambda a^{2^{r+1}} b^{2^{2r}} + \lambda a^{2^{2r}} b^{2^{r+1}})\right)\right) + constant \\
&= tr_1^n\left(x\left(\lambda^{2^r} b^{2^r} a^{2^{2r+1}} + \lambda^{2^r} a^{2^r} b^{2^{2r+1}} + \lambda^{2^{2r-1}} b^{2^{2r-1}} a^{2^{r-1}}\right.\right. \\
&\quad \left.\left. + \lambda^{2^{2r-1}} a^{2^{2r-1}} b^{2^{r-1}} + \lambda a^{2^{r+1}} b^{2^{2r}} + \lambda a^{2^{2r}} b^{2^{r+1}}\right)\right) + constant \\
&= tr_1^n\left(x P_{\lambda,a}(b)\right) + constant.
\end{aligned}$$

It is clear that $D_bD_af(x)$ is constant if and only if $P_{\lambda,a}(b) = 0$. The kernel $\mathcal{E}_{D_af}$ of D_af is defined as

$$\mathcal{E}_{D_af} = \{b \in \mathbb{F}_{2^n} : \ P_{\lambda,a}(b) = 0\},$$

i.e., $\mathcal{E}_{D_af}$ is the set of zeroes of the polynomial $P_{\lambda,a}(b)$, or equivalently the set of zeroes of the polynomial $(P_{\lambda,a}(b))^{2^{2r+1}}$. Now, we copute

$$\begin{aligned} L_{\lambda,a}(b) = (P_{\lambda,a}(b))^{2^{2r+1}} &= \Big(\lambda^{2^r} b^{2^r} a^{2^{2r+1}} + \lambda^{2^r} a^{2^r} b^{2^{2r+1}} + \lambda^{2^{2r-1}} b^{2^{2r-1}} a^{2^{r-1}} \\ &\qquad + \lambda^{2^{2r-1}} a^{2^{2r-1}} b^{2^{r-1}} + \lambda a^{2^{r+1}} b^{2^{2r}} + \lambda a^{2^{2r}} b^{2^{r+1}}\Big)^{2^{2r+1}} \\ &= \lambda^2 a^2 b^{2^{r+2}} + \lambda^{2^{2r+1}} a^4 b^{2^{r+1}} + \lambda^{2^r} a b^{2^r} + \lambda^{2^{2r+1}} a^{2^{r+1}} b^4 + \lambda^2 b^2 a^{2^{r+2}} + \lambda^{2^r} a^{2^r} b. \end{aligned}$$

Since $L_{\lambda,a}(b)$ is a linearized polynomial in b of degree at most 2^{r+2}, it follows that the dimension k of $\mathcal{E}_{D_af}$ is at most $r+2$. Therefore, for every $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$, the WHT is given by

$$W_{D_af}(\alpha) = 2^{\frac{n+k}{2}} \leq 2^{\frac{n+r+2}{2}}.$$

The nonlinearity of the derivative D_af of $f \in \mathcal{B}_n$ is

$$nl(D_af) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_{2^n}} |W_{D_af}(\lambda)|.$$

From which, we get

$$nl(D_af) \geq 2^{n-1} - 2^{\frac{n+r}{2}}. \tag{3.2.1}$$

Using Proposition 2.8.3, we obtain

$$\begin{aligned} nl_2(f) &\geq \frac{1}{2}\left(2^{n-1} - 2^{\frac{n+r}{2}}\right) \\ &= 2^{n-2} - 2^{\frac{n+r-2}{2}}. \end{aligned} \tag{3.2.2}$$

On comparing 3.2.1 and Corollary 2.8.7, we get $M = 1, m = \frac{n+r}{2}$. Now, by using the result

in Corollary 2.8.7, we get

$$\begin{aligned} nl_2(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)M2^{m+1}+2^n} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n+r+2}{2}}+2^n}. \end{aligned} \tag{3.2.3}$$

On subtracting the lower bound in (3.2.2) from the lower bound in (3.2.3), and using $n = 3r$, we get

$$\begin{aligned} &2^{n-1} - \tfrac{1}{2}\sqrt{(2^n-1)2^{\frac{n+r+2}{2}}+2^n} - \tfrac{1}{2}\left(2^{n-1} - 2^{\frac{n+r}{2}}\right) \\ &= 2^{n-2} + 2^{\frac{4n-6}{6}} - \tfrac{1}{2}\sqrt{(2^n-1)2^{\frac{4n+6}{6}}+2^n} \ > 0. \end{aligned}$$

for every value of n. Therefore, from the context it is clear that the bounds obtained in (3.2.3) are better than the lower bounds in (3.2.2). Therefore, we have

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n+r+2}{2}}+2^n}.$$

■

In the following result, we obtain the lower bounds on second order nonlinearities of the function $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$ for every $x \in \mathbb{F}_{2^n}$, with $n = 5r$, $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$.

Theorem 3.2.2. *Suppose $f \in \mathcal{B}_n$ such that $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$ for every $x \in \mathbb{F}_{2^n}$ with $n = 5r$ and $\lambda \in \mathbb{F}_{2^n} \setminus \{0\}$. Then*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n+3r+2}{2}}+2^n}.$$

Proof. The proof is almost similar to the proof of Theorem 3.2.1. ■

Remark 3.2.3. *The general lower bounds on second order nonlinearities of Boolean functions due to Carlet [15] and Iwata-Kurosawa [74] are $2^{n-1} - 2^{n-\frac{3}{2}}$ and $2^{n-2} - 2^{n-4}$, respectively. Clearly,*

$$(2^{n-2} - 2^{n-4}) - (2^{n-1} - 2^{n-\frac{3}{2}}) = 2^{n-4}(4\sqrt{2} - 5) \geq 0.$$

Hence, the bounds obtained by Iwata-Kurosawa [74] are better than Carlet's general bounds [15]. Now, on subtracting Iwata-Kurosawa's bounds from the bounds obtained in Theorem 3.2.2 and using $n = 5r$, we get

$$\begin{aligned}&\left(2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{n+3r+2}{2}} + 2^n}\right) - \left(2^{n-2} - 2^{n-4}\right)\\ &= 5\ 2^{n-4} - \frac{1}{2}\sqrt{(2^n-1)2^{\frac{8n+10}{10}} + 2^n}\ > 0\end{aligned}$$

if and only if $n \geq 12$. Therefore, in Theorem 3.2.2 we investigate a class of highly nonlinear cubic Boolean functions whose lower bounds of second order nonlinearities (for all $n \geq 12$) are better than the lower bounds obtained by Iwata-Kurosawa [74].

Theorem 3.2.4. *Suppose $f \in \mathcal{B}_n$ such that $f(x) = tr_1^n(\lambda x^{2^{2r}+2^r+1})\ \forall x \in \mathbb{F}_{2^n}$, with $n = 3r$ and $\lambda \in \mathbb{F}_{2^r} \setminus \{0\}$. Then*

$$nl_2(f) \geq 2^{n-1} - 2^{\frac{3n+r-4}{4}}.$$

Proof. We have $f(x) = tr_1^n(\lambda x^{2^{2r}+2^r+1})$ for all $x \in \mathbb{F}_{2^n}$ with $n = 3r$ and $\lambda \in \mathbb{F}_{2^r} \setminus \{0\}$. The first order derivative f w. r. t. $a \neq 0, a \in \mathbb{F}_{2^n}$, is

$$\begin{aligned}D_a f(x) &= tr_1^n(\lambda(x+a)^{2^{2r}+2^r+1}) + tr_1^n(\lambda x^{2^{2r}+2^r+1})\\ &= tr_1^n(\lambda(ax^{2^{2r}+2^r} + a^{2^r}x^{2^{2r}+1} + a^{2^{2r}}x^{2^r+1})) + l(x),\end{aligned} \tag{3.2.4}$$

where $l(x)$ is an affine function. Let $b \in \mathbb{F}_{2^n}$ such that $a \neq b$, $b \neq 0$, then

$$\begin{aligned}D_b D_a f(x) &= tr_1^n\Big(a\lambda((x+b)^{2^{2r}+2^r} + x^{2^{2r}+2^r}) + a^{2^r}\lambda((x+b)^{2^{2r}+1} + x^{2^{2r}+1})\\ &\qquad + a^{2^{2r}}\lambda((x+b)^{2^r+1} + x^{2^r+1})\Big)\\ &= tr_1^n\Big(a\lambda(b^{2^r}x^{2^{2r}} + b^{2^{2r}}x^{2^r} + b^{2^r}x^{2^{2r}} + b^{2^{2r}+2^r}) + a^{2^r}\lambda(bx^{2^{2r}} + b^{2^{2r}}x + b^{2^{r+1}})\\ &\qquad + a^{2^{2r}}\lambda(bx^{2^r} + b^{2^r}x + b^{2^{r+1}})\Big)\\ &= tr_1^n(x^{2^{2r}}\lambda(ab^{2^r} + a^{2^r}b) + x^{2^r}\lambda(ab^{2^{2r}} + a^{2^{2r}}b) + x\lambda(a^{2^r}b^{2^{2r}} + a^{2^{2r}}b^{2^r})) + constant.\end{aligned}$$

Therefore, $D_b D_a f(x)$ is constant if and only if the coefficient of x in $D_b D_a f(x)$ is zero, i.e.,

$$\lambda^{2^{n-2r}}(ab^{2^r} + a^{2^r}b)^{2^{n-2r}} + \lambda^{2^{n-r}}(ab^{2^{2r}} + a^{2^{2r}}b)^{2^{n-r}} + \lambda(a^{2^r}b^{2^{2r}} + a^{2^{2r}}b^{2^r}) = 0.$$

Since $\lambda \in \mathbb{F}_{2^r} \setminus \{0\}$ and $n = 3r$, therefore, we have

$$\begin{aligned} \lambda((ab^{2^r} + a^{2^r}b)^{2^{n-2r}} + (ab^{2^{2r}} + a^{2^{2r}}b)^{2^{n-r}} + (a^{2^r}b^{2^{2r}} + a^{2^{2r}}b^{2^r})) &= 0 \\ \text{i.e., } ((ab^{2^r} + a^{2^r}b)^{2^{n-2r}} + (ab^{2^{2r}} + a^{2^{2r}}b)^{2^{n-r}} + (a^{2^r}b^{2^{2r}} + a^{2^{2r}}b^{2^r}))^{2^{2r}} &= 0 \\ \text{i.e., } ab^{2^r} + a^{2^r}b + a^{2^r}b^{2^{3r}} + a^{2^{3r}}b^{2^r} + a^{2^{3r}}b^{2^{4r}} + a^{2^{4r}}b^{2^{3r}} &= 0. \end{aligned}$$

Now using $n = 3r$ and the property that $x^{2^n} = x$ for all $x \in \mathbb{F}_{2^n}$, we get $ab^{2^r} + a^{2^r}b = 0$, which implies $(b/a)^{2^r-1} = 1$, and hence $b \in a\mathbb{F}_{2^r}$. Thus, for any non zero $a \in \mathbb{F}_{2^n}$, the number of ways in which b can be chosen for which $D_bD_af(x)$ is constant is 2^r (including the case $b = 0$). Hence by Lemma 2.5.2, we have dimension k of the kernel associated with D_af is r i.e., $k = r$. Therefore, the WHT of D_af at any point $\alpha \in \mathbb{F}_{2^n}$ is

$$W_{D_af}(\alpha) = 2^{\frac{n+k}{2}} = 2^{\frac{n+r}{2}}.$$

Therefore, nonlinearity of D_af is

$$nl(D_af) = 2^{n-1} - 2^{\frac{n+r-2}{2}}. \tag{3.2.5}$$

By using Proposition 2.8.3, we get

$$nl_2(f) \geq 2^{n-2} - 2^{\frac{n+r-4}{2}}.$$

By using Corollary 2.8.7, there is a scope to get better bounds. On comparing (3.2.5) and Corollary 2.8.7, we obtain $M = 1$ and $m = \frac{n+r-2}{2}$. Therefore, by Corollary 2.8.7, we get

$$\begin{aligned} nl_2(f) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{\frac{n+r-2}{2}+1} + 2^n} \\ &\approx 2^{n-1} - 2^{\frac{n+\frac{n+r-2}{2}-1}{2}} \\ &\approx 2^{n-1} - 2^{\frac{3n+r-4}{4}}. \end{aligned}$$

■

3.3 Lower bounds for the functions based on secondary constructions

In this section, we have deduced the lower bounds on second order nonlinearities of some classes of Boolean functions based on secondary constructions.

Lemma 3.3.1. *Let $g_\lambda(x,y) = (1+y)tr_1^t(\lambda(x^r+x)) + ytr_1^t(\lambda x^r),\ \lambda \in \mathbb{F}_{2^t} \setminus \{0\}$ be a Boolean function defined on $\mathbb{F}_{2^n}, n = t+1$. Then the dimension of the kernel of the bilinear form associated with $D_(a,b)g_\lambda$ is $(k+1)$, where k is the dimension of the kernel of the bilinear form associated with $D_a f_\lambda(x)$ with $f_\lambda(x) = tr_1^t(\lambda x^r)$ with $x \in \mathbb{F}_{2^t}, y \in \mathbb{F}_2$, and f_λ be a cubic Boolean function.*

Proof. The function g_λ can be written as $g_\lambda(x,y) = tr_1^t(\lambda(x+xy)) + tr_1^t(\lambda x^r)$. Consider a 2-dimensional subspace V generated by two vectors (a,b) and (c,d). The second order derivative of g at V is given by

$$\begin{aligned} D_V g_\lambda(x,y) &= D_{(c,d)}D_{(a,b)}g_\lambda(x,y) \\ &= D_V f_\lambda + constant. \end{aligned} \tag{3.3.1}$$

Clearly, the derivative $D_{(a,b)}g_\lambda(x,y)$ is a quadratic function. Hence by Lemma 2.5.2, the kernel of $D_{(a,b)}g_\lambda$ can be expressed as

$$\begin{aligned} \varepsilon_{D_{(a,b)}g_\lambda} &= \{(c,d) \in \mathbb{F}_{2^t} \times \mathbb{F}_2 :\ D_{(c,d)}D_{(a,b)}g_\lambda = constant\} \\ &= \{(c,d) \in \mathbb{F}_{2^t} \times \mathbb{F}_2 :\ D_{(c,d)}D_{(a,b)}f_\lambda = constant\}. \end{aligned} \tag{3.3.2}$$

Also, it is given that the kernel $\varepsilon_{D_c f_\lambda}$ is of dimension k. From (3.3.2) it follows that c has 2^k distinct values, and corresponding to each value of c, d can be chosen in 2 ways. Therefore, the total number of ways in which (c,d) can be chosen so that $D_{(c,d)}D_{(a,b)}g_\lambda$ is constant is $2^k \cdot 2 = 2^{k+1}$. Hence, $\varepsilon_{D_{(a,b)}g_\lambda}$ contains exactly 2^{k+1} elements. ∎

Theorem 3.3.2. *Let $n = t+1$ be an even integer, and l be an integer such that $l = \frac{t+1}{2}$ or $l = \frac{t-1}{2}$. Define a function $g(x,y) = (1+y)tr_1^t(x^{2^l+3} + x) + ytr_1^t(x^{2^l+3})$ on $\mathbb{F}_{2^n}$. Then the*

second order nonlinearity of g satisfies the relation

$$nl_2(g) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+4}{2}} - 2^{\frac{n+6}{2}}}.$$

Proof. We have $g(x,y) = (1+y)tr_1^t(x^{2^l+3} + x) + ytr_1^t(x^{2^l+3})$. On comparing this equation with Lemma 3.3.1 for $\lambda = 1$, we get $f(x) = tr_1^t(x^{2^l+3})$. It is given in [15] that the dimension k of the kernel $\varepsilon_{D_a f}$ is ≤ 3, i.e., $k \leq 3$ for all $a \in \mathbb{F}_{2^t} \setminus \{0\}$. Hence, by Lemma 3.3.1, the dimension $k(a,b)$ of the kernel $\varepsilon_{D_{(a,b)}g}$ is ≤ 4, i.e., $k(a,b) \leq 4$ for all $(a,b) \in \mathbb{F}_{2^t} \times \mathbb{F}_2 (a \neq 0)$. Therefore, the WHT of $D_{(a,b)}g$ for all $(\lambda,\mu) \in \mathbb{F}_{2^t} \times \mathbb{F}_2$ satisfies

$$W_{D_{(a,b)}g}(\lambda,\mu) \leq 2^{\frac{n+k(a,b)}{2}}.$$

Hence,

$$\begin{aligned} nl(D_{(a,b)}g) &= 2^{n-1} - \frac{1}{2}\max_{(\lambda,\mu)\in\mathbb{F}_{2^t}\times\mathbb{F}_2} |W_{D_{(a,b)}g}(\lambda,\mu)| \\ &\geq 2^{n-1} - \frac{1}{2}2^{\frac{n+k(a,b)}{2}} \\ &\geq 2^{n-1} - 2^{\frac{n+2}{2}}. \end{aligned}$$

By using Proposition 2.8.4, we get

$$\begin{aligned} nl_2(g) &= 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2(2^n - 2)(2^{n-1} - 2^{\frac{n+2}{2}})} \\ &\approx 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+4}{2}} - 2^{\frac{n+6}{2}}}. \end{aligned}$$

■

Theorem 3.3.3. *Let $g_\lambda \in \mathcal{B}_n$ be such that $g_\lambda(x,y) = ytr_1^6(\lambda x^{2^3-1}) + (1+y)tr_1^6(\lambda(x^{2^3-1}+x)$. Then the second order nonlinearity of g_λ defined on 7-variables satisfies*

$$nl_2(g_\lambda) = 24.$$

Proof. Since g_λ is a cubic Boolean function and it has been proved in [150] that the dimension of the kernel $\varepsilon_{D_{(a=1)}f_\lambda}$ is 2, where $f_\lambda(x,y) = tr_1^6(\lambda x^{2^3-1})$. Using Lemma 3.3.1, we obtain

the dimension $k(a,b)$ of the kernel $\varepsilon_{D_{(a=1)}g_\lambda}$ as 3, i.e., $k(1,b)=3$. Therefore, the WHT of $D_{(1,b)}g_\lambda$ for all $(\lambda,\mu)\in\mathbb{F}_{2^t}\times\mathbb{F}_2$ is given by

$$\begin{aligned} W_{D_{(1,b)}g_\lambda}(\lambda,\mu) &= 2^{\frac{n+k(1,b)}{2}} \\ &= 2^{\frac{7+3}{2}} = 2^5. \end{aligned}$$

Hence, the nonlinearity of $D_{(1,b)}g_\lambda$ will be

$$\begin{aligned} nl(D_{(1,b)}g_\lambda) &= 2^{n-1} - \frac{1}{2}\max_{(\lambda,\mu)\in\mathbb{F}_{2^t}\times\mathbb{F}_2}|W_{D_{(1,b)}f}(\lambda,\mu)| \\ &= 2^6 - 2^{5-1} = 48. \end{aligned}$$

Therefore, by using Proposition 2.8.3, we obtain $nl_2(g_\lambda)\geq 24$. ■

Theorem 3.3.4. *Let $g\in\mathcal{B}_n$ such that $g(x,y)=ytr_1^6(x^{2^3-1})+(1+y)tr_1^6((x^{2^3-1}+x)$. Then the second order nonlinearity of g defined on 7-variables is*

$$nl_2(g)\geq 28.$$

Proof. Since $g(x,y)$ is a cubic Boolean function and it is known from [150] that the dimension of the kernel ε_{D_af} is 2 at 49 points and 4 at 14 points in $\mathbb{F}_{2^6}$, where $f(x,y)=tr_1^6(x^{2^3-1})$. Hence by Lemma 3.3.1, the dimension $k(a,b)$ of the kernel $\varepsilon_{D_{(a,b)}g}$ is 3 at 98 points and 5 at 28 points in $\mathbb{F}_{2^7}$. Therefore, the nonlinearity of $D_{(a,b)}g$ will be

$$nl(D_{(a,b)}g)=\begin{cases} 2^6-2^{\frac{7+3}{2}-1}=48, & \text{if } k=3,\\ 2^6-2^{\frac{7+5}{2}-1}=32, & \text{if } k=5. \end{cases}$$

By using Proposition 2.8.4, we get

$$\begin{aligned} nl_2(g) &\geq 2^6 - \frac{1}{2}\sqrt{2^{14}-2\sum_{(a,b)\in\mathbb{F}_{2^6}\times\mathbb{F}_2} nl(D_{(a,b)}g_\lambda)} \\ &= 2^6 - \frac{1}{2}\sqrt{16384-2(98\cdot 48+28\cdot 32)} = 28. \end{aligned} \tag{3.3.3}$$

■

Theorem 3.3.5. *Let $g_\lambda \in \mathcal{B}_n$ be such that $g_\lambda(x,y) = (1+y)(f_\lambda(x)+x) + yf_\lambda(x)$, where $f_\lambda(x) = tr_1^n(\lambda x^{2^{2l}+2^l+1}), \lambda \in \mathbb{F}_{2^t}$ and l is a positive integer such that $gcd(t,l) = l$. Then for $t > 4$ the second order nonlinearity of g_λ is*

$$nl_2(g_\lambda) \geq \begin{cases} 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+5}{2}} - 2^{\frac{n+7}{2}}}, & \text{if } n \equiv 1 \mod 2, \\ 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+4}{2}} - 2^{\frac{n+6}{2}}}, & \text{if } n \equiv 0 \mod 2. \end{cases}$$

Proof. The function $f_\lambda(x) = tr_1^n(\lambda x^{2^{2l}+2^l+1})$ is a cubic Boolean function. Let $k(a)$ be the dimension of the kernel ε_{D_af} associated with $D_af_\lambda(x)$. It is proved in [53] that for all non-zero $a \in \mathbb{F}_{2^t}$, $k(a) \leq 4$ if t is even, else $k(a) \leq 3$. Hence, by Lemma 3.3.1, it follows that for all $a \in \mathbb{F}_{2^t} \setminus \{0\}$, the dimension $k(a,b)$ of the kernel $\varepsilon_{D_{(a,b)}g_\lambda}$ is ≤ 5, if t is even, else $k(a,b) \leq 4$. Therefore, for $(\mu,\eta) \in \mathbb{F}_{2^t} \times \mathbb{F}_2$, the WHT of $D_{(a,b)}g_\lambda$ will be

$$W_{D_{(a,b)}g_\lambda}(\mu,\eta) = 2^{\frac{n+k(a,b)}{2}} \leq \begin{cases} 2^{\frac{n+4}{2}}, & \text{if } n \equiv 0 \mod 2, \\ 2^{\frac{n+4}{2}}, & \text{if } n \equiv 1 \mod 2. \end{cases} \tag{3.3.4}$$

Therefore, the nonlinearity of $D_{(a,b)}g_\lambda$ for all $(a,b) \in \mathbb{F}_{2^t} \times \mathbb{F}_2$ (except for $a = 0$ and $a = b$) is

$$nl(D_{(a,b)}g_\lambda) \geq \begin{cases} 2^{n-1} - \frac{1}{2}2^{\frac{n+4}{2}}, & \text{if } n \equiv 0 \mod 2, \\ 2^{n-1} - \frac{1}{2}2^{\frac{n+5}{2}}, & \text{if } n \equiv 1 \mod 2. \end{cases}$$

Now, we consider following two cases:

Case 1: For n even, from proposition 2.8.4, we get

$$\begin{aligned} nl_2(g_\lambda) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2(2^n-2)(2^{n-1} - 2^{\frac{n+2}{2}})} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+4}{2}} - 2^{\frac{n+6}{2}}}. \end{aligned}$$

Case 2: For n odd, from proposition 2.8.4, we get

$$\begin{aligned} nl_2(g_\lambda) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2(2^n-2)(2^{n-1} - 2^{\frac{n+3}{2}})} \\ &= 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1} + 2^{\frac{3n+5}{2}} - 2^{\frac{n+7}{2}}}. \end{aligned}$$

■

3.4 Comparison

In this section, we present numerical comparison of the lower bounds obtained in this chapter with some existing lower bounds. Table 3.1 presents the numerical comparison between the lower bounds obtained in Theorem 3.2.1 with the lower bounds obtained by Iwata-Kurosawa [74], Gangopadhyay et al. [50], Sun-Wu [147] and the general bounds obtained by Carlet in [15]. It is clear from Table 3.1 that for $n \geq 9$, the lower bounds obtained in Theorem 3.2.1, for cubic Boolean functions, are better than the bounds obtained in [15, 50, 74, 147]. Further, it is observed from remark 3.2.3 and Table 3.2 that the bounds obtained in Theorem 3.2.2 are larger than the bounds obtained by Iwata-Kurosawa in [74] and Carlet's general bounds in [15].

Table 3.1: Numerical comparison of the lower bounds on second-order nonlinearities obtained in Theorem 3.2.1 using McEliece's theorem with the bounds obtained in [15, 50, 53, 74, 147]

n	6	9	12	15	18	21	24
Bounds in Theorem 3.2.1	10	128	1328	12288	107904	917504	7.647232×10^6
Due to Iwata-Kurosawa [74]	12	96	764	6144	49152	393216	3.145728×10^6
Due to [50, Theorem 1]	10	–	1024	–	84732	–	6.291456×10^6
Due to Sun-Wu [147]	–	–	1318	–	–	–	7.339910×10^6
Carlet's general bounds [15]	10	76	600	4800	38392	307122	2.456968×10^6
Due to [53]	10	128	1024	12288	84731	736832	6.625120×10^6

Table 3.2: Numerical comparison of the lower bounds on second-order nonlinearities obtained by Theorem 3.2.2 using McEliece's theorem with the bounds obtained in [15, 74]

n	15	20	25	30	35
Bounds in Theorem 3.2.2	8192	338944	12582912	441965056	$1.5032385536 \times 10^{10}$
Due to Iwata-Kurosawa [74]	6144	196608	6291456	201326592	6.442450944×10^9
Carlet's general bounds [15]	4800	153562	4913934	157245850	5.031867186×10^9

In Table 3.3, we provide numerical comparison between the lower bounds obtained in Theorem 3.2.4 with the lower bounds obtained by Iwata-Kurosawa [74], Gode and Gangopadhyay [53], and Carlet's general bounds [15]. We observe that the bounds obtained in Theorem 3.2.4, for cubic Boolean functions, are better than the bounds obtained in [15, 53, 74]. Also, it is observed that for $n \in \{3, 6, 9\}$ the lower bounds obtained in Theorem 3.2.4 are very close to the covering radius of $RM(2, n)$ [47].

Further, in Table 3.4, we present numerical comparison of lower bounds, obtained for n even, in Theorem 3.3.2 and Theorem 3.3.5 with the lower bounds obtained in [15, 47, 53]. The case for n odd is presented in Table 3.5. It may be noted that for n even, the lower bounds in Theorem 3.3.2 and Theorem 3.3.5 are better than Carlet's general bounds in [15] and are consistent with the bounds in [53].

Table 3.3: Numerical comparison of the lower bounds on second-order nonlinearities obtained by Theorem 3.2.4 with some other known bounds in [15, 47, 53]

n, r (with $n = 3r$)	$3, 1$	$6, 2$	$9, 3$	$12, 4$	$15, 5$	$18, 6$
Bounds obtained in Theorem 3.2.4	2	16	166	1536	13488	114688
Due to [53]	−−	10	128	1024	10592	85732
Carlet's general lower bounds [15]	2	10	75	600	4799	38391
Hmax* [47]	1	18	196	1760	−−	−−

Hmax* denotes the maximum known Hamming distance.

Table 3.4: Numerical comparison of the lower bounds on second-order nonlinearities obtained by Theorem 3.3.2 and 3.3.5 (for n even) with some existing bounds in [15, 22, 47, 53]

n	6	8	10	12
Bounds obtained in Theorem 3.3.2 and in Theorem 3.3.5	10	64	331	1536
Bounds obtained in [53]	10	64	331	1536
Carlet's general lower bounds [15]	10	38	150	600
Maximum known Hamming distance Hmax* [47]	18	84	400	1760

Table 3.5: Numerical comparison of the lower bounds on second-order nonlinearities obtained by Theorem 3.3.2 and 3.3.5 (for n odd) with some existing bounds in [15, 47, 53]

n	7	9	11	13
Bounds obtained in Theorem 3.3.2 and in Theorem 3.3.5	19	128	661	3071
Carlet's general lower bounds [15]	19	75	300	1200
Maximum known Hamming distance Hmax* [47]	40	196	848	−−

Remark 3.4.1. *It is important to note that, high first order nonlinearity of a Boolean function does not implies the high second order nonlinearity. For example: bent function* $tr_1^n(x^{2^i+1})$ *possess maximum possible first order nonlinearity but their second order nonlinearity is zero. The results in this chapter show that the lower bounds of second order nonlinearity of these classes of Boolean functions are also high. Therefore, we expect that these results may be useful in choosing cryptographically significant Boolean functions.*

Chapter 4

Construction of highly nonlinear resilient functions with disjoint spectra

4.1 Introduction

The resiliency and the nonlinearity are two important cryptographic criteria for the design of Boolean functions used in various cryptosystems. High resiliency provide protection against correlation attacks [32, 116, 141], whereas high nonlinearity helps to prevent the ciphers from linear cryptanalysis [103] and best affine approximation attacks [56, 103]. A resilient function is a correlation immune and balanced function. A balanced function with high nonlinearity is considered to be a good candidate for various cryptographic applications. Such functions are used as combiner functions in LSFR based stream ciphers. Therefore, it is important to construct resilient functions with high nonlinearity. Several constructions of resilient functions satisfying some other important cryptographic criteria have been reported in the literature. Sarkar-Maitra [126], Maitra-Pasalic [98] and Zhang-Xiao [161] have reported some constructions of resilient function with high nonlinearity. For more study on constructions of resilient functions and their properties we refer to [18, 98, 101, 120, 126, 154, 161]. Recently, Gao et al. [52] have provided a technique to

construct resilient Boolean functions with high nonlinearity.

In this chapter, we use the approach proposed by Gao et al. [52] for the construction of highly nonlinear resilient functions. We provide some new constructions of highly nonlinear resilient Boolean functions on large number of variables having disjoint spectra by concatenating Boolean functions on small number of variables with disjoint spectra. After analyzing the profiles of the constructed functions, we observe that the nonlinearity of some of the concatenated functions (as constructed in Theorem 4.3.1) has improved upon the nonlinearity bounds obtained by Gao et al. [52].

4.2 Preliminaries

In this section, we provide some important definitions and results that will be used to obtain the results in this chapter.

Recall that a function $f \in \mathcal{B}_n$ is called *plateaued* if for every $\mathbf{u} \in \mathbb{F}_2^n$, $W_f(\mathbf{u}) \in \{0, \pm 2^k\}$, $k \in \mathbb{N}$. Two functions $f, g \in \mathcal{B}_n$ are said to be *disjoint spectra functions* if $W_f(\omega)W_g(\mathbf{w}) = 0$ for all $\mathbf{w} \in \mathbb{F}_2^n$. A function $f \in \mathcal{B}_n$ is called *balanced* if $W_f(\mathbf{0}) = 0$. A function $f \in \mathcal{B}_n$ is said to be *correlation immune* of order m if $W_f(\alpha) = 0$ for every $\alpha \in \mathbb{F}_2^n$ with $1 \leq w_H(\alpha) \leq m$. A balanced and correlation immune function of order m is called *m-resilient*.

The following result is due to Iwata and Kurosawa [74] which provides a relationship between nonlinearity of a function on n variables and its subfunctions on $(n-1)$ variables.

Lemma 4.2.1. *[74] Let f_0 be the restriction of $f \in \mathcal{B}_n$ to the linear hyperplane H having equation $x_n = 0$, and f_1 be the restriction of f to the affine hyperplane H' having equation $x_n = 1$. Then both the functions f_0 and f_1 are $(n-1)$ variable Boolean functions. The r-th order nonlinearity of f satisfies the relation*

$$nl_r(f) \geq nl_r(f_0) + nl_r(f_1).$$

For the construction of desired functions, we have used concatenation of Boolean functions on less number of variables [102]. The concatenation of two n-variable Boolean func-

tions f_1 and f_2, is an $(n+1)$-variable Boolean function, denoted by $f = f_1 \parallel f_2$, and defined by

$$f(x_{n+1}, ..., x_1) = (1 + x_{n+1})f_1(x_n, ..., x_1) + x_{n+1}f_2(x_n, ..., x_1).$$

We denote the *profile* of a Boolean function by 4-tupple (a, b, c, d), where a is the number of variables, b the order of resiliency, c the algebraic degree, and d the nonlinearity of the function.

In the following result, Sarkar and Maitra [126] have obtained the profile of a concatenated function on $(n+1)$ variables in terms of the profile of its subfunction on n variables.

Lemma 4.2.2. *[126] Let $f \in \mathcal{B}_n$ be of profile $(n, m, n-m-1, nl)$. Then the profile of the concatenated function $f \parallel \overline{f}$ is $(n+1, m+1, n-m-1, 2nl)$, where $\overline{f}$ is the complement function of f.*

The following result on resiliency of the function concatenation is due to Siegenthaler [140].

Lemma 4.2.3. *[140] If f_1 and f_2, are two m-resilient Boolean functions, then the concatenated function $f = f_1 \parallel f_2$ is also m-resilient.*

Let $\mathbf{v} = (v_r, ..., v_1)$ and $f \in \mathcal{B}_n$. The restriction function of f with respect to v is defined as

$$f_{\mathbf{v}}(x_{n-r}, ..., x_1) = f(x_n = v_r, ..., x_{n-r+1} = v_1, x_{n-r}, ..., x_1).$$

Let $\mathbf{u} = (u_r, ..., u_1) \in \mathbb{F}_2^r$ and $\mathbf{w} = (w_{n-r}, ..., w_1) \in \mathbb{F}_2^{n-r}$. The vector concatenation of u and v is defined as

$$\mathbf{uw} = (\mathbf{u}, \mathbf{w}) = (u_r, ..., u_1, w_{n-r}, ..., w_1).$$

Definition 4.2.4. *The spectrum characterization matrix $NZ(f)$ of $f \in \mathcal{B}_n$ is a matrix whose rows are the vectors of $\mathbb{F}_2^n$ at which the WHS values of f are non-zero, i.e.,*

$$NZ(f) = \{\mathbf{w} \in \mathbb{F}_2^n : W_f(\mathbf{w}) \neq 0\}.$$

Further, if $\mathbf{u}$ is a string of some fixed length, then we denote the matrix $\{\mathbf{uw} : \mathbf{w} \in NZ(f)\}$ by $\mathbf{u} \parallel NZ(f)$.

Gao et al. [52] have provided a relationship between the WHT of a Boolean function f and the WHT its subfunctions. Using this result, they have provided a method to construct disjoint spectra functions on higher dimensions from the given disjoint spectra functions on lower dimensions. Using this method they have constructed highly nonlinear resilient Boolean functions. The following result is due to Gao et al. [52].

Proposition 4.2.5. *[52, Theorem 1] Let $f \in \mathcal{B}_n$, $\mathbf{u} = (u_r, \ldots, u_1) \in \mathbb{Z}_2^r$ and $\mathbf{w} = (w_{n-r}, \ldots, w_1) \in \mathbb{F}_2^{n-r}$. Then the WHT of f in terms of its subfunction is given by*

$$W_f(\mathbf{uw}) = \sum_{\mathbf{y} \in \mathbb{F}_2^r} W_{f_\mathbf{y}}(\mathbf{w})(-1)^{\langle \mathbf{u}, \mathbf{y} \rangle}.$$

4.3 Constructions of highly nonlinear resilient functions with disjoint spectra

In the following result, we present construction of disjoint spectra functions on $n+4$ variables by using disjoint spectra functions on n variables.

Theorem 4.3.1. *Let $f_0, g_0 \in \mathcal{B}_n$ be optimal plateaued resilient Boolean functions having disjoint spectra. Define the functions $f = (x_{n+1} + 1)f_0 + x_{n+1}g_0$, $g = x_{n+1} + f_0$ and $h = x_{n+1} + g_0$. Then $F = f \parallel \overline{f} \parallel f \parallel \overline{f} \parallel \overline{f} \parallel \overline{f} \parallel f \parallel f$ and $G = g \parallel h \parallel h \parallel g \parallel \overline{g} \parallel \overline{h} \parallel \overline{h} \parallel \overline{g}$ are also disjoint spectra functions on $\mathbb{F}_2^{n+4}$.*

Proof. Since f_0 and g_0 are disjoint spectra functions, therefore, from definition it follows that $W_{f_0}(\mathbf{w})W_{g_0}(\mathbf{w}) = 0$ for every $\mathbf{w} \in \mathbb{F}_2^n$. It is easy to verify that $W_f(\mathbf{w}) = -W_{\overline{f}}(\mathbf{w})$. Now, if $\mathbf{w} \in NZ(f_0)$ or $NZ(g_0)$, then by using Proposition 4.2.5, we get

$$W_f(0\mathbf{w}) = W_{f_0}(\mathbf{w}) + W_{g_0}(\mathbf{w}) \neq 0, \text{ and}$$
$$W_f(1\mathbf{w}) = W_{f_0}(\mathbf{w}) - W_{g_0}(\mathbf{w}) \neq 0.$$

Therefore, the spectrum characterization matrix of the function f will be

$$NZ(f) = \begin{pmatrix} 0 & \| \ NZ(f_0) \\ 1 & \| \ NZ(f_0) \\ 0 & \| \ NZ(g_0) \\ 1 & \| \ NZ(g_0) \end{pmatrix}.$$

Now, for the function $F = f \parallel \overline{f} \parallel f \parallel \overline{f} \parallel \overline{f} \parallel \overline{f} \parallel f \parallel f$, using Proposition 4.2.5, we get

$W_F(000\mathbf{w}) = 0$, $W_F(001\mathbf{w}) = 4W_f(\mathbf{w})$, $W_F(010\mathbf{w}) = -4W_f(\mathbf{w})$, $W_F(011\mathbf{w}) = 0$, $W_F(100\mathbf{w}) = 0$, $W_F(101\mathbf{w}) = 4W_f(\mathbf{w})$, $W_F(110\mathbf{w}) = 4W_f(\mathbf{w})$, $W_F(111\mathbf{w}) = 0$.

The spectrum characterization matrix of F can therefore be given by

$$NZ(F) = \begin{pmatrix} 001 & \| \ NZ(f) \\ 010 & \| \ NZ(f) \\ 101 & \| \ NZ(f) \\ 110 & \| \ NZ(f) \end{pmatrix} = \begin{pmatrix} 0010 & \| \ NZ(f_0) \\ 0011 & \| \ NZ(f_0) \\ 0100 & \| \ NZ(f_0) \\ 0101 & \| \ NZ(f_0) \\ 1010 & \| \ NZ(f_0) \\ 1011 & \| \ NZ(f_0) \\ 1100 & \| \ NZ(f_0) \\ 1101 & \| \ NZ(f_0) \\ 0010 & \| \ NZ(g_0) \\ 0011 & \| \ NZ(g_0) \\ 0100 & \| \ NZ(g_0) \\ 0101 & \| \ NZ(g_0) \\ 1010 & \| \ NZ(g_0) \\ 1011 & \| \ NZ(g_0) \\ 1100 & \| \ NZ(g_0) \\ 1101 & \| \ NZ(g_0) \end{pmatrix}.$$

Now, for the function $G = g \parallel h \parallel h \parallel g \parallel \overline{g} \parallel \overline{h} \parallel \overline{h} \parallel \overline{g}$, using Proposition 4.2.5, we get $W_G(000\mathbf{w}) = 0$, $W_G(001\mathbf{w}) = 0$, $W_G(010\mathbf{w}) = 0$, $W_G(011\mathbf{w}) = 0$, $W_G(100\mathbf{w}) = 4W_g(\mathbf{w}) + 4W_h(\mathbf{w})$, $W_G(101\mathbf{w}) = 0$, $W_G(110\mathbf{w}) = 0$, $W_G(111\mathbf{w}) = 4W_g(\mathbf{w}) - 4W_h(\mathbf{w})$.

Therefore, the spectrum characterization matrix of g, h and G are given by

$$NZ(g) = 1 \parallel NZ(f_0) \;\; \textit{and} \;\; NZ(h) = 1 \parallel NZ(g_0),$$

$$NZ(G) = \begin{pmatrix} 100 & \parallel NZ(g) \\ 111 & \parallel NZ(g) \\ 100 & \parallel NZ(h) \\ 111 & \parallel NZ(h) \end{pmatrix} = \begin{pmatrix} 1001 & \parallel NZ(f_0) \\ 1111 & \parallel NZ(f_0) \\ 1001 & \parallel NZ(g_0) \\ 1111 & \parallel NZ(g_0) \end{pmatrix}.$$

From the spectrum characterization matrix of concatenated functions F and G, it is observed that F and G are disjoint spectra Boolean functions on $\mathbb{F}_2^{n+4}$. ■

In the following result, we obtain the profiles for the functions F and G as constructed in Theorem 4.3.1. We investigate the order of resiliency and the nonlinearities of the constructed functions F and G, and show that the disjoint spectra functions F and G are highly nonlinear and resilient on $\mathbb{F}_2^{n+4}$.

Theorem 4.3.2. *Let f_0 and g_0 be two disjoint spectra optimal plateaued resilient Boolean functions with profile $(n, m, n-m-1, 2^{n-1} - 2^{m+1})$, and f, g, h are same as defined in Theorem 4.3.1. Then the functions F and G as constructed in Theorem 4.3.1 are disjoint spectra highly nonlinear resilient functions with profile $(n+4, m+1, n-m, 2^{n+3} - 2^{m+3})$ and $(n+4, m+2, n-m, 2^{n+3} - 2^{m+4})$, respectively.*

Proof. Since $f = f_0 \parallel g_0$, therefore, by Lemma 4.2.2 and Lemma 4.2.3, it follows that the function $f \parallel \overline{f}$ is an $(m+1)$-resilient function having nonlinearity $nl(f \parallel \overline{f}) = 2nl(f)$. Let $P = f \parallel \overline{f} \parallel f \parallel \overline{f}$. Then by using Proposition 4.2.5, for any $\mathbf{w} \in \mathbb{F}_2^n$, we get $W_P(00\mathbf{w}) = 0$, $W_P(01\mathbf{w}) = 4W_f(\mathbf{w})$, $W_P(10\mathbf{w}) = 0$, $W_P(11\mathbf{w}) = 0$. Also, if $w_H(01\mathbf{w}) \leq m+1$, then it implies that $w_H(\mathbf{w}) \leq m$. Since f is an m-resilient Boolean function, therefore, we have $W_f(\mathbf{w}) = 0$, which implies that $W_P(01\mathbf{w}) = 0$. Hence, P is an $(m+1)$-resilient Boolean function, and from Lemma 4.2.1, the nonlinearity of P is will be $nl(P) = 4nl(f)$.

Now consider the function $F = f \parallel \overline{f} \parallel f \parallel \overline{f} \parallel \overline{f} \parallel \overline{f} \parallel f \parallel f$. Using Proposition 4.2.5, we get $W_F(000\mathbf{w}) = 0$, $W_F(001\mathbf{w}) = 4W_f(\mathbf{w})$, $W_F(010\mathbf{w}) = -4W_f(\mathbf{w})$, $W_F(100\mathbf{w}) = 0$,

$W_F(011\mathbf{w}) = 0$, $W_F(101\mathbf{w}) = 4W_f(\mathbf{w})$, $W_F(110\mathbf{w}) = 4W_f(\mathbf{w})$, $W_F(111\mathbf{w}) = 0$. Now if $w_H(001\mathbf{w})$, $w_H(010\mathbf{w}) \leq (m+1)$, then $w_H(\mathbf{w}) \leq m$. Hence, by using Proposition 4.2.5 we obtain, $W_F(001\mathbf{w}) = 0$, $W_F(010\mathbf{w}) = 0$, $W_F(101\mathbf{w}) = 0$, $W_F(110\mathbf{w}) = 0$. Therefore, F is an $(m+1)$-resilient Boolean function on $\mathbb{F}_2^{n+4}$.

From the profile of the function f it is clear that $max_{\mathbf{w}\in\mathbb{F}_2^{n+1}}|W_f(\mathbf{w})| = 2^{m+2}$, and the spectrum of F shows that $max_{u\in\mathbb{F}_2^3,\mathbf{w}\in\mathbb{F}_2^{n+1}}|W_F(u,\mathbf{w})| = 4\max_{\mathbf{w}\in\mathbb{F}_2^{n+1}}|W_f(\mathbf{w})| = 2^{m+4}$. Therefore, the nonlinearity of F is given by $nl(F) = 2^{n+3} - 2^{m+3}$.

From the construction of disjoint spectra functions $g = f_0 \parallel \overline{f_0}$, $h = g_0 \parallel \overline{g_0}$ and Lemma 4.2.2, it follows that g and h are the functions of profile $(n+1, m+1, n-m-1, 2^n - 2^{m+2})$. Now, on interchanging variables x_{n+1} and x_{n+2} in $g \parallel h = f_0 \parallel \overline{f_0} \parallel g_0 \parallel \overline{g_0}$, we get the function $f_0 \parallel g_0 \parallel \overline{f_0} \parallel \overline{g_0}$, which is same as the function concatenation $f \parallel \overline{f}$. Using Lemma 4.2.2, we get the nonlinearity $nl(g \parallel h) = 2nl_f$. Let $Q = g \parallel h \parallel h \parallel g$. Then by using Proposition 4.2.5, we get $W_Q(00\mathbf{w}) = 2W_g(\mathbf{w}) + 2W_h(\mathbf{w})$, $W_Q(01\mathbf{w}) = 0$, $W_Q(10\mathbf{w}) = 0$, $W_Q(11\mathbf{w}) = 2W_g(\mathbf{w}) - 2W_h(\mathbf{w})$. Now, if $w_H(00\mathbf{w}) \leq m+1$, then obviously $w_H(\mathbf{w}) \leq m+1$. Also, g and h are $(m+1)$-resilient functions, from which it follows that $W_g(\mathbf{w}) = 0$, $W_h(\mathbf{w}) = 0$, and hence $W_Q(11\mathbf{w}) = 0$. Therefore, Q is an $(m+1)$-resilient function and the nonlinearity of Q is given by $nl(Q) = 2nl(g \parallel h) = 4nl(f)$.

Now consider the function $G = g \parallel h \parallel h \parallel g \parallel \overline{g} \parallel \overline{h} \parallel \overline{h} \parallel \overline{g}$. Using Proposition 4.2.5, we get, $W_G(000\mathbf{w}) = 0$, $W_G(001\mathbf{w}) = 0$, $W_G(010\mathbf{w}) = 0$, $W_G(100\mathbf{w}) = 4W_g(\mathbf{w}) + 4W_h(\mathbf{w})$, $W_G(011\mathbf{w}) = 0$, $W_G(101\mathbf{w}) = 0$, $W_G(110\mathbf{w}) = 0$, $W_G(111\mathbf{w}) = 4W_g(\mathbf{w}) - 4W_h(\mathbf{w})$. Further, $w_H(100\mathbf{w}) \leq (m+2)$ implies that $w_H(\mathbf{w}) \leq m+1$. Since both g and h are $(m+1)$-resilient functions, therefore, $W_g(\mathbf{w}) = 0$, $W_h(\mathbf{w}) = 0$, from which it follows that $W_G(100\mathbf{w}) = 0$, $W_G(111\mathbf{w}) = 0$. Therefore, G is an $(m+2)$-resilient function.

From the profile of the functions g and h it is clear that $max_{\mathbf{w}\in\mathbb{F}_2^{n+1}}\{|W_g(\mathbf{w})|, |W_h(\mathbf{w})|\} = 2^{m+3}$. Since g and h are disjoint spectra functions, therefore, from the spectrum of G, we get

$$max_{u\in\mathbb{F}_2^3,\mathbf{w}\in\mathbb{F}_2^{n+1}}|W_F(u,\mathbf{w})| = 4max_{\mathbf{w}\in\mathbb{F}_2^{n+1}}\{|W_g(\mathbf{w})|, |W_h(\mathbf{w})|\} = 2^{m+5}.$$

Hence, the nonlinearity of G is $nl(G) = 2^{n+3} - 2^{m+4}$. From spectrum characterization matrices and the constructions of the functions F and G, it is clear that they are disjoint

spectra plateaued resilient functions with profiles $(n+4, m+1, n-m, 2^{n+3}-2^{m+3})$ and $(n+4, m+2, n-m, 2^{n+3}-2^{m+4})$, respectively. ■

It can be observed that the nonlinearity of some constructed functions (as constructed in Theorem 4.3.1) is better than the nonlinearity bounds obtained in [52].

In the following result, we construct another pair of concatenated functions. We prove that the constructed functions are highly nonlinear resilient and have disjoint spectra. We analyze the profiles of the constructed functions.

Theorem 4.3.3. *Let $F, G \in \mathcal{B}_{n+4}$ such that $F = f \parallel f \parallel \overline{f} \parallel \overline{f} \parallel \overline{f} \parallel \overline{f} \parallel f \parallel f$ and $G = g \parallel \overline{g} \parallel \overline{h} \parallel h \parallel \overline{g} \parallel g \parallel \overline{h} \parallel h$, where f, g, h are same as defined in Theorem 4.3.1. Then F and G are disjoint spectra resilient functions with the profile $(n+4, m+2, n-m, 2^{n+3}-2^{m+4})$.*

Proof. We have $F = f \parallel f \parallel \overline{f} \parallel \overline{f} \parallel \overline{f} \parallel \overline{f} \parallel f \parallel f$ and $G = g \parallel \overline{g} \parallel \overline{h} \parallel h \parallel \overline{g} \parallel g \parallel \overline{h} \parallel h$. Using Proposition 4.2.5, we obtain WHS of F and G as follows:

$W_F(000\mathbf{w}) = 0$, $W_F(001\mathbf{w}) = 0$, $W_F(010\mathbf{w}) = 0$, $W_F(011\mathbf{w}) = 0$, $W_F(100\mathbf{w}) = 0$,
$W_F(101\mathbf{w}) = 0$, $W_F(110\mathbf{w}) = 8W_f(\mathbf{w})$, $W_F(111\mathbf{w}) = 0$, and
$W_G(000\mathbf{w}) = 0$, $W_G(001\mathbf{w}) = -4W_h(\mathbf{w})$, $W_G(010\mathbf{w}) = 0$, $W_G(011\mathbf{w}) = 4W_h(\mathbf{w})$,
$W_G(100\mathbf{w}) = 0$, $W_G(101\mathbf{w}) = 4W_g(\mathbf{w})$, $W_G(110\mathbf{w}) = 0$, $W_G(111\mathbf{w}) = 4W_g(\mathbf{w})$.

Now, by using Proposition 4.2.5, we obtain the spectrum characterization matrix for f and hence for the function F as follows:

$$NZ(f) = \begin{pmatrix} 0 & \parallel NZ(f_0) \\ 1 & \parallel NZ(f_0) \\ 0 & \parallel NZ(g_0) \\ 1 & \parallel NZ(g_0) \end{pmatrix}$$

and

$$NZ(F) = \begin{pmatrix} 110 & \parallel NZ(f) \end{pmatrix} = \begin{pmatrix} 1100 & \parallel NZ(f_0) \\ 1101 & \parallel NZ(f_0) \\ 1100 & \parallel NZ(g_0) \\ 1101 & \parallel NZ(g_0) \end{pmatrix}.$$

Using similar computation, the spectrum characterization matrix of G is given by

$$NZ(g) = 1 \parallel NZ(f_0), \quad NZ(h) = 1 \parallel NZ(g_0) \text{ and,}$$

$$NZ(G) = \begin{pmatrix} 001 & \parallel NZ(g) \\ 011 & \parallel NZ(g) \\ 101 & \parallel NZ(g) \\ 111 & \parallel NZ(g) \\ 001 & \parallel NZ(h) \\ 011 & \parallel NZ(h) \\ 101 & \parallel NZ(h) \\ 111 & \parallel NZ(h) \end{pmatrix} = \begin{pmatrix} 0011 & \parallel NZ(f_0) \\ 0111 & \parallel NZ(f_0) \\ 1011 & \parallel NZ(f_0) \\ 1111 & \parallel NZ(f_0) \\ 0011 & \parallel NZ(g_0) \\ 0111 & \parallel NZ(g_0) \\ 1011 & \parallel NZ(g_0) \\ 1111 & \parallel NZ(g_0) \end{pmatrix}.$$

From the construction of the functions F and G, and their spectrum characterization matrices, we observe that F and G are disjoint spectra resilient Boolean functions on $\mathbb{F}_2^{n+4}$. Also, it is noted that both F and G have same profile $(n+4, m+2, n-m, 2^{n+3} - 2^{m+4})$. ■

Given below are two more constructions of highly nonlinear resilient Boolean function with disjoint spectra.

(i) If $F = \overline{f} \parallel f \parallel \overline{f} \parallel f \parallel f \parallel \overline{f} \parallel f \parallel \overline{f}$ and $G = \overline{g} \parallel \overline{g} \parallel g \parallel g \parallel \overline{h} \parallel \overline{h} \parallel h \parallel h$.

(ii) If $F = g \parallel \overline{g} \parallel \overline{h} \parallel h \parallel \overline{g} \parallel g \parallel \overline{h} \parallel h$ and $G = \overline{g} \parallel \overline{g} \parallel g \parallel g \parallel \overline{h} \parallel \overline{h} \parallel h \parallel h$.

After analyzing the profiles of these functions, we found that their profiles match with the profiles of the functions discussed in Theorem 4.3.3.

Chapter 5

Some results on q-ary bent functions

5.1 Introduction

The present chapter is devoted to the study of q-ary functions. A q-ary function is a function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, where $\mathbb{Z}_q$ is the ring of integers modulo q. These functions were introduced by Kumar et al. [87] as a generalization of the classical Boolean functions. Let $\mathcal{B}_{n,q}$ be the set of all q-ary functions on n-variables. It is well known that most of the cryptographic criteria of the functions employed in various cryptosystems can be determined by means of their Walsh-Hadamard transform (WHT). The WHT of $f \in \mathcal{B}_{n,q}$ is a complex valued function on $\mathbb{Z}_q^n$ defined by

$$\mathcal{W}_f(\mathbf{u}) = \frac{1}{q^{\frac{n}{2}}} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{f(\mathbf{x}) + \langle \mathbf{x}, \mathbf{u} \rangle},$$

where $\xi = e^{\frac{2\pi i}{q}}$ denotes the complex q-th primitive root of unity and $\langle \mathbf{x},\ \mathbf{u} \rangle$ is the usual inner product in $\mathbb{Z}_q^n$.

A function $f \in \mathcal{B}_{n,q}$ is called *q-ary bent* if $|\mathcal{W}_f(\mathbf{u})| = 1$ for every $\mathbf{u} \in \mathbb{Z}_q^n$. It has been proved in [87] that the q-ary bent functions exist for every value of q and n, except when n is odd and $q \equiv 2 \mod 4$. It is well known that Boolean bent functions [124] exist only for even n. Kumar et al. [87] have discussed several important properties of q-ary bent functions in terms of their WHT and autocorrelation spectrum. They have provided an analogue of classical Maiorana-McFarland class of bent functions in the q-ary setup and discussed several properties of these functions. They have remarked that establishing properties of q-ary bent

functions analogous to binary functions is far more difficult. q-ary bent functions are widely applicable in Code-Division Multiple-Access (CDMA) communications systems [131]. For more results on q-ary bent functions we refer to [20, 70–72, 75, 142].

Recall that the crosscorrelation between two functions $f, g \in \mathcal{B}_{n,q}$ at $\mathbf{u} \in \mathbb{Z}_q^n$ is given by

$$\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})},$$

and for $f = g$, the sum $\mathcal{C}_{f,f}(\mathbf{u}) = \mathcal{C}_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-f(\mathbf{x}+\mathbf{u})}$ is called the autocorrelation of f at $\mathbf{u}$.

The low crosscorrelation of sequences is relevant to the CDMA applications. Kumar et al. [86] have introduced a large family of quaternary sequences with low correlation.

It follows from Shannon's basic design principles *confusion and diffusion* [137] of secret key cryptosystems, that it is good if the constituent functions of secret key system have low crosscorrelation and certain uniformity properties. Therefore, it is important to study the correlation properties of cryptographic functions and investigating functions with low correlation. Recently, Sarkar and Maitra [128], and Zhou et al. [166] have reported some interesting results in this direction.

The SAC [155, 156] and the PC of Boolean functions [122] are two important cryptographic criteria, but they determine only the local properties of the functions. For global analysis, Zhang and Zheng [162] have introduced the concept of global avalanche characteristic (GAC) and proposed two indicators: the *sum-of-squares indicator* and the *absolute indicator* of one Boolean function. Zhou et al. [166] have studied these indicators for two Boolean functions to analyze the global behaviour of cryptographic functions.

In this chapter, analogous to the two indicators proposed in [162], we define two similar indicators: the *sum-of-squares-of-modulus indicator* (SSMI) and *modulus indicator* (MI) of crosscorrelation between two functions in the q-ary setup. The SSMI of $f, g \in \mathcal{B}_{n,q}$ is defined as

$$\sigma_{f,g} = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\mathbf{u})|^2,$$

and the MI of $f, g \in \mathcal{B}_{n,q}$ is defined as

$$\triangle_{f,g} = \max_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\mathbf{u})|.$$

For $f = g$, the SSMI of $f \in \mathcal{B}_{n,q}$ is defined as

$$\sigma_f = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_f(\mathbf{u})|^2,$$

and the MI of $f \in \mathcal{B}_{n,q}$ is defined as

$$\triangle_f = \max_{\mathbf{u}\in\mathbb{Z}_q^n, \mathbf{u}\neq\mathbf{0}} |\mathcal{C}_f(\mathbf{u})|.$$

We study the q-ary functions in terms of these two indicators, the SSMI and the MI, and obtain some lower and upper bounds on these indicators. Further, we compute the crosscorrelation of a subclass of Maiorana-McFarland (MM) type q-ary bent functions and obtain the values of the indicators the SSMI and the MI for these functions. We provide a characterization of quaternary ($q = 4$) bent functions on $n + 1$ variables in terms of their subfunctions on n-variables. We have generalized several cryptographic properties of Boolean functions to the q-ary setup. Several properties of q-ary functions are presented in terms of their WHT, autocorrelation and crosscorrelation spectra. We also present some constructions of balanced quaternary functions with high nonlinearity under the Lee metric.

The following lemma is an important property and will be frequently used in the subsequent chapters including this chapter.

Lemma 5.1.1. *[87] Let n be a positive integer and $\mathbf{u} \in \mathbb{Z}_q^n$, then*

$$\sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{<\mathbf{u},\ \mathbf{x}>} = \begin{cases} q^n, & \text{if } \mathbf{u} = 0, \\ 0, & \text{otherwise .} \end{cases}$$

5.2 Properties of WHT in the q-ary setup

In this section, we present several properties regarding the behavior of WHT on various combinations of q-ary functions, and deduce its relationship with their crosscorrelation and autocorrelation spectra.

Theorem 5.2.1. *If $f, g \in \mathcal{B}_{n,q}$ and $\mathbf{u}, \mathbf{y} \in \mathbb{Z}_q^n$, then*

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\ \xi^{\langle -\mathbf{u},\ \mathbf{y}\rangle} = q^n \mathcal{W}_f(\mathbf{y})\overline{\mathcal{W}_g(\mathbf{y})},\ \textit{and}$$

$$\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{y})\overline{\mathcal{W}_g(\mathbf{y})}\ \ \xi^{\langle \mathbf{u},\ \mathbf{y}\rangle}.$$

Proof. The crosscorrelation between f and g is

$$\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})}.$$

By using Lemma 5.1.1, we get

$$\begin{aligned}
\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\xi^{\langle -\mathbf{u},\ \mathbf{y}\rangle} &= \sum_{\mathbf{u}\in\mathbb{Z}_q^n}\sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})+\langle -\mathbf{u},\ \mathbf{y}\rangle} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{-g(\mathbf{x}+\mathbf{u})+\langle -\mathbf{u},\ \mathbf{y}\rangle} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{-g(\mathbf{u})+\langle \mathbf{x}-\mathbf{u},\ \mathbf{y}\rangle} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})+\langle \mathbf{x},\ \mathbf{y}\rangle} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{-(g(\mathbf{u})+\langle \mathbf{u},\ \mathbf{y}\rangle)} \\
&= q^n \mathcal{W}_f(\mathbf{y})\overline{\mathcal{W}_g(\mathbf{y})}.
\end{aligned}$$

Therefore,
$$\begin{aligned}
\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{y})\overline{\mathcal{W}_g(\mathbf{y})}\xi^{\langle \mathbf{u},\ \mathbf{y}\rangle} &= \frac{1}{q^n}\sum_{\mathbf{y}\in\mathbb{Z}_q^n}\sum_{\mathbf{v}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{v})\xi^{\langle -\mathbf{v},\ \mathbf{y}\rangle+\langle \mathbf{u},\ \mathbf{y}\rangle} \\
&= \frac{1}{q^n}\sum_{\mathbf{v}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{v}) \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{\langle \mathbf{u}-\mathbf{v},\ \mathbf{y}\rangle} \\
&= \mathcal{C}_{f,g}(\mathbf{u}).
\end{aligned}$$

■

In particular, if $f = g$, then we have the following corollary.

Corollary 5.2.2. *Let f be a q-ary function on $\mathbb{Z}_q^n$ then the autocorrelation of f is*

$$\mathcal{C}_f(\mathbf{x}) = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{y})|^2 \xi^{\langle \mathbf{x},\ \mathbf{y}\rangle}.$$

By putting $\mathbf{x} = \mathbf{0}$ in the above corollary, we obtain

$$\sum_{\mathbf{y}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{y})|^2 = q^n,$$

which is known as Parseval's identity in the q-ary setup.

The following corollary is due to Kumar et al. [87, Property 4]. An alternative proof of this result follows from Lemma 5.1.1 and Corollary 5.2.2.

Corollary 5.2.3. *A function $f \in \mathcal{B}_{n,q}$ is q-ary bent if and only if $\mathcal{C}_f(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n \setminus \{0\}$.*

In Theorem 5.2.5 below, we present a generalization of [169, Theorem 1] (obtained for $q = 2$) to the q-ary functions. To prove the result, we need following lemma.

Lemma 5.2.4. *Let $f, g, h \in \mathcal{B}_{n,q}$ be such that $h(\mathbf{x}) = f(\mathbf{x}) - g(\mathbf{x})$. Then*

$$\mathcal{W}_h(\mathbf{v}) = \frac{1}{q^{n/2}} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{u}+\mathbf{v})\overline{\mathcal{W}_g(\mathbf{u})}, \quad \forall\ \mathbf{v} \in \mathbb{Z}_q^n.$$

Proof. For any $\mathbf{v} \in \mathbb{Z}_q^n$, using Lemma 5.1.1, we have

$$\begin{aligned}
\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{u}+\mathbf{v})\overline{\mathcal{W}_g(\mathbf{u})} &= \frac{1}{q^n} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})+\langle \mathbf{u}+\mathbf{v},\mathbf{x}\rangle} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{-g(\mathbf{y})-\langle \mathbf{u},\mathbf{y}\rangle} \\
&= \frac{1}{q^n} \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-g(\mathbf{y})+\langle \mathbf{v},\mathbf{x}\rangle} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{\langle \mathbf{u},\mathbf{x}-\mathbf{y}\rangle} \\
&= q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-g(\mathbf{x})+\langle \mathbf{v},\mathbf{x}\rangle} = q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{h(\mathbf{x})+\langle \mathbf{v},\mathbf{x}\rangle} \\
&= q^{n/2}\mathcal{W}_h(\mathbf{v}).
\end{aligned} \tag{5.2.1}$$

This completes the proof. ∎

Theorem 5.2.5. *If $f, g \in \mathcal{B}_{n,q}$ and $\mathbf{e} \in \mathbb{Z}_q^n$. Then for any $\mathbf{v} \in \mathbb{Z}_q^n$, we have*

$$\mathcal{W}_{D_{\mathbf{e}}(f,g)}(\mathbf{v}) = \frac{1}{q^{n/2}} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \xi^{\langle \mathbf{u}, \mathbf{e} \rangle} \mathcal{W}_f(\mathbf{u}+\mathbf{v}) \overline{\mathcal{W}_g(\mathbf{u})}, \quad \textit{and} \tag{5.2.2}$$

$$\mathcal{W}_f(\mathbf{u}+\mathbf{v}) \overline{\mathcal{W}_g(\mathbf{u})} = \frac{1}{q^{n/2}} \sum_{\mathbf{e} \in \mathbb{Z}_q^n} \xi^{-\langle \mathbf{u}, \mathbf{e} \rangle} \mathcal{W}_{D_{\mathbf{e}}(f,g)}(\mathbf{v}). \tag{5.2.3}$$

Proof. Let $g_{\mathbf{e}}(\mathbf{x}) = g(\mathbf{e}+\mathbf{x})$. Then

$$\mathcal{W}_{g_{\mathbf{e}}}(\mathbf{u}) = \xi^{-\langle \mathbf{u}, \mathbf{e} \rangle} \mathcal{W}_g(\mathbf{u}). \tag{5.2.4}$$

From Lemma 5.2.4, replacing g by $g_{\mathbf{e}}$ and h by $D_{\mathbf{e}}(f,g)$, we get

$$\mathcal{W}_{D_{\mathbf{e}}(f,g)}(\mathbf{v}) = \frac{1}{q^{n/2}} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{u}+\mathbf{v}) \overline{\mathcal{W}_{g_{\mathbf{e}}}(\mathbf{u})}. \tag{5.2.5}$$

Combining equations (5.2.4) and (5.2.5), we obtain the desired result in (5.2.2).

Now, from Lemma 5.1.1 and (5.2.2), we have

$$\begin{aligned}
\sum_{\mathbf{e} \in \mathbb{Z}_q^n} \xi^{-\langle \mathbf{u}, \mathbf{e} \rangle} \mathcal{W}_{D_{\mathbf{e}}(f,g)}(\mathbf{v}) &= \frac{1}{q^{n/2}} \sum_{\mathbf{e} \in \mathbb{Z}_q^n} \xi^{-\langle \mathbf{u}, \mathbf{e} \rangle} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{\langle \mathbf{x}, \mathbf{e} \rangle} \mathcal{W}_f(\mathbf{x}+\mathbf{v}) \overline{\mathcal{W}_g(\mathbf{x})} \\
&= \frac{1}{q^{n/2}} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{x}+\mathbf{v}) \overline{\mathcal{W}_g(\mathbf{x})} \sum_{\mathbf{e} \in \mathbb{Z}_q^n} \xi^{\langle \mathbf{e}, \mathbf{x}-\mathbf{u} \rangle} \\
&= q^{n/2} \mathcal{W}_f(\mathbf{u}+\mathbf{v}) \overline{\mathcal{W}_g(\mathbf{u})}.
\end{aligned}$$

Hence the result. ∎

5.3 Characterizations of q-ary bent functions

Let $\mathbf{v} = (v_r, \ldots, v_1)$ and $f \in \mathcal{B}_{n,q}$. We define restriction function $f_{\mathbf{v}}$ of f as follows

$$f_{\mathbf{v}}(x_{n-r}, \ldots, x_1) = f(x_n = v_r, \ldots, x_{n-r+1} = v_1, x_{n-r}, \ldots, x_1).$$

Also recall that the concatenation $\mathbf{uw}$ of two elements $\mathbf{u} = (u_r, \ldots, u_1) \in \mathbb{Z}_q^r$ and

$\mathbf{w} = (w_{n-r}, \ldots, w_1) \in \mathbb{Z}_q^{n-r}$ is the following element in $\mathbb{Z}_q^n$.

$$\mathbf{uw} = (\mathbf{u}, \mathbf{w}) = (u_r, \ldots, u_1, w_{n-r}, \ldots, w_1).$$

Theorem 5.3.1. *Let $\mathbf{u} \in \mathbb{Z}_q^r$, $\mathbf{w} \in \mathbb{Z}_q^{n-r}$ and f be an n-variable q-ary function on $\mathbb{Z}_q^n$. Then the autocorrelation of f is given by*

$$\mathcal{C}_f(\mathbf{uw}) = \sum_{\mathbf{v} \in \mathbb{Z}_q^r} \mathcal{C}_{f_\mathbf{v}, f_{\mathbf{v}+\mathbf{u}}}(\mathbf{w}).$$

Proof. We have

$$\begin{aligned}
\mathcal{C}_f(\mathbf{uw}) &= \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{f(\mathbf{x}) - f(\mathbf{x}+\mathbf{uw})} \\
&= \sum_{\mathbf{v} \in \mathbb{Z}_q^r} \sum_{\mathbf{z} \in \mathbb{Z}_q^{n-r}} \xi^{f(\mathbf{vz}) - f(\mathbf{vz}+\mathbf{uw})} \\
&= \sum_{\mathbf{v} \in \mathbb{Z}_q^r} \sum_{\mathbf{z} \in \mathbb{Z}_q^{n-r}} \xi^{f_\mathbf{v}(\mathbf{z}) - f_{\mathbf{v}+\mathbf{u}}(\mathbf{z}+\mathbf{w})} \\
&= \sum_{\mathbf{v} \in \mathbb{Z}_q^r} \mathcal{C}_{f_\mathbf{v}, f_{\mathbf{v}+\mathbf{u}}}(\mathbf{w}).
\end{aligned}$$

■

Any two q-ary functions f and g are said to have *complementary autocorrelation* if $\mathcal{C}_f(\mathbf{u}) + \mathcal{C}_g(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}\}$. The following result gives a necessary and sufficient condition for two q-ary functions to have complementary autocorrelation.

Theorem 5.3.2. *Any two generalized q-ary functions f and g on $\mathbb{Z}_q^n$ have complementary autocorrelation if and only if*

$$|\mathcal{W}_f(\mathbf{u})|^2 + |\mathcal{W}_g(\mathbf{u})|^2 = 2, \text{ for all } \mathbf{u} \in \mathbb{Z}_q^n.$$

Proof. Let $f, g \in \mathcal{B}_{n,q}$. Suppose that f and g possess complimentary autocorrelation. Then

$$q^n(|\mathcal{W}_f(\mathbf{u})|^2 + |\mathcal{W}_g(\mathbf{u})|^2) = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} (\mathcal{C}_f(\mathbf{x}) + \mathcal{C}_g(\mathbf{x}))\xi^{\langle -\mathbf{u}, \mathbf{x} \rangle} = 2q^n,$$

which implies that, $|\mathcal{W}_f(\mathbf{u})|^2 + |\mathcal{W}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{Z}_q^n$.

Conversely, suppose that $|\mathcal{W}_f(\mathbf{u})|^2 + |\mathcal{W}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{Z}_q^n$. Then

$$\begin{aligned}\mathcal{C}_f(\mathbf{x}) + \mathcal{C}_g(\mathbf{x}) &= \sum_{\mathbf{u}\in\mathbb{Z}_q^n} (|\mathcal{W}_f(\mathbf{u})|^2 + |\mathcal{W}_g(\mathbf{u})|^2)\xi^{\langle \mathbf{u},\mathbf{x}\rangle} \\ &= 2\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{\langle \mathbf{u},\mathbf{x}\rangle} = 2q^n\delta_{\mathbf{0}}(\mathbf{x}),\end{aligned}$$

and therefore, $\mathcal{C}_f(\mathbf{x}) + \mathcal{C}_g(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}\}$. Thus, the functions f and g have complementary autocorrelation. ■

Tokareva [151] has presented a sufficient condition for the direct sum of two q-ary functions to be q-ary bent. The following theorem is a slightly generalized version of this result [151, Theorem 3].

Theorem 5.3.3. *Let $f_1 \in \mathcal{B}_{r,q}$ and $f_2 \in \mathcal{B}_{s,q}$. Then a function $g \in \mathcal{B}_{r+s,q}$ expressed as*

$$g(x_{r+s}, \ldots, x_{r+1}, x_r, \ldots, x_1) = f_1(x_r, \ldots, x_1) + f_2(x_{r+s}, \ldots, x_{r+1}),$$

is q-ary bent if and only if f_1 and f_2 both are q-ary bent functions.

Proof. Let $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^r \times \mathbb{Z}_q^s$. Then

$$\begin{aligned}\mathcal{W}_g(\mathbf{u}, \mathbf{v}) &= \frac{1}{q^{\frac{r+s}{2}}} \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{Z}_q^r\times\mathbb{Z}_q^s} \xi^{f(\mathbf{x},\mathbf{y})+\langle \mathbf{u},\mathbf{x}\rangle+\langle \mathbf{v},\mathbf{y}\rangle} \\ &= \frac{1}{q^{\frac{r}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_q^r} \xi^{f_1(\mathbf{x})+\langle \mathbf{u},\mathbf{x}\rangle} \ \frac{1}{q^{\frac{s}{2}}} \sum_{\mathbf{y}\in\mathbb{Z}_q^s} \xi^{f_2(\mathbf{y})+\langle \mathbf{v},\mathbf{y}\rangle} \\ &= \mathcal{W}_{f_1}(\mathbf{u})\mathcal{W}_{f_2}(\mathbf{v}).\end{aligned}$$

Now if f_1 and f_2 both are q-ary bent functions, then $|\mathcal{W}_{f_1}(\mathbf{u})| = 1$ and $|\mathcal{W}_{f_2}(\mathbf{v})| = 1$, implying that, $|\mathcal{W}_f(\mathbf{u}, \mathbf{v})| = |\mathcal{W}_{f_1}(\mathbf{u})||\mathcal{W}_{f_2}(\mathbf{v})| = 1$ for all $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^r \times \mathbb{Z}_q^s$. Hence, g is a q-ary bent function.

Conversely, suppose that g is a q-ary bent function. We want to show that the functions f_1 and f_2 are also q-ary bent. Let us suppose that f_1 is not a q-ary bent function. Then

there exists $\mathbf{u} \in \mathbb{Z}_q^r$ such that $|\mathcal{W}_{f_1}(\mathbf{u})| > 1$. This implies that $|\mathcal{W}_{f_2}(\mathbf{v})| < 1$ for every $\mathbf{v} \in \mathbb{Z}_q^s$. Since $|\mathcal{W}_{f_1}(\mathbf{u})||\mathcal{W}_{f_2}(\mathbf{v})| = 1$, this contradicts the fact that $\sum_{\mathbf{v}\in\mathbb{Z}_q^s} |\mathcal{W}_{f_2}(\mathbf{v})|^2 = q^s$. ■

5.4 Two indicators of crosscorrelation for q-ary functions

Recall that a function $f \in \mathcal{B}_{n,q}$ is said to be *balanced* if $|\{\mathbf{x} : \ f(\mathbf{x}) = k\}| = q^{n-1}$ for all $k \in \mathbb{Z}_q$.

In the following result, by using the definition of $\triangle_{f,g}$, we obtain a lower and an upper bound on $\triangle_{f,g}$. The result for binary case is proved by Zhou et al. in [166].

Theorem 5.4.1. *Let $f, g \in \mathcal{B}_{n,q}$. Then*

(a) $\triangle_{f,g} = 0$ *if and only if* $f(\mathbf{x}) - g(\mathbf{x}+\mathbf{u})$ *is balanced for all* $\mathbf{u} \in \mathbb{Z}_q^n$.

(b) $\triangle_{f,g} = q^n$ *if and only if* $f(\mathbf{x}) = g(\mathbf{x}+\mathbf{u}) + a$, $a \in \mathbb{Z}_q$ *for some* $\mathbf{u} \in \mathbb{Z}_q^n$.

(c) $0 \leq \triangle_{f,g} \leq q^n$.

Proof. (a) Let $f(\mathbf{x}) - g(\mathbf{x}+\mathbf{u})$ is a balanced for all $\mathbf{u} \in \mathbb{Z}_q^n$. Then

$$|\{\mathbf{x} : \ f(\mathbf{x}) - g(\mathbf{x}+\mathbf{u}) = k\}| = q^{n-1} \ \text{ for all } k \in \mathbb{Z}_q.$$

Therefore, the crosscorrelation of $f, g \in \mathcal{B}_{n,q}$ at $\mathbf{u} \in \mathbb{Z}_q^n$ becomes

$$\begin{aligned} \mathcal{C}_{f,g}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})} = q^{n-1} \sum_{k\in\mathbb{Z}_q} \xi^k \\ &= q^{n-1}\left(\frac{1-\xi^q}{1-\xi}\right) = 0. \end{aligned}$$

Since $f(\mathbf{x}) - g(\mathbf{x}+\mathbf{u})$ is balanced for all $\mathbf{u} \in \mathbb{Z}_q^n$, therefore $\mathcal{C}_{f,g}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n$. Therefore, by definition, we get $\triangle_{f,g} = 0$.

The results in part (b) and (c) directly follow from the definition of $\triangle_{f,g}$. ■

Definition 5.4.2. *[128] Let $f, g \in \mathcal{B}_{n,q}$. Then f and g are said to be* perfectly uncorrelated *if $\mathcal{W}_f(\mathbf{u})\mathcal{W}_g(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n$.*

In the following theorem, we provide the lower and upper bounds on the indicator $\sigma_{f,g}$. For $q = 2$, the results were obtained in [166].

Theorem 5.4.3. *Let $f, g \in \mathcal{B}_{n,q}$. Then*

(*a*) $|\mathcal{C}_{f,g}(0)|^2 \leq \sigma_{f,g} \leq q^{3n}$

(*b*) $\sigma_{f,g} = q^{3n}$ *if and only if f and g are affine functions.*

(*c*) $\sigma_{f,g} = |\mathcal{C}_{f,g}(0)|^2$ *if and only if f and g are either generalized bent functions or perfectly uncorrelated.*

Proof. (*a*) Using Theorem 5.2.1 and Cauchy-Schwarz inequality, $\left(\sum_i a_i b_i\right)^2 \leq \sum_i a_i^2 \sum_i b_i^2$ for all $a_i, b_i \in \mathbb{R}$, we have

$$\begin{aligned}
\sigma_{f,g} &= \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{f,g}(\mathbf{u})} \\
&= \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{x})\overline{\mathcal{W}_g(\mathbf{x})}\xi^{\langle -\mathbf{u},\ \mathbf{x}\rangle} \overline{\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{y})\overline{\mathcal{W}_g(\mathbf{y})}\xi^{\langle -\mathbf{u},\ \mathbf{y}\rangle}} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{x})\overline{\mathcal{W}_f(\mathbf{y})\mathcal{W}_g(\mathbf{x})}\mathcal{W}_g(\mathbf{y}) \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{\langle \mathbf{u},\ \mathbf{y}-\mathbf{x}\rangle} \\
&= q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 |\mathcal{W}_g(\mathbf{x})|^2 \leq q^n \left(\sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})\mathcal{W}_g(\mathbf{x})| \right)^2 \\
&\leq q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_g(\mathbf{x})|^2 = q^{3n}.
\end{aligned}$$

(*b*) From (*a*), we get that $\sigma_{f,g} = q^{3n}$ if and only if

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u})|^2 |\mathcal{W}_g(\mathbf{u})|^2 = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u})|^2 \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{W}_g(\mathbf{u})|^2.$$

That is, $\sum_{\mathbf{u},\mathbf{v}\in\mathbb{Z}_q^n \ \ \mathbf{u}\neq\mathbf{v}} |\mathcal{W}_f(\mathbf{u})|^2 |\mathcal{W}_g(\mathbf{v})|^2 = 0$ if and only if $|\mathcal{W}_f(\mathbf{u})|^2 |\mathcal{W}_g(\mathbf{v})|^2 = 0$ for any $\mathbf{u} \neq \mathbf{v}$.

If $|\mathcal{W}_f(\mathbf{u})|^2 = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n$, then it contradicts the Parseval's identity. Therefore $|\mathcal{W}_f(\mathbf{u}_0)|^2 \neq 0$ for at least one $\mathbf{u}_0 \in \mathbb{Z}_q^n$. Consider now the following cases:

(1) If there exist only one $\mathbf{u}_0 \in \mathbb{Z}_q^n$ such that $|\mathcal{W}_f(\mathbf{u}_0)|^2 \neq 0$ then $|\mathcal{W}_g(\mathbf{v})|^2 = 0$ for all $\mathbf{v} \in \mathbb{Z}_q^n$ except $\mathbf{v} \neq \mathbf{u}_0$. By Parseval identity, we have $|\mathcal{W}_f(\mathbf{u}_0)|^2 = q^n$, which implies that $f(\mathbf{x}) = a - \langle \mathbf{u}_0, \mathbf{x} \rangle$ for some $a \in \mathbb{Z}_q$. On the other hand, $|\mathcal{W}_g(\mathbf{v})|^2 = 0$ for any $\mathbf{v} \neq \mathbf{u}_0$ implies that $|\mathcal{W}_g(\mathbf{u}_0)|^2 = q^n$. That is, $g(\mathbf{x}) = b - \langle \mathbf{u}_0, \mathbf{x} \rangle$ for some $b \in \mathbb{Z}_q$. Thus, f and g are affine.

(2) If there exist only two $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}_q^n$ $(\mathbf{u}_1 \neq \mathbf{u}_2)$ such that $|\mathcal{W}_f(\mathbf{u}_1)|^2 \neq 0$ and $|\mathcal{W}_f(\mathbf{u}_2)|^2 \neq 0$, then $|\mathcal{W}_g(\mathbf{u})|^2 = 0$ for any $\mathbf{u} \neq \mathbf{u}_1$ and $|\mathcal{W}_g(\mathbf{u})|^2 = 0$ for any $\mathbf{u} \neq \mathbf{u}_2$ accordingly. That is, $|\mathcal{W}_g(\mathbf{u})|^2 = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n$, which contradicts the Parseval's identity. Similarly, there do not exist only k distinct $\mathbf{u}_i \in \mathbb{Z}_q^n$, $1 \leq i \leq k$, $3 \leq k \leq 2^n$, such that $|\mathcal{W}_f(\mathbf{u}_i)|^2 \neq 0$.

(*c*) $\sigma_{f,g} = (\mathcal{C}_{f,g}(0))^2$ if and only if

$$\sum_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u})|^2 |\mathcal{W}_g(\mathbf{u})|^2 \sum_{\mathbf{u} \in \mathbb{Z}_q^n} 1^2 = \left(\sum_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u}) \overline{\mathcal{W}_g(\mathbf{u})}| \times 1 \right)^2,$$

if and only if, by Cauchy-Schwartz's inequality, for any $\mathbf{u} \in \mathbb{Z}_q^n$, $|\mathcal{W}_f(\mathbf{u})\overline{\mathcal{W}_g(\mathbf{u})}|/1 = \phi(\mathbf{u})$ such that $|\phi(\mathbf{u})| = k$ (constant). There are two cases:

(1) If $k = 0$, then f and g are perfectly uncorrelated.

(2) If $k \neq 0$, then $|\mathcal{W}_f(\mathbf{u})\overline{\mathcal{W}_g(\mathbf{u})}| = k$ for all $\mathbf{u} \in \mathbb{Z}_q^n$. So, $|\mathcal{W}_f(\mathbf{u})\overline{\mathcal{W}_g(\mathbf{u})}| = |\mathcal{W}_f(\mathbf{v})\overline{\mathcal{W}_g(\mathbf{v})}| = k$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_q^n$. This is equivalent to $\frac{|\mathcal{W}_f(\mathbf{u})|}{|\mathcal{W}_f(\mathbf{v})|} = \frac{|\mathcal{W}_g(\mathbf{v})|}{|\mathcal{W}_g(\mathbf{u})|} = t$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_q^n$, where t is a positive real number. That is, $|\mathcal{W}_f(\mathbf{u})| = t|\mathcal{W}_f(\mathbf{v})|$ and $|\mathcal{W}_g(\mathbf{v})| = t|\mathcal{W}_g(\mathbf{u})|$. Using Parseval's identity, we get $t^2 = 1$. Therefore, $|\mathcal{W}_f(\mathbf{u})|^2$ and $|\mathcal{W}_g(\mathbf{u})|^2$ are constants for all $\mathbf{u} \in \mathbb{Z}_q^n$. Again by using Parseval's identity, we get $|\mathcal{W}_f(\mathbf{u})| = 1 = |\mathcal{W}_g(\mathbf{u})|$ for all $\mathbf{u} \in \mathbb{Z}_q^n$ which proves that f and g both are generalized bent functions.

■

For any $\mathbf{u} \in \mathbb{Z}_q^n$, it is easy to verify that

$$| W_f(\mathbf{u}) |^2 = \frac{1}{q^n} \sum_{a \in \mathbb{Z}_q^n} \xi^{\langle \mathbf{a}, \mathbf{u} \rangle} \overline{C_f(a)} = \frac{1}{q^n} \sum_{a \in \mathbb{Z}_q^n} \xi^{\langle -a, \mathbf{u} \rangle} C_f(a). \tag{5.4.1}$$

A relationship between the WHT and the autocorrelation of any two q-ary functions is obtained in the following result.

Theorem 5.4.4. *Let $f, g \in \mathcal{B}_{n,q}$, and $\mathbf{v} \in \mathbb{Z}_q^n$. Then*

$$\sum_{\mathbf{u} \in \mathbb{Z}_q^n} | W_f(\mathbf{u}) |^2 | W_g(\mathbf{u} + \mathbf{v}) |^2 = \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} C_f(\mathbf{a}) \overline{C_g(\mathbf{a})} \xi^{\langle \mathbf{a}, \mathbf{v} \rangle}. \tag{5.4.2}$$

Proof. From (5.4.1), for any $\mathbf{v} \in \mathbb{Z}_q^n$, we have

$$\begin{aligned}
\sum_{\mathbf{u} \in \mathbb{Z}_q^n} | W_f(\mathbf{u}) |^2 | W_g(\mathbf{u} + \mathbf{v}) |^2 &= \frac{1}{q^{2n}} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} \xi^{\langle -\mathbf{a}, \mathbf{u} \rangle} C_f(\mathbf{a}) \sum_{\mathbf{b} \in \mathbb{Z}_q^n} \xi^{\langle \mathbf{b}, \mathbf{u} + \mathbf{v} \rangle} \overline{C_g(\mathbf{b})} \\
&= \frac{1}{q^{2n}} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} \sum_{\mathbf{b} \in \mathbb{Z}_q^n} C_f(\mathbf{a}) \overline{C_g(\mathbf{b})} \xi^{\langle -\mathbf{a} + \mathbf{b}, \mathbf{u} \rangle + \langle \mathbf{b}, \mathbf{v} \rangle} \\
&= \frac{1}{q^{2n}} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} \sum_{\mathbf{b} \in \mathbb{Z}_q^n} C_f(\mathbf{a}) \overline{C_g(\mathbf{b})} \xi^{\langle \mathbf{b}, \mathbf{v} \rangle} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \xi^{\langle -\mathbf{a} + \mathbf{b}, \mathbf{u} \rangle} \\
&= \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} C_f(\mathbf{a}) \overline{C_g(\mathbf{a})} \xi^{\langle \mathbf{a}, \mathbf{v} \rangle}.
\end{aligned}$$

■

The following corollary is obtained by setting $f = g$, in the above theorem.

Corollary 5.4.5. *Let $f \in \mathcal{B}_{n,q}$. Then for any $\mathbf{v} \in \mathbb{Z}_q^n$, we have*

$$\sum_{\mathbf{u} \in \mathbb{Z}_q^n} | W_f(\mathbf{u}) |^2 | W_f(\mathbf{u} + \mathbf{v}) |^2 = \frac{1}{q^n} \sum_{\mathbf{a} \in \mathbb{Z}_q^n} | C_f(\mathbf{a}) |^2 \xi^{\langle \mathbf{a}, \mathbf{v} \rangle}. \tag{5.4.3}$$

By setting $\mathbf{v} = 0$ in (5.4.2) and using Lemma 5.1.1, we obtain the following corollary.

Corollary 5.4.6. *Let $f, g \in \mathcal{B}_{n,q}$. Then*

$$\sigma_{f,g} = q^n \sum_{\mathbf{u} \in \mathbb{Z}_q^n} | W_f(\mathbf{u}) |^2 | W_g(\mathbf{u}) |^2 . \tag{5.4.4}$$

Further, by putting $f = g$, in the above result, we get

$$\sigma_f = q^n \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mid W_f(\mathbf{u}) \mid^4 . \tag{5.4.5}$$

5.4.1 Crosscorrelation of Maiorana-McFarland type q-ary bent functions

In this section, we obtain crosscorrelation between two bent functions in a subclass of Maiorana-McFarland type q-ary bent functions.

Kumar et al. [87, Theorem 1] have given a natural generalization of the classical Maiorana-McFarland construction. The following lemma is due to Kumar et al. [87].

Lemma 5.4.7. *[87, Theorem 1] Let $n = 2m$, where m is a positive integer. Then a function $f : \mathbb{Z}_q^m \times \mathbb{Z}_q^m \longrightarrow \mathbb{Z}_q$ expressed as*

$$f(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x},\ \pi(\mathbf{y})\rangle +\ g(\mathbf{y}),$$

where $g : \mathbb{Z}_q^m \longrightarrow \mathbb{Z}_q$ is any q-ary function and $\pi : \mathbb{Z}_q^m \longrightarrow \mathbb{Z}_q^m$ is any permutation of elements of $\mathbb{Z}_q^m$, is bent, and the Walsh-Hadamard transform of f at $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m$ is given by

$$\mathcal{W}_f(\mathbf{u}, \mathbf{v}) = \xi^{g(\pi^{-1}(-\mathbf{u}))+\langle \mathbf{v},\ \pi^{-1}(-\mathbf{u})\rangle}.$$

Let $\mathcal{P}$ be the set of all ordered pairs π_1, π_2 of permutations of $\mathbb{Z}_q^m$ such that $\pi_1^{-1} - \pi_2^{-1}$ is also a permutation of $\mathbb{Z}_q^m$. That is

$$\mathcal{P} = \{(\pi_1, \pi_2) :\ \pi_1, \pi_2 \in Sym(\mathbb{Z}_q^m) \text{ and } (\pi_1^{-1} - \pi_2^{-1}) \in Sym(\mathbb{Z}_q^m)\},$$

where $Sym(\mathbb{Z}_q^m)$ is the symmetric group of $\mathbb{Z}_q^m$.

Theorem 5.4.8. *Let $n = 2m$, m a positive integer. Let f_1, f_2 be two q-ary Maiorana-McFarland type generalized bent functions on $\mathbb{Z}_q^n$, i.e., $f_1(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x},\ \pi_1(\mathbf{y})\rangle +\ g_1(\mathbf{y})$ and $f_2(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x},\ \pi_2(\mathbf{y})\rangle +\ g_2(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^m$, where π_1, π_2 are permutations on $\mathbb{Z}_q^m$ and*

$g_1, g_2 \in \mathcal{B}_{m,q}$. *If* $\pi_1, \pi_2 \in \mathcal{P}$, *then*

$$|\mathcal{C}_{f_1,f_2}(\mathbf{u},\mathbf{v})| = q^m, \quad \forall\ (\mathbf{u},\mathbf{v}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m.$$

Proof. By Lemma 5.1.1 and Lemma 5.4.7, we have

$$\begin{aligned}
\mathcal{C}_{f_1,f_2}(\mathbf{u},\mathbf{v}) &= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^m} \mathcal{W}_{f_1}(\mathbf{x},\mathbf{y})\overline{\mathcal{W}_{f_2}(\mathbf{x},\mathbf{y})}\xi^{\langle \mathbf{x},\ \mathbf{u}\rangle+\langle \mathbf{y},\ \mathbf{v}\rangle} \\
&= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^m} (\xi^{g_1(\pi_1^{-1}(-\mathbf{x}))+\langle \mathbf{y},\ \pi_1^{-1}(-\mathbf{x})\rangle})\overline{(\xi^{g_2(\pi_2^{-1}(-\mathbf{x}))+\langle \mathbf{y},\ \pi_2^{-1}(-\mathbf{x})\rangle})}\xi^{\langle \mathbf{x},\ \mathbf{u}\rangle+\langle \mathbf{y},\ \mathbf{v}\rangle} \\
&= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^m} \xi^{g_1(\pi_1^{-1}(-\mathbf{x}))+\langle \mathbf{y},\ \pi_1^{-1}(-\mathbf{x})\rangle-g_2(\pi_2^{-1}(-\mathbf{x}))-\langle \mathbf{y},\ \pi_2^{-1}(-\mathbf{x})\rangle+\langle \mathbf{x},\ \mathbf{u}\rangle+\langle \mathbf{y},\ \mathbf{v}\rangle} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{g_1(\pi_1^{-1}(-\mathbf{x}))-g_2(\pi_2^{-1}(-\mathbf{x}))+\langle \mathbf{x},\ \mathbf{u}\rangle} \sum_{\mathbf{y}\in\mathbb{Z}_q^m} \xi^{\langle \mathbf{y},\ \mathbf{v}+\pi_1^{-1}(-\mathbf{x})-\pi_2^{-1}(-\mathbf{x})\rangle} \\
&= q^m \xi^{g_1(\pi_1^{-1}(\pi_2^{-1}-\pi_1^{-1})^{-1}(\mathbf{v}))-g_2(\pi_2^{-1}(\pi_2^{-1}-\pi_1^{-1})^{-1}(\mathbf{v}))+\langle \mathbf{u},\ -(\pi_2^{-1}-\pi_1^{-1})^{-1}(\mathbf{v})\rangle}.
\end{aligned}$$

Therefore, $\mathcal{C}_{f_1,f_2}(\mathbf{u},\mathbf{v}) = q^m$. This completes the proof. ∎

It is to be noted that smaller values for $\triangle_{f,g}$ and $\sigma_{f,g}$ correspond to low correlation between f and g. From Theorem 5.4.8, we have $\triangle_{f_1,f_2} = q^m$ and $\sigma_{f_1,f_2} = q^{2n}$. These bounds are much better than the trivial bounds obtained in Theorem 5.4.1 and 5.4.3.

5.4.2 Relationship among crosscorrelation of four q-ary functions

In the Theorem 5.4.9 below, we establish a relationship among crosscorrelation of four arbitrary q-ary functions. The result was proved in a different context in [168].

Theorem 5.4.9. *Let* $f, g, h, k \in \mathcal{B}_{n,q}$. *Then*

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{h,k}(\mathbf{u}+\mathbf{e})} = \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \mathcal{C}_{f,h}(\mathbf{a})\overline{\mathcal{C}_{g,k}(\mathbf{a}+\mathbf{e})}, \quad \forall \mathbf{e} \in \mathbb{Z}_q^n. \tag{5.4.6}$$

Proof. For any $\mathbf{e} \in \mathbb{Z}_q^n$, we have

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{h,k}(\mathbf{u}+\mathbf{e})} = \sum_{\mathbf{u}\in\mathbb{Z}_q^n}\sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})}\overline{\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{h(\mathbf{y})-k(\mathbf{y}+\mathbf{u}+\mathbf{e})}}$$

$$
\begin{aligned}
&= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-h(\mathbf{y})} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{-g(\mathbf{x}+\mathbf{u})+k(\mathbf{y}+\mathbf{u}+\mathbf{e})} \\
&= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-h(\mathbf{y})} \sum_{\lambda\in\mathbb{Z}_q^n} \xi^{-g(\lambda)+k(\mathbf{y}-\mathbf{x}+\lambda+\mathbf{e})} \\
&= \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{y}-\mathbf{a})-h(\mathbf{y})} \sum_{\lambda\in\mathbb{Z}_q^n} \xi^{-g(\lambda)+k(\lambda+\mathbf{a}+\mathbf{e})} \\
&= \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{y})-h(\mathbf{y}+\mathbf{a})} \overline{\mathcal{C}_{g,k}(\mathbf{a}+\mathbf{e})} \\
&= \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \mathcal{C}_{f,h}(\mathbf{a}) \overline{\mathcal{C}_{g,k}(\mathbf{a}+\mathbf{e})}.
\end{aligned}
$$

■

In particular, if we take $f = h$ and $g = k$, then we have the following result.

Corollary 5.4.10. *Let $f, g \in \mathcal{B}_{n,q}$, then*

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u}) \overline{\mathcal{C}_{f,g}(\mathbf{u}+\mathbf{e})} = \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \mathcal{C}_f(\mathbf{a}) \overline{\mathcal{C}_g(\mathbf{a}+\mathbf{e})}.$$

For $\mathbf{e} = \mathbf{0}$, we obtain

$$\sigma_{f,g} = \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \mathcal{C}_f(\mathbf{a}) \overline{\mathcal{C}_g(\mathbf{a})}. \tag{5.4.7}$$

If $g = k$ in (5.4.6), then we get $\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u}) \overline{\mathcal{C}_{h,g}(\mathbf{u}+\mathbf{e})} = \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \mathcal{C}_{f,h}(\mathbf{a}) \overline{\mathcal{C}_g(\mathbf{a}+\mathbf{e})}$. Moreover, if g is q-ary bent function, then we have the following proposition.

Proposition 5.4.11. *Let $f, g, h \in \mathcal{B}_{n,q}$ such that g is a q-ary bent function. Then*

(1) $\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u}) \overline{\mathcal{C}_{h,g}(\mathbf{u}+\mathbf{e})} = q^n \mathcal{C}_{f,h}(-\mathbf{e}) \phi_{\{-\mathbf{e}\}}(\mathbf{a})$, *where* $\phi_{\{\mathbf{v}\}}(\mathbf{u}) = \begin{cases} 1, & \text{if } \mathbf{u} = \mathbf{v}, \\ 0, & \text{otherwise}. \end{cases}$

(2) $\sigma_{f,g} = q^{2n}$.

(3) *If $\mathbf{e} \neq 0$ and $f(\mathbf{x})$ is a q-ary bent function, then* $\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u}) \overline{\mathcal{C}_{h,g}(\mathbf{u}+\mathbf{e})} = 0$.

In the following result, we obtain lower bounds on MI for two q-ary functions one of which is q-ary bent.

Theorem 5.4.12. *Let $f, g \in \mathcal{B}_{n,q}$ such that g is q-ary bent function. Then*

1. $\triangle_{f,g} \geq q^{n/2}$, *and*

2. $\max_{\mathbf{u}\in\mathbb{Z}_q^n\setminus\{\mathbf{0}\}} |\mathcal{C}_{f,g}(\mathbf{u})| \geq \sqrt{\frac{q^{2n}-|\mathcal{C}_{f,g}(0)|^2}{q^n-1}}$.

Proof. (1) We have $\sigma_{f,g} = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\mathbf{u})|^2$. Thus, the absolute value of each $\mathcal{C}_{f,g}(\mathbf{u})$ will be minimum only when they all have equal values. Therefore the minimum value of $\triangle_{f,g}$ is $\sqrt{\sigma_{f,g}/q^n}$. From property (2) of Proposition 5.4.11, we have $\sigma_{f,g} = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\mathbf{u})|^2 = q^{2n}$. Since the sum on the left side has q^n non-negative terms, therefore $\triangle_{f,g} \geq \sqrt{q^{2n}/q^n} = q^{n/2}$.

For (2), since $\sum_{\mathbf{u}\in\mathbb{Z}_q^n\setminus\{0\}} |\mathcal{C}_{f,g}(\mathbf{u})|^2 = q^{2n} - |\mathcal{C}_{f,g}(\mathbf{0})|^2$ and the sum on left side has $q^n - 1$ non-negative terms, therefore $\max_{\mathbf{u}\in\mathbb{Z}_q^n\setminus\{0\}} |\mathcal{C}_{f,g}(\mathbf{u})| \geq \sqrt{\frac{q^{2n}-|\mathcal{C}_{f,g}(0)|^2}{q^n-1}}$. ∎

Corollary 5.4.13. *Let $f, g \in \mathcal{B}_{n,q}$ such that g is a q-ary bent function. If $|\mathcal{C}_{f,g}(0)| < q^{n/2}$, then $\max_{\mathbf{u}\in\mathbb{Z}_q^n\setminus\{0\}} |\mathcal{C}_{f,g}(\mathbf{u})| > q^{n/2}$.*

5.5 Results on quaternary functions

In this section, we discuss some results on q-ary functions for a particular value $q = 4$. These functions are known as 4-*ary functions* or *quaternary functions*.

5.5.1 Characterization of quaternary bent functions in $\mathcal{B}_{n+1,4}$ from the functions in $\mathcal{B}_{n,4}$

Theorem 5.5.1. *Let n be a positive integer. A function $h \in \mathcal{B}_{n+1,4}$ expressed as*

$$h(x_{n+1}, x_n, \ldots, x_1) = (1 + x_{n+1})f(x_n, \ldots, x_1) + x_{n+1}g(x_n, \ldots, x_1),$$

where $f, g \in \mathcal{B}_{n,4}$, is quaternary bent if and only if

(i) $|\sum_{j=0}^{3} \mathcal{W}_{h_j}(\mathbf{u})| = 2$ *for all* $\mathbf{u} \in \mathbb{Z}_4^n$.

(ii) $\frac{\mathcal{W}_{h_0}(\mathbf{u})-\mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u})-\mathcal{W}_{h_3}(\mathbf{u})} = \phi(\mathbf{u})$ *and* $\frac{\mathcal{W}_{h_0}(\mathbf{u})+\mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u})+\mathcal{W}_{h_3}(\mathbf{u})} = \imath\psi(\mathbf{u})$, *where* $\phi(\mathbf{u}), \psi(\mathbf{u}) \in \mathbb{R}$.

(iii) $\sum_{j=0}^{3} |\mathcal{W}_{h_j}(\mathbf{u})|^2 = 4$ *for all* $\mathbf{u} \in \mathbb{Z}_4^n$, *and*

$$\mathcal{W}_{h_0}(\mathbf{u})\overline{\mathcal{W}_{h_2}(\mathbf{u})} + \overline{\mathcal{W}_{h_0}(\mathbf{u})}\mathcal{W}_{h_2}(\mathbf{u}) + \mathcal{W}_{h_1}(\mathbf{u})\overline{\mathcal{W}_{h_3}(\mathbf{u})} + \overline{\mathcal{W}_{h_1}(\mathbf{u})}\mathcal{W}_{h_3}(\mathbf{u}) = 0.$$

Proof. Let us identify $(x_{n+1}, x_n, \ldots, x_1) \in \mathbb{Z}_4^{n+1}$ with $(x_{n+1}, \mathbf{x}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$. Suppose that the function

$$h(x_{n+1}, \mathbf{x}) = (1 + x_{n+1})f(\mathbf{x}) + x_{n+1}g(\mathbf{x})$$

is quaternary bent. The Walsh-Hadamard transform of h at $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$ is

$$\begin{aligned}\mathcal{W}_h(a, \mathbf{u}) &= \frac{1}{4^{\frac{n+1}{2}}} \sum_{(x_{n+1}, \mathbf{x}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n} \imath^{h(x_{n+1}, \mathbf{x}) + a x_{n+1} + \langle \mathbf{u},\ \mathbf{x} \rangle} \\ &= \frac{1}{2^{n+1}} \sum_{j=0}^{3} \sum_{\mathbf{x} \in \mathbb{Z}_4^n} \imath^{h_j(\mathbf{x}) + aj + \langle \mathbf{u},\ \mathbf{x} \rangle} = \frac{1}{2} \sum_{j=0}^{3} \imath^{aj} \mathcal{W}_{h_j}(\mathbf{u}) \\ &= \frac{1}{2}(\mathcal{W}_{h_0}(\mathbf{u}) + \imath^a \mathcal{W}_{h_1}(\mathbf{u}) + (-1)^a \mathcal{W}_{h_2}(\mathbf{u}) + (-\imath)^a \mathcal{W}_{h_3}(\mathbf{u})),\end{aligned} \tag{5.5.1}$$

where $h_j(x_n, ..., x_1) = h(j, x_n, ..., x_1)$ for all $j \in \mathbb{Z}_4$.

Since h is a quaternary bent function, $|\mathcal{W}_h(a, \mathbf{u})| = 1$ for all $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$. This implies that

$$|\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})| = 2. \tag{5.5.2}$$

$$|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u}) + \imath(\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u}))| = 2. \tag{5.5.3}$$

$$|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})| = 2. \tag{5.5.4}$$

$$|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u}) - \imath(\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u}))| = 2. \tag{5.5.5}$$

Let $\frac{\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})} = \alpha(\mathbf{u})$ (say), where $\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u}) \neq 0$. On combining (5.5.2) and (5.5.4), we get $\alpha(\mathbf{u}) = -\overline{\alpha(\mathbf{u})}$, which implies that $\alpha(\mathbf{u})$ is purely imaginary i.e.,

$$\alpha(\mathbf{u}) = \imath\psi(\mathbf{u}), \text{ where } \psi(\mathbf{u}) \in \mathbb{R}. \tag{5.5.6}$$

Similarly, on combining (5.5.3) and (5.5.5), we obtain that

$$\frac{\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})} = \phi(\mathbf{u}), \phi(\mathbf{u}) \in \mathbb{R}. \tag{5.5.7}$$

From (5.5.3) and (5.5.7), we have

$$\begin{aligned} & |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 \, |(\imath + \phi(\mathbf{u}))|^2 = 4 \\ i.e., \quad & |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 \left(1 + \phi(\mathbf{u})^2\right) = 4 \\ i.e., \quad & |\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})|^2 + |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 = 4. \end{aligned} \tag{5.5.8}$$

Similarly, from (5.5.4) and (5.5.6), we get

$$|\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})|^2 + |\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})|^2 = 4. \tag{5.5.9}$$

It follows from (5.5.8) and (5.5.9) that

$$\mathcal{W}_{h_0}(\mathbf{u})\overline{\mathcal{W}_{h_2}(\mathbf{u})} + \overline{\mathcal{W}_{h_0}(\mathbf{u})}\mathcal{W}_{h_2}(\mathbf{u}) + \mathcal{W}_{h_1}(\mathbf{u})\overline{\mathcal{W}_{h_3}(\mathbf{u})} + \overline{\mathcal{W}_{h_1}(\mathbf{u})}\mathcal{W}_{h_3}(\mathbf{u}) = 0, \tag{5.5.10}$$

and

$$\sum_{j=0}^{3} |\mathcal{W}_{h_j}(\mathbf{u})|^2 = 4.$$

Conversely, suppose that the conditions (i), (ii) and (iii) are true. Condition (ii) implies that the terms $\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})$ and $\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})$ (as well as $\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})$ and $\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})$) cannot be zero simultaneously. Suppose $\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u}) = 0$. Then $|\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})| = 2$ (as well as, if $\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u}) = 0$ then $|\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})| = 2$). Now consider the case when $|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})| \, |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})| = 0$ and $|\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})| \, |\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})| = 0$.

Let $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$ be arbitrary. Condition (i) implies that $|\mathcal{W}_h(0, \mathbf{u})| = 1$.

Using conditions (ii) and (iii), we obtain

$$\begin{aligned} 4 \ |\mathcal{W}_h(1, \mathbf{u})|^2 &= |\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u}) + \imath(\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u}))|^2 \\ &= |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 |\phi(\mathbf{u}) + \imath|^2 \\ &= |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 \left(1 + \phi^2(\mathbf{u})\right) \\ &= \left(|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})|^2 + |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2\right) \end{aligned}$$

$$= \sum_{j=1}^{3} |\mathcal{W}_{h_j}(\mathbf{u})|^2 - \Big(\mathcal{W}_{h_0}(\mathbf{u})\overline{\mathcal{W}_{h_2}(\mathbf{u})} + \overline{\mathcal{W}_{h_0}(\mathbf{u})}\mathcal{W}_{h_2}(\mathbf{u})$$
$$+ \mathcal{W}_{h_1}(\mathbf{u})\overline{\mathcal{W}_{h_3}(\mathbf{u})} + \overline{\mathcal{W}_{h_1}(\mathbf{u})}\mathcal{W}_{h_3}(\mathbf{u})\Big)$$
$$= 4,$$

which implies that $|\mathcal{W}_h(1, \mathbf{u})| = 1$.

Similarly for $a = 2, 3$ we have from conditions (ii) and (iii) that $|\mathcal{W}_h(a, \mathbf{u})| = 1$. Therefore, $|\mathcal{W}_h(a, \mathbf{u})| = 1$ for all $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$. ■

5.5.2 Secondary constructions on quaternary balanced functions with five valued WHS

In this section, we construct some balanced quaternary functions with high nonlinearity under the Lee metric.

The *support* of a function $f \in \mathcal{B}_{n,4}$ is defined as $supp(f) = \{u \in \mathbb{Z}_4^n : \ f(u) \neq 0\}$, and the *relative support* of f is defined as $supp_j(f) = \{u \in \mathbb{Z}_4^n : f(u) = j\}$ for all $j \in \mathbb{Z}_4$. We use the notation $\eta_j(f)$ to denote the size of $supp_j(f)$. A function $f \in \mathcal{B}_{n,4}$ is balanced if for all $j \in \mathbb{Z}_4$, $\eta_j(f) = 4^{n-1}$. The Hamming weight $w_H(f)$ of f is the size of its support and the Hamming distance between two functions $f, g \in \mathcal{B}_{n,4}$ is defined by $d_H(f, g) = w_H(f - g)$. The Lee weights of $0, 1, 2, 3$ in $\mathbb{Z}_4$ are $0, 1, 2, 1$ respectively and the Lee weight $w_L(u)$ of an element $u \in \mathbb{Z}_4^n$ is the rational sum of the Lee weights of its components.

The Lee distance between two functions $f, g \in \mathcal{B}_{n,4}$ is defined by $d_L(f, g) = w_L(f - g)$.

Definition 5.5.2. *Let $\mathcal{A}_{n,4}$ be set of all affine functions in $\mathcal{B}_{n,4}$. The nonlinearity of any $f \in \mathcal{B}_{n,4}$ is defined as $nl_4^H(f) = \min_{g \in \mathcal{A}_{n,4}} d_H(f, g)$ under the Hamming metric and $nl_4^L(f) = \min_{g \in \mathcal{A}_{n,4}} d_L(f, g)$ under the Lee metric.*

A function $f \in \mathcal{B}_{n,4}$ is quaternary bent [75] if and only if $|\mathcal{W}_f(\mathbf{u})| = 1$, i.e., $\mathcal{W}_f(\mathbf{u}) \in \{\pm 1, \pm\imath\}$ for all $\mathbf{u} \in \mathbb{Z}_4^n$.

Proposition 5.5.3 and Proposition 5.5.4 given below are due to Jadda and Parraud [75] and stated here in terms of *normalized* Walsh-Hadamard transform.

Proposition 5.5.3. *[75, Proposition 3] The nonlinearity of $f \in \mathcal{B}_{n,4}$ under the Lee metric is given by*

$$\begin{aligned} nl_4^L(f) &= 4^n - 2^n \max_{\mathbf{u}\in\mathbb{Z}_4^n, \beta\in\mathbb{Z}_4} \{Re[\imath^\beta \mathcal{W}_F(\mathbf{u})]\} \\ &= 4^n - 2^n \max_{\mathbf{u}\in\mathbb{Z}_4^n} \{|Re[\mathcal{W}_F(\mathbf{u})]|, |Im[\mathcal{W}_F(\mathbf{u})]|\}, \end{aligned}$$

where $Re[z]$ and $Im[z]$ respectively denote the real and imaginary part of a complex number z.

Proposition 5.5.4. *[75, Theorem 2] Let f be an n variables quaternary bent function. Then*

$$nl_4^L(f) = 4^n - 2^n.$$

In the following result, we present a construction of balanced quaternary function with high $\mathbb{Z}_4$-nonlinearity under the Lee metric by using quaternary bent function.

Theorem 5.5.5. *Suppose $g \in \mathcal{B}_{n+1,4}$ is expressed as*

$$g(x_{n+1}, x_n, \ldots, x_1) = x_{n+1} + f(x_n, \ldots, x_1),$$

where $f \in \mathcal{B}_{n,4}$ is a quaternary bent function. Then g is balanced and its nonlinearity under the Lee metric is given by

$$nl_4^L(g) = 4^{n+1} - 2^{n+2}.$$

Proof. Let $\mathbf{x} = (x_n, \ldots, x_1) \in \mathbb{Z}_4^n$ and $j \in \mathbb{Z}_4$.

$$\begin{aligned} supp_j(g) &= \{\mathbf{x}' = (x_{n+1}, \mathbf{x}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n \ : \ g(\mathbf{x}') = j\} \\ &= \{\mathbf{x} \in \mathbb{Z}_4^n, x_{n+1} \in \mathbb{Z}_4 \ : \ f(\mathbf{x}) + x_{n+1} = j\} \\ &= \cup_{l=0}^3 \{\mathbf{x} \in \mathbb{Z}_4^n \ : \ f(\mathbf{x}) = l = (j - x_{n+1}) \mod 4\} = \cup_{l=0}^3 supp_l(f). \end{aligned}$$

Recall that $\eta_j(f) = |\{\mathbf{x} \in \mathbb{Z}_4^n : \ f(\mathbf{x}) = j\}|$ for all $j \in \mathbb{Z}_4$, which implies that $\eta_j(g) = |\cup_{l=0}^3 supp_l(f)| = \sum_{l=0}^3 \eta_l(f) = 4^n$ for all $j \in \mathbb{Z}_4$. Hence g is balanced.

The Walsh-Hadamard transform of g at $(u_{n+1}, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$ is

$$\begin{aligned}
\mathcal{W}_g(u_{n+1}, \mathbf{u}) &= \frac{1}{2^{n+1}} \sum_{(x_{n+1}, \mathbf{x}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n} \imath^{g(x_{n+1}, \mathbf{x}) + \langle \mathbf{u}, \mathbf{x} \rangle + u_{n+1} x_{n+1}} \\
&= \frac{1}{2^{n+1}} \sum_{(x_{n+1}, \mathbf{x}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n} \imath^{f(\mathbf{x}) + \langle \mathbf{u}, \mathbf{x} \rangle + (u_{n+1}+1) x_{n+1}} \\
&= \frac{1}{2^{n+1}} \sum_{\mathbf{x} \in \mathbb{Z}_4^n} \imath^{f(\mathbf{x}) + \langle \mathbf{u}, \mathbf{x} \rangle} \sum_{x_{n+1} \in \mathbb{Z}_4} \imath^{(u_{n+1}+1) x_{n+1}} \\
&= \begin{cases} 2\ \mathcal{W}_f(\mathbf{u}), & \text{if } u_{n+1} = 3, \\ 0, & \text{otherwise .} \end{cases}
\end{aligned} \tag{5.5.11}$$

Since f is a quaternary bent function, therefore $\mathcal{W}_f(\mathbf{u}) \in \{\pm 1, \pm \imath\}$ for every $\mathbf{u} \in \mathbb{Z}_4^n$. Using (5.5.11), we obtain

$$\mathcal{W}_g(u_{n+1}, \mathbf{u}) = \begin{cases} \pm 2 \text{ or } \pm 2\imath, & \text{if } u_{n+1} = 3, \\ 0, & \text{otherwise .} \end{cases}$$

Thus the Walsh-Hadamard spectrum of g contains 5 distinct values from the set $\{\pm 2, \pm 2\imath, 0\}$ for every $(u_{n+1}, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$. By Proposition 5.5.3, we obtain

$$\begin{aligned}
nl_4^L(g) &= 4^{n+1} - 2^{n+1} \max_{(u_{n+1}, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n} \{|Re[\mathcal{W}_g(u_{n+1}, \mathbf{u})]|, |Im[\mathcal{W}_g(u_{n+1}, \mathbf{u})]|\} \\
&= 4^{n+1} - 2^{n+2}.
\end{aligned}$$

■

Remark 5.5.6. *A function $g \in \mathcal{B}_{n+1,4}$ expressed as*

$$g(x_{n+1}, x_n, \ldots, x_1) = x_{n+1} + f(x_n, \ldots, x_1),$$

where $f \in \mathcal{B}_{n,4}$, is balanced and its nonlinearity under the Lee metric is

$$nl_4^L(g) = 4\ nl_4^L(f).$$

Proof. The proof is a direct consequence of Lemma 5.1.1 and Proposition 5.5.3. ■

Chapter 6

Constructions of balanced q-ary functions with good GAC

6.1 Introduction

In designing a cryptographic system, we need functions which satisfy some design criteria such as balancedness, high nonlinearity, low autocorrelation, low crosscorrelation, PC and good GAC. In the construction of cryptographically significant functions, the most common problem is to fulfill the requirement of a number of criteria including those mentioned above. Some of the cryptographic criteria are at conflict with each other. The most suitable example is perhaps the bent functions, they possess maximum possible nonlinearity and satisfy avalanche criteria with respect to each non-zero element. But being not balanced, not correlation immune, and non existent in case of odd number of variables, they are not proper for direct use in cryptographic systems. Therefore, from the cryptographic point of view, there is a need to construct balanced functions with good GAC and satisfying PC.

In Chapter 5, we introduced the indicators, the sum-of-squares-of-modulus indicator (SSMI) and the modulus indicator (MI), and derived some upper and lower bounds on these indicators. The present chapter is devoted to the construction of q-ary functions with good GAC measured in terms of the indicators, the SSMI and the MI, and satisfying PC. The two indicators, the SSMI and the MI are directly linked with the crosscorrelation (or with the

autocorrelation) of the functions. The lower value of these indicators for the cryptographic functions correspond to low correlation between them. It can be noted that for $q = 2$ the indicators, the SSMI and the MI coincide with the indicators, the sum-of-squares indicator and the absolute indicator, respectively introduced by Zhang and Zheng [162] in the Boolean context. During last few years, it became the topic of great interest to construct balanced Boolean functions with low values of these indicators, and to deduce lower and upper bounds for these indicators. For more study regarding the construction of functions with good GAC in the Boolean context we refer to [143, 148, 162, 165–168].

It is well known that balanced functions are suitable candidate for various cryptographic applications. In the present chapter, we construct two classes of q-ary functions in $2m$-variables and in $(2m + 1)$-variables, which satisfy some important cryptographic criteria. The constructed functions have good global avalanche characteristics measured in terms of the indicators, the SSMI and the MI. A remarkable property of the constructed functions is that they are balanced and satisfy PC. Also, we derive upper bounds on SSMI, MI and PC by characterizing their autocorrelation spectrum. We show that the SSMI, MI and PC of q-ary functions are invariant under the affine transformations. Further, we give a construction of q-ary s-plateaued functions and obtain their SSMI. We present a relationship between the autocorrelation spectrum of a cubic Boolean function and the dimension of the kernel of the bilinear form associated with the derivative of the function. Using this result, we identify several classes of cubic semi-bent Boolean functions which have good bounds on their SSMI and MI, and hence show good behavior with respect to the GAC.

6.2 Constructions of q-ary balanced functions with good GAC

In this section, we present construction of two classes of cryptographic functions in $2m$-variables and in $(2m + 1)$-variables, which satisfy some desired cryptographic criteria. The constructed functions have good global avalanche characteristics measured in terms of the indicators the SSMI and the MI. A remarkable property of the constructed functions is that

they are balanced and satisfy PC.

6.2.1 Functions on $\mathbb{Z}_q^{2m}$

First we present construction of balanced q-ary functions in even ($n = 2m$) number of variables and discuss several cryptographic criteria for these functions by computing their WHS and autocorrelation spectrum.

Construction 1: Let $n = 2m$, m a positive integer. Let π be a permutation on $\mathbb{Z}_q^m \setminus \{\mathbf{0}\}$. Define a function $f : \mathbb{Z}_q^m \times \mathbb{Z}_q^m \to \mathbb{Z}_q$ such that

$$f(\mathbf{x}, \mathbf{y}) = \begin{cases} \langle \mathbf{a}, \mathbf{x} \rangle, & \text{if } \mathbf{y} = \mathbf{0}, \\ \langle \pi(\mathbf{y}), \mathbf{x} \rangle, & \text{if } \mathbf{y} \neq \mathbf{0}, \end{cases} \tag{6.2.1}$$

where $\mathbf{a} \in \mathbb{Z}_q^m$ is a non-zero fixed vector.

Theorem 6.2.1. *The q-ary function f as constructed in* (6.2.1) *is balanced, and*

(a) *the autocorrelation spectrum of f is given by*

$$\mathcal{C}_f(\mathbf{u}, \mathbf{v}) = \begin{cases} q^m \left(\xi^{-\langle \mathbf{a}, \mathbf{u} \rangle} - 1 \right), & \text{if } \mathbf{v} = \mathbf{0} \\ q^m \left(\xi^{-\langle \pi(\mathbf{v}), \mathbf{u} \rangle} \delta_{\mathbf{0}}(\mathbf{a} - \pi(\mathbf{v})) + \xi^{-\langle \mathbf{a}, \mathbf{u} \rangle} \delta_{\mathbf{0}}(\pi(-\mathbf{v}) - \mathbf{a}) \right), & \text{if } \mathbf{v} \neq \mathbf{0}. \end{cases}$$

(b) *the MI of f is $\triangle_f \leq 2q^m$.*

(c) *f satisfies PC with respect to at least $q^{2m} - 3q^m + q^{m-1} - 1$ non-zero vectors in $\mathbb{Z}_q^n$.*

(d) *the SSMI of f is $\sigma_f \leq q^{4m} + 8q^{3m} - 4q^{3m-1}$ if q is even and $(q/2, q/2, \ldots, q/2) = \pi^{-1}(\mathbf{a})$ for some $\mathbf{a} \neq \mathbf{0}$. Otherwise, $\sigma_f \leq q^{4m} + 6q^{3m} - 4q^{3m-1}$.*

(e) *the WHS of f is $\{0, 1 + \xi^{\langle \mathbf{v}, \pi^{-1}(\mathbf{a}) \rangle} : \mathbf{v} \in \mathbb{Z}_q^m\} \bigcup \{\xi^{\langle \mathbf{v}, \pi^{-1}(-\mathbf{u}) \rangle} : \mathbf{u}, \mathbf{v} \in \mathbb{Z}_q^m$ and $\mathbf{u} \neq \mathbf{0}, -\mathbf{a}\}$, and so, $|\mathcal{W}_f(\mathbf{u}, \mathbf{v})| \leq 2$ for all $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m$.*

Proof. We have $supp_j(f) = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m : f(\mathbf{x}, \mathbf{y}) = j\} = \{\mathbf{x} \in \mathbb{Z}_q^m : \langle \mathbf{a}, \mathbf{x} \rangle = j\} \bigcup_{\mathbf{y}_0 \in \mathbb{Z}_q^m \setminus \{\mathbf{0}\}} \{\mathbf{x} \in \mathbb{Z}_q^m : \langle \pi(\mathbf{y}_0), \mathbf{x} \rangle = j\}$. Also, for any $\mathbf{u} \neq \mathbf{0}$, $\langle \mathbf{u}, \mathbf{x} \rangle$ is a non-zero linear function and hence balanced. Therefore, for any $j \in \mathbb{Z}_q$, the cardinality of $supp_j(f)$ is $q^{m-1} + (q^m - 1)q^{m-1} = q^{n-1}$, which implies that the function f is balanced.

(a) The autocorrelation of f at $(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m \setminus \{(\mathbf{0},\mathbf{0})\}$ is

$$\mathcal{C}_f(\mathbf{u},\mathbf{v}) = \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \sum_{\mathbf{y}\in\mathbb{Z}_q^m} \xi^{f(\mathbf{x},\mathbf{y})-f(\mathbf{x}+\mathbf{u},\mathbf{y}+\mathbf{v})}. \tag{6.2.2}$$

We consider the following two cases:

Case 1. If $\mathbf{v} = \mathbf{0}$, then by (6.2.2), the autocorrelation of f at $(\mathbf{u},\mathbf{0})$, $\mathbf{u} \neq \mathbf{0}$, is

$$\begin{aligned}
\mathcal{C}_f(\mathbf{u},\mathbf{0}) &= \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{f(\mathbf{x},\mathbf{0})-f(\mathbf{x}+\mathbf{u},\mathbf{0})} + \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \sum_{\mathbf{y}\neq\mathbf{0}} \xi^{f(\mathbf{x},\mathbf{y})-f(\mathbf{x}+\mathbf{u},\mathbf{y})} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{-\langle \mathbf{a},\mathbf{u}\rangle} + \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \sum_{\mathbf{y}\neq\mathbf{0}} \xi^{-\langle \pi(\mathbf{y}),\mathbf{u}\rangle} \\
&= q^m \xi^{-\langle \mathbf{a},\mathbf{u}\rangle} + \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \sum_{\mathbf{z}\neq\mathbf{0}} \xi^{-\langle \mathbf{z},\mathbf{u}\rangle} \\
&= q^m \xi^{-\langle \mathbf{a},\mathbf{u}\rangle} + \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \left(\sum_{\mathbf{z}\in\mathbb{Z}_q^m} \xi^{-\langle \mathbf{z},\mathbf{u}\rangle} - 1 \right) \\
&= q^m \xi^{-\langle \mathbf{a},\mathbf{u}\rangle} + \sum_{\mathbf{x}\in\mathbb{Z}_q^m} (q^m \delta_{\mathbf{0}}(\mathbf{u}) - 1) \\
&= q^m \left(\xi^{-\langle \mathbf{a},\mathbf{u}\rangle} - 1 \right).
\end{aligned} \tag{6.2.3}$$

Case 2. If $\mathbf{v} \neq \mathbf{0}$, then since π is a permutation, therefore, $\pi(\mathbf{y}) - \pi(\mathbf{y}+\mathbf{v}) \neq \mathbf{0}$ for all $\mathbf{y} \in \mathbb{Z}_q^m$. By (6.2.2), the autocorrelation of f at $(\mathbf{u},\mathbf{v})$ is

$$\begin{aligned}
\mathcal{C}_f(\mathbf{u},\mathbf{v}) &= \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \sum_{\mathbf{y}\in\mathbb{Z}_q^m\setminus\{\mathbf{0},-\mathbf{v}\}} \xi^{f(\mathbf{x},\mathbf{y})-f(\mathbf{x}+\mathbf{u},\mathbf{y}+\mathbf{v})} + \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{f(\mathbf{x},\mathbf{0})-f(\mathbf{x}+\mathbf{u},\mathbf{v})} + \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{f(\mathbf{x},-\mathbf{v})-f(\mathbf{x}+\mathbf{u},\mathbf{0})} \\
&= \sum_{\mathbf{y}\in\mathbb{Z}_q^m\setminus\{\mathbf{0},-\mathbf{v}\}} \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{\langle \pi(\mathbf{y}),\mathbf{x}\rangle-\langle \pi(\mathbf{y}+\mathbf{v}),\mathbf{x}+\mathbf{u}\rangle} + \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{\langle \mathbf{a},\mathbf{x}\rangle-\langle \pi(\mathbf{v}),\mathbf{x}+\mathbf{u}\rangle} \\
&\quad + \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{\langle \pi(-\mathbf{v}),\mathbf{x}\rangle-\langle \mathbf{a},\mathbf{x}+\mathbf{u}\rangle} \\
&= \sum_{\mathbf{y}\in\mathbb{Z}_q^m\setminus\{\mathbf{0},-\mathbf{v}\}} \xi^{-\langle \pi(\mathbf{y}+\mathbf{v}),\mathbf{u}\rangle} \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{\langle \pi(\mathbf{y})-\pi(\mathbf{y}+\mathbf{v}),\mathbf{x}\rangle} + \xi^{-\langle \pi(\mathbf{v}),\mathbf{u}\rangle} \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{\langle \mathbf{a}-\pi(\mathbf{v}),\mathbf{x}\rangle} \\
&\quad + \xi^{-\langle \mathbf{a},\mathbf{u}\rangle} \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{\langle \pi(-\mathbf{v})-\mathbf{a},\mathbf{x}\rangle}
\end{aligned}$$

$$\begin{aligned}
&= q^m \sum_{\mathbf{y}\in\mathbb{Z}_q^m\setminus\{\mathbf{0},-\mathbf{v}\}} \xi^{-\langle\pi(\mathbf{y}+\mathbf{v}),\mathbf{u}\rangle}\delta_{\mathbf{0}}(\pi(\mathbf{y})-\pi(\mathbf{y}+\mathbf{v})) + \xi^{-\langle\pi(\mathbf{v}),\mathbf{u}\rangle}q^m\delta_{\mathbf{0}}(\mathbf{a}-\pi(\mathbf{v})) \\
&+ q^m\xi^{-\langle\mathbf{a},\mathbf{u}\rangle}\delta_{\mathbf{0}}(\pi(-\mathbf{v})-\mathbf{a}) \\
&= q^m\xi^{-\langle\pi(\mathbf{v}),\mathbf{u}\rangle}\delta_{\mathbf{0}}(\mathbf{a}-\pi(\mathbf{v})) + q^m\xi^{-\langle\mathbf{a},\mathbf{u}\rangle}\delta_{\mathbf{0}}(\pi(-\mathbf{v})-\mathbf{a}).
\end{aligned} \tag{6.2.4}$$

(b) From (a), it follows that the autocorrelation of f is $|\mathcal{C}_f(\mathbf{u},\mathbf{v})| \le 2q^m$ for all non-zero vectors $(\mathbf{u},\mathbf{v})$ of $\mathbb{Z}_q^m \times \mathbb{Z}_q^m$, which implies that the MI of f is $\triangle_f \le 2q^m$.

(c) Since the function $\langle\mathbf{a},\mathbf{u}\rangle$ is balanced for any $\mathbf{a}\neq\mathbf{0}$, by (6.2.3), the number of vectors $(\mathbf{u},\mathbf{0}) \neq (\mathbf{0},\mathbf{0})$ for which $\mathcal{C}_f(\mathbf{u},\mathbf{0}) = 0$ (or equivalently, $\langle\mathbf{a},\mathbf{u}\rangle = 0$) are $q^{m-1}-1$. Next, if $\mathbf{v}\neq\mathbf{0}$, then by (6.2.4), $\mathcal{C}_f(\mathbf{u},\mathbf{v}) = 0$ if $\mathbf{v} \neq \pm\,\pi^{-1}(\mathbf{a})$. Since π is a permutation, therefore, in this case the number of vectors $(\mathbf{u},\mathbf{v})$ for which $\mathcal{C}_f(\mathbf{u},\mathbf{v}) = 0$ is $q^m(q^m-3)$. Thus, the number of vectors $(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m$ for which $\mathcal{C}_f(\mathbf{u},\mathbf{v}) = 0$ is $q^{2m} - 3q^m + q^{m-1} - 1$.

The condition $\mathbf{v} = -\mathbf{v} = (v_m,\ldots,v_1)$ holds if q is even and $v_i = \frac{q}{2}$ for all i. Now if $\mathbf{v} = (q/2,\ldots,q/2) = \pi^{-1}(\mathbf{a})$ for some $\mathbf{a}\neq\mathbf{0}$, then by (6.2.4), we have $|\mathcal{C}_f(\mathbf{u},\mathbf{v})| = 2q^m$. Therefore, in this case the function f as constructed in (6.2.1) satisfies PC with respect to $q^{2m} - 2q^m + q^{m-1} - 1$ vectors in $\mathbb{Z}_q^n$, and $\triangle_f = 2q^m$.

(d) If q is even and $(q/2, q/2, \ldots, q/2) = \pi^{-1}(\mathbf{a})$, then $\pi^{-1}(\mathbf{a}) = -\pi^{-1}(\mathbf{a})$. Then for the SSMI of f we have

$$\begin{aligned}
\sigma_f &= \sum_{(\mathbf{u},\mathbf{v})\in\mathbb{Z}_q^m\times\mathbb{Z}_q^m} |\mathcal{C}_f(\mathbf{u},\mathbf{v})|^2 \\
&= |\mathcal{C}_f(\mathbf{0},\mathbf{0})|^2 + \sum_{\mathbf{u}\in\mathbb{Z}_q^m\setminus\{\mathbf{0}\}} |\mathcal{C}_f(\mathbf{u},\mathbf{0})|^2 + \sum_{(\mathbf{u},\mathbf{v})\in\mathbb{Z}_q^m\times\mathbb{Z}_q^m,\mathbf{v}\neq\mathbf{0}} |\mathcal{C}_f(\mathbf{u},\mathbf{v})|^2 \\
&\le q^{2n} + (q^m - q^{m-1})(2q^m)^2 + q^m(2q^m)^2 \\
&= q^{4m} + 8q^{3m} - 4q^{3m-1}.
\end{aligned}$$

In the other cases, there exist two distinct vectors $\mathbf{v}_1 = \pi^{-1}(\mathbf{a})$, $\mathbf{v}_2 = -\pi^{-1}(\mathbf{a})$. So, by (6.2.4), we have $|\mathcal{C}_f(\mathbf{u},\mathbf{v}_i)| = q^m$ $(i = 1, 2)$. Therefore, it follows from (6.2.3) and (6.2.4) that the SSMI of f will be

$$\sigma_f = |\mathcal{C}_f(\mathbf{0},\mathbf{0})|^2 + \sum_{\mathbf{u}\in\mathbb{Z}_q^m\setminus\{\mathbf{0}\}} |\mathcal{C}_f(\mathbf{u},\mathbf{0})|^2 + \sum_{(\mathbf{u},\mathbf{v})\in\mathbb{Z}_q^m\times\mathbb{Z}_q^m,\mathbf{v}\neq\mathbf{0}} |\mathcal{C}_f(\mathbf{u},\mathbf{v})|^2$$

$$\leq q^{2n} + (q^m - q^{m-1})(2q^m)^2 + 2q^m(q^m)^2$$
$$= q^{4m} + 6q^{3m} - 4q^{3m-1}.$$

(e) The WHT of f at $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m$ is given by

$$\mathcal{W}_f(\mathbf{u}, \mathbf{v}) = \frac{1}{q^m} \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \xi^{\langle (\mathbf{a}+\mathbf{u}), \mathbf{x} \rangle} + \frac{1}{q^m} \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \sum_{\mathbf{y} \in \mathbb{Z}_q^m \setminus \{\mathbf{0}\}} \xi^{\langle (\pi(\mathbf{y})+\mathbf{u}), \mathbf{x} \rangle + \langle \mathbf{v}, \mathbf{y} \rangle}$$
$$= \delta_{\mathbf{0}}(\mathbf{a}+\mathbf{u}) + \frac{1}{q^m} \sum_{\mathbf{y} \in \mathbb{Z}_q^m \setminus \{\mathbf{0}\}} \xi^{\langle \mathbf{v}, \mathbf{y} \rangle} \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \xi^{\langle (\pi(\mathbf{y})+\mathbf{u}), \mathbf{x} \rangle}$$
$$= \begin{cases} 0, & \text{if } \mathbf{u} = \mathbf{0} \\ \delta_{\mathbf{0}}(\mathbf{a}+\mathbf{u}) + \xi^{\langle \mathbf{v}, \pi^{-1}(-\mathbf{u}) \rangle}, & \text{if } \mathbf{u} \neq \mathbf{0}. \end{cases}$$

Therefore, the WHS of the constructed function f is

$\mathcal{W}_f(\mathbf{u}, \mathbf{v}) \in \{0, 1 + \xi^{\langle \mathbf{v}, \pi^{-1}(\mathbf{a}) \rangle} : \mathbf{v} \in \mathbb{Z}_q^m\} \cup \{\xi^{\langle \mathbf{v}, \pi^{-1}(-\mathbf{u}) \rangle} : \mathbf{u}, \mathbf{v} \in \mathbb{Z}_q^m, \mathbf{u} \neq \mathbf{0}, -\mathbf{a}\}$.

This completes the proof. ∎

6.2.2 Functions on $\mathbb{Z}_q^{2m+1}$

Now, we present construction of balanced q-ary functions on an odd ($n = 2m + 1$) number of variables and analyze several properties of these functions in terms their WHS and autocorrelation spectrum.

Construction 2: Let $n = t + 1$, where t is a positive integer, and $f \in \mathcal{B}_{t,q}$. Let $h \in \mathcal{B}_{n,q}$ be such that

$$h(\mathbf{x}, x_n) = x_n + f(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{Z}_q^t, \ x_n \in \mathbb{Z}_q. \tag{6.2.5}$$

It is proved in Theorem 5.5.5 that the function h as constructed in (6.2.5) is balanced for $q = 4$. The result can easily be generalized to show that h is balanced for arbitrary $q \geq 2$. It is to be noted that if f is a q-ary bent function, then the function h is q-ary semi-bent. In the following result, we construct q-ary balanced functions on an odd number of variables with good GAC.

Lemma 6.2.2. *Let $h \in \mathcal{B}_{n,q}$ be a q-ary function as constructed in* (6.2.5). *Then h is*

balanced, and for any $(\mathbf{u}, u_n) \in \mathbb{Z}_q^t \times \mathbb{Z}_q$*, the autocorrelation and the WHT of* h *are*

$$\mathcal{C}_h(\mathbf{u}, u_n) = q\xi^{-u_n}\mathcal{C}_f(\mathbf{u}), \text{ and } \mathcal{W}_h(\mathbf{u}, u_n) = \sqrt{q}\mathcal{W}_f(\mathbf{u})\delta_0(1+u_n),$$

respectively.

Proof. The proof directly follows from the definitions of the autocorrelation and the WHT of h. ∎

Theorem 6.2.3. *Let* h *be as constructed in* (6.2.5) *and the function* f *therein be as constructed in* (6.2.1) *(i.e.,* $t = 2m$*), then*

(*a*) *the autocorrelation spectrum of* h *is given by*

$$\mathcal{C}_h(\mathbf{u}, \mathbf{v}, u_n) = \begin{cases} q^n, & \text{if } (\mathbf{u}, \mathbf{v}, u_n) = (\mathbf{0}, \mathbf{0}, 0), \\ q^{m+1}\left(\xi^{-\langle \mathbf{a}, \mathbf{u}\rangle} - 1\right)\xi^{u_n}, & \text{if } \mathbf{u} \in \mathbb{Z}_q^m \setminus \{\mathbf{0}\}, \mathbf{v} = \mathbf{0}, \\ q^{m+1}\Big(\xi^{u_n - \langle \pi(\mathbf{v}), \mathbf{u}\rangle}\delta_{\mathbf{0}}(\mathbf{a} - \pi(\mathbf{v})) & \\ \qquad + \xi^{u_n - \langle \mathbf{a}, \mathbf{u}\rangle}\delta_{\mathbf{0}}(\pi(-\mathbf{v}) - \mathbf{a})\Big), & \text{otherwise.} \end{cases} \tag{6.2.6}$$

(*b*) h *satisfy PC with respect to* $q^{2m+1} - 2q^{m+1} + q^m - q$ *non-zero vectors in* $\mathbb{Z}_q^{2m+1}$ *if* q *is even and* $(q/2, q/2, \ldots, q/2) = \pi^{-1}(\mathbf{a})$*, and otherwise with respect to* $q^{2m+1} - 3q^{m+1} + q^m - q$ *non-zero vectors in* $\mathbb{Z}_q^{2m+1}$.

(*c*) *the MI of* h *is given as* $\triangle_h = 2q^{m+1}$ *if* q *is even and* $(q/2, q/2, \ldots, q/2) = \pi^{-1}(\mathbf{a})$. *Otherwise* $\triangle_h \leq 2q^{m+1}$.

(*d*) *the SSMI of* h *is given as* $\sigma_h \leq q^{4m+3} + 8q^{3m+3} - 4q^{3m+2}$ *if* q *is even and* $(q/2, q/2, \ldots, q/2) = \pi^{-1}(\mathbf{a})$. *Otherwise* $\sigma_h \leq q^{4m+3} + 6q^{3m+3} - 4q^{3m+2}$.

(*e*) *the WHS of* h *satisfies* $|\mathcal{W}_h(\mathbf{u}, \mathbf{v}, u_n)| \leq 2\sqrt{q}$ *for all* $(\mathbf{u}, \mathbf{v}, u_n) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m \times \mathbb{Z}_q$.

Proof. Parts (*a*), (*b*), (*c*) and (*e*) follow from Theorem 6.2.1 and Lemma 6.2.2.

(d) If q is even and $(q/2, q/2, \ldots, q/2) = \pi^{-1}(\mathbf{a})$, then $\pi^{-1}(\mathbf{a}) = -\pi^{-1}(\mathbf{a})$. Therefore, it follows from (6.2.6) that the SSMI of h is given by

$$\begin{aligned}
\sigma_h &= \sum_{(\mathbf{u},\mathbf{v},u_n)\in\mathbb{Z}_q^m\times\mathbb{Z}_q^m\times\mathbb{Z}_q} |\mathcal{C}_h(\mathbf{u},\mathbf{v},u_n)|^2 \\
&= \sum_{u_n\in\mathbb{Z}_q} |\mathcal{C}_h(\mathbf{0},\mathbf{0},u_n)|^2 + \sum_{\mathbf{u}\in\mathbb{Z}_q^m\setminus\{\mathbf{0}\},u_n\in\mathbb{Z}_q} |\mathcal{C}_h(\mathbf{u},\mathbf{0},u_n)|^2 + \sum_{\mathbf{u}\in\mathbb{Z}_q^m,u_n\in\mathbb{Z}_q,\mathbf{v}\neq\mathbf{0}} |\mathcal{C}_h(\mathbf{u},\mathbf{v},u_n)|^2 \\
&\leq q(q^{2m+1})^2 + q(q^m - q^{m-1})(2q^{m+1})^2 + q^{m+1}(2q^{m+1})^2 \\
&= q^{4m+3} + 8q^{3m+3} - 4q^{3m+2}.
\end{aligned}$$

In the other cases, there exist two distinct vectors $\mathbf{v}_1 = \pi^{-1}(\mathbf{a})$, $\mathbf{v}_2 = -\pi^{-1}(\mathbf{a})$, and so, by (6.2.6), it follows that the autocorrelation of h is $|\mathcal{C}_h(\mathbf{u},\mathbf{v}_i,u_n)| = q^{m+1}$, for $i = 1, 2$. Thus, $\sum_{\mathbf{u}\in\mathbb{Z}_q^m,u_n\in\mathbb{Z}_q,\mathbf{v}\neq\mathbf{0}} |\mathcal{C}_h(\mathbf{u},\mathbf{v},u_n)|^2 = 2q^{m+1}(q^{m+1})^2$.

Therefore, the SSMI of h is given by

$$\begin{aligned}
\sigma_h &= \sum_{u_n\in\mathbb{Z}_q} |\mathcal{C}_h(\mathbf{0},\mathbf{0},u_n)|^2 + \sum_{\mathbf{u}\in\mathbb{Z}_q^m\setminus\{\mathbf{0}\},u_n\in\mathbb{Z}_q} |\mathcal{C}_h(\mathbf{u},\mathbf{0},u_n)|^2 + \sum_{\mathbf{u}\in\mathbb{Z}_q^m,u_n\in\mathbb{Z}_q,\mathbf{v}\neq\mathbf{0}} |\mathcal{C}_h(\mathbf{u},\mathbf{v},u_n)|^2 \\
&\leq q(q^{2m+1})^2 + q(q^m - q^{m-1})(2q^{m+1})^2 + 2q^{m+1}(q^{m+1})^2 \\
&= q^{4m+3} + 6q^{3m+3} - 4q^{3m+2}.
\end{aligned}$$

This completes the proof. ∎

Similar to Theorem 5.4.1 and Theorem 5.4.3, it can be shown that $0 \leq \triangle_f \leq q^n$ and $q^{2n} \leq \sigma_f \leq q^{3n}$ for any $f \in \mathcal{B}_{n,q}$. Thus, the bounds obtained in Theorem 6.2.1 and Theorem 6.2.3 are much better than the trivial bounds, and hence the functions so constructed have good GACs.

In Theorem 6.2.4 below, it is shown that the cryptographic criteria SSMI, MI and PC of q-ary functions are invariant under the affine transformations:

$$g(\mathbf{x}) = f(\mathbf{x}A + \mathbf{a}) \ + \langle \mathbf{b}, \mathbf{x}\rangle + \ d, \quad \text{for all} \ \ \mathbf{x} \in \mathbb{Z}_q^n, \tag{6.2.7}$$

where $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_q^n$, $d \in \mathbb{Z}_q$ and $A \in GL(n, \mathbb{Z}_q)$.

Theorem 6.2.4. *Let $g, f \in \mathcal{B}_{n,q}$ as defined in* (6.2.7)*, then*

(*a*) $\sigma_{g_1,g_2} = \sigma_{f_1,f_2}$ *and* $\triangle_{g_1,g_2} = \triangle_{f_1,f_2}$. *In particular,* $\sigma_g = \sigma_f$ *and* $\triangle_g = \triangle_f$.

(*b*) *Both* f *and* g *satisfy PC for an equal number of non-zero vectors in* $\mathbb{Z}_q^n$.

Proof. (*a*) The crosscorrelation between $g_1(\mathbf{x}) = f_1(\mathbf{x}A + \mathbf{a}) + \langle \mathbf{b}, \mathbf{x} \rangle + d$ and $g_2(\mathbf{x}) = f_2(\mathbf{x}A + \mathbf{a}) + \langle \mathbf{b}, \mathbf{x} \rangle + d$ at $\mathbf{u} \in \mathbb{Z}_q^n$ is given by

$$\begin{aligned}
\mathcal{C}_{g_1,g_2}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{g_1(\mathbf{x})-g_2(\mathbf{x}+\mathbf{u})} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f_1(\mathbf{x}A+\mathbf{a})+\langle \mathbf{b},\mathbf{x}\rangle - f_2((\mathbf{x}+\mathbf{u})A+\mathbf{a})-\langle \mathbf{b},\mathbf{x}+\mathbf{u}\rangle} \\
&= \xi^{-\langle \mathbf{b},\mathbf{u}\rangle} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f_1(\mathbf{x}A+\mathbf{a})-f_2((\mathbf{x}A+\mathbf{a})+\mathbf{u}A)} \\
&= \xi^{-\langle \mathbf{b},\mathbf{u}\rangle} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f_1(\mathbf{x})-f_2(\mathbf{x}+\mathbf{u}A)} \\
&= \xi^{-\langle \mathbf{b},\mathbf{u}\rangle} \mathcal{C}_{f_1,f_2}(\mathbf{u}A). \qquad (6.2.8)
\end{aligned}$$

From which it follows that, $|\mathcal{C}_{g_1,g_2}(\mathbf{u})| = |\mathcal{C}_{f_1,f_2}(\mathbf{u}A)|$, and therefore $\sigma_{g_1,g_2} = \sigma_{f_1,f_2}$ and $\triangle_{g_1,g_2} = \triangle_{f_1,f_2}$.

By setting $g_1 = g_2 = g$ (i.e., $f_1 = f_2 = f$) in (6.2.8), we get $|\mathcal{C}_g(\mathbf{u})| = |\mathcal{C}_f(\mathbf{u}A)|$ for all $\mathbf{u} \in \mathbb{Z}_q^n$, and hence $\sigma_g = \sigma_f$. Since A is invertible, $\mathbf{u}A \neq \mathbf{0}$ for all $\mathbf{u} \neq \mathbf{0}$. This implies that $\triangle_g = \triangle_f$. Thus, the SSMI and the MI of q-ary functions f and g are invariant under the affine transformations.

(*b*) follows directly from (6.2.8). ∎

Thus, for any given q-ary function with good GACs, one can construct a large number of q-ary functions with the same GAC criteria.

6.3 Constructions of q-ary s-plateaued functions and their SSMI

In this section, we obtain the SSMI for q-ary s-plateaued functions. Further, we give a construction of such functions.

Theorem 6.3.1. *The SSMI of a q-ary s-plateaued function $f \in \mathcal{B}_{n,q}$ is q^{2n+s}, $s = 1, 2, \ldots, n$.*

Proof. Since f is an s-plateaued function, $|\mathcal{W}_f(\mathbf{u})| \in \{0, q^{\frac{s}{2}}\}$ for every $\mathbf{u} \in \mathbb{Z}_q^n$. Let k be the number of $\mathbf{u}'s$ for which $\mathcal{W}_f(\mathbf{u}) \neq 0$. Then by the Parseval's identity, we get $k = q^{n-s}$. Now by Corollary 5.4.6 of Chapter 5, we have

$$\begin{aligned}\sigma_f &= q^n \sum_{\mathbf{u}\in\mathbb{Z}_q^n} | W_f(\mathbf{u}) |^4 \\ &= q^n \left(q^{n-s}\right) \left(q^{\frac{s}{2}}\right)^4 = q^{2n+s}.\end{aligned}$$

■

Theorem 6.3.2. *Let n, s be integers such that $n + s$ is even. Then a function $f : \mathbb{Z}_q^{\frac{n+s}{2}} \times \mathbb{Z}_q^{\frac{n-s}{2}} \to \mathbb{Z}_q$ expressed as*

$$f(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x}, \phi(\mathbf{y}) \rangle + \ g(\mathbf{y}), \ \textit{for all } (\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_q^{\frac{n+s}{2}} \times \mathbb{Z}_q^{\frac{n-s}{2}}, \tag{6.3.1}$$

where $g \in \mathcal{B}_{\frac{n-s}{2},q}$, and $\phi : \mathbb{Z}_q^{\frac{n-s}{2}} \to \mathbb{Z}_q^{\frac{n+s}{2}}$ is an injective function, is q-ary s-plateaued.

Proof. The WHT of f at $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^{\frac{n+s}{2}} \times \mathbb{Z}_q^{\frac{n-s}{2}}$ is

$$\begin{aligned}\mathcal{W}_f(\mathbf{u}, \mathbf{v}) &= \frac{1}{q^{\frac{n}{2}}} \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{Z}_q^{\frac{n+s}{2}}\times\mathbb{Z}_q^{\frac{n-s}{2}}} \xi^{f(\mathbf{x},\mathbf{y})+\langle\mathbf{u},\mathbf{x}\rangle+\langle\mathbf{v},\mathbf{y}\rangle} \\ &= \frac{1}{q^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_q^{\frac{n+s}{2}}} \sum_{\mathbf{y}\in\mathbb{Z}_q^{\frac{n-s}{2}}} \xi^{\langle\mathbf{x},\phi(\mathbf{y})\rangle+g(\mathbf{y})+\langle\mathbf{u},\mathbf{x}\rangle+\langle\mathbf{v},\mathbf{y}\rangle} \\ &= \frac{1}{q^{\frac{n}{2}}} \sum_{\mathbf{y}\in\mathbb{Z}_q^{\frac{n-s}{2}}} \xi^{g(\mathbf{y})+\langle\mathbf{v},\mathbf{y}\rangle} \sum_{\mathbf{x}\in\mathbb{Z}_q^{\frac{n+s}{2}}} \xi^{\langle\mathbf{x},(\phi(\mathbf{y})+\mathbf{u})\rangle} \\ &= q^{\frac{s}{2}} \sum_{\mathbf{y}\in\mathbb{Z}_q^{\frac{n-s}{2}}} \xi^{g(\mathbf{y})+\langle\mathbf{v},\mathbf{y}\rangle} \delta_{\mathbf{0}}(\phi(\mathbf{y}) + \mathbf{u}) \\ &= \begin{cases} q^{\frac{s}{2}} \xi^{g(\mathbf{y})+\langle\mathbf{v},\mathbf{y}\rangle} & \text{if } \mathbf{y} = \phi^{-1}(-\mathbf{u}), \\ 0 & \text{otherwise,} \end{cases}\end{aligned}$$

from which follows that the function f is q-ary s-plateaued. ■

The q-ary 1-plateaued functions for odd n (resp. 2-plateaued functions, for even n) are referred to as q-ary semi-bent functions. Recall that a function $f \in \mathcal{B}_{n,q}$ is called q-ary semi-bent if for any $\mathbf{a} \in \mathbb{Z}_q^n$, $(i) \mid W_f(\mathbf{a}) \mid \in \{0, \sqrt{q}\}$ for odd n, and $(ii) \mid W_f(\mathbf{a}) \mid \in \{0, q\}$ for even n. The following corollary is corresponding to $s = 1, 2$.

Corollary 6.3.3. *The q-ary function f as constructed in (6.3.1) is semi-bent if $s = 1, 2$, and its SSMI is $\sigma_f = q^{2n+1}$ for odd n, and $\sigma_f = q^{2n+2}$ for even n.*

The following theorem shows that the direct-sum of two q-ary semi-bent functions defined on odd number of variables is also q-ary semi-bent. Recall that a similar computation is provided in Chapter 5 for *q-ary bent* functions.

Theorem 6.3.4. *Let $f_1 \in \mathcal{B}_{r,q}$ and $f_2 \in \mathcal{B}_{s,q}$, where r and s are odd integers. Then a function $f \in \mathcal{B}_{r+s,q}$ expressed as*

$$f(\mathbf{x}, \mathbf{y}) = f_1(\mathbf{x}) + f_2(\mathbf{y}), \quad \textit{for all } \mathbf{x} \in \mathbb{Z}_q^r,\ \mathbf{y} \in \mathbb{Z}_q^s$$

is q-ary semi-bent if f_1 and f_2 both are q-ary semi-bent functions.

Proof. Let $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^r \times \mathbb{Z}_q^s$. Then we have

$$\begin{aligned} \mathcal{W}_f(\mathbf{u}, \mathbf{v}) &= \frac{1}{q^{\frac{r+s}{2}}} \sum_{\mathbf{x} \in \mathbb{Z}_q^r, \mathbf{y} \in \mathbb{Z}_q^s} \xi^{f(\mathbf{x},\mathbf{y}) + \langle \mathbf{u}, \mathbf{x} \rangle + \langle \mathbf{v}, \mathbf{y} \rangle} \\ &= \frac{1}{q^{\frac{r}{2}}} \sum_{\mathbf{x} \in \mathbb{Z}_q^r} \xi^{f_1(\mathbf{x}) + \langle \mathbf{u}, \mathbf{x} \rangle} \frac{1}{q^{\frac{s}{2}}} \sum_{\mathbf{y} \in \mathbb{Z}_q^s} \xi^{f_2(\mathbf{y}) + \langle \mathbf{v}, \mathbf{y} \rangle} \\ &= \mathcal{W}_{f_1}(\mathbf{u}) \mathcal{W}_{f_2}(\mathbf{v}). \end{aligned} \tag{6.3.2}$$

Since f_1 and f_2 both are q-ary semi-bent, then for every $\mathbf{u} \in \mathbb{Z}_q^r$, $|\mathcal{W}_{f_1}(\mathbf{u})| \in \{0, \sqrt{q}\}$, and for every $\mathbf{v} \in \mathbb{Z}_q^s$, $|\mathcal{W}_{f_2}(\mathbf{v})| \in \{0, \sqrt{q}\}$. This implies that $|\mathcal{W}_f(\mathbf{u}, \mathbf{v})| = |\mathcal{W}_{f_1}(\mathbf{u})||\mathcal{W}_{f_2}(\mathbf{v})| \in \{0, q\}$ for all $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^r \times \mathbb{Z}_q^s$. Hence f is q-ary semi-bent. ∎

6.4 Bounds on σ_f and $\triangle_f$ for some well-known classes of cubic Boolean functions

In this section, for convenience we denote $\mathbb{Z}_2$ by $\mathbb{F}_2$, and $\mathbb{F}_{2^n}$ denotes the field of order 2^n. Recall that, in the binary case, the MI is additive autocorrelation and SSMI is the sum-of-squares indicators [59, 162].

Gong and Khoo [59] have introduced the concept of dual of a non-bent Boolean function f (the dual of $f \in \mathcal{B}_n$ is a function $\tilde{f} \in \mathcal{B}_n$ defined by $\tilde{f}(x) = 1$ if $W_f(x) \neq 0$ and $\tilde{f}(x) = 0$ if $W_f(x) = 0$). They provide a relationship between the autocorrelation spectrum of the function and WHT of its dual as follows

Lemma 6.4.1. *[59] Let $f \in \mathcal{B}_n$ such that $W_f(a) \in \{0, \pm 2^i\}$ for all $a \in \mathbb{F}_{2^n}$. Then*

$$C_f(a) = -2^{2i-(n+1)} W_{\tilde{f}}(a), \text{ for all } a \in \mathbb{F}_{2^n} \setminus \{0\}.$$

Using this result, they have investigated several classes of semi-bent Boolean functions such as: Dillon-Dobbertin, Kasami, Segre hyperoval and Welch-Gong transformation functions for which the bounds on absolute indicator (MI) has optimal value (for an odd n, a balanced Boolean function $f \in \mathcal{B}_n$ has optimal additive autocorrelation if $\triangle_f = 2^{\frac{n+1}{2}}$ [59]). For a function from any of the above classes we can construct a large number of semi-bent Boolean functions with same values of these indicators using Theorem 6.2.4 for $q = 2$.

The Hamming weight $w_H(f)$ of a semi-bent function $f \in \mathcal{B}_n$, for even n, takes value from the set $\{2^{n-1}, 2^{n-1} \pm 2^{\frac{n}{2}}\}$. Also, $w_H(\tilde{f}) = 2^{n-2}$. The following result follows from Lemma 6.4.1 and [59, Proposition 3].

Theorem 6.4.2. *Let n be an even positive integer and $f \in \mathcal{B}_n$ be a semi-bent function. Then the dual $\tilde{f}$ of f is neither a bent function nor a semi-bent function. Moreover, f never achieves the optimal value of the additive autocorrelation.*

The derivative of a cubic Boolean function is at most quadratic, and the WHT (the weight distribution) of affine and quadratic function $f \in \mathcal{B}_n$ is fully characterized in terms of the dimension k of the kernel $\mathcal{E}_f$ of the bilinear form associated with f [10]. If we take

$f = g$ with $\deg(g) \leq 3$ in [166, Theorem 8], then $\triangle_f \leq 2^n$ and $\sigma_f \leq 2^{3n}$, which are well known (trivial) bounds of $\triangle_f$ and σ_f, that is, we get no new information about the two indicators: $\triangle_f$ and σ_f.

Now we consider bounds on two indicators $\triangle f$ and σ_f for some classes of cubic Boolean functions.

Lemma 6.4.3. *The autocorrelation of a cubic function $f \in \mathcal{B}_n$ at $\mathbf{a} \in \mathbb{F}_2^n$ is given by*

$$|C_f(\mathbf{a})|^2 = 2^n \sum_{\mathbf{b} \in \mathcal{E}_{D_\mathbf{a} f}} (-1)^{\epsilon_{\mathbf{a},\mathbf{b}}}, \text{ and } |C_f(\mathbf{a})|^2 \leq 2^n |\mathcal{E}_{D_\mathbf{a} f}|,$$

where $\mathcal{E}_{D_\mathbf{a} f}$, the kernel of $D_\mathbf{a} f$ is given by

$$\mathcal{E}_{D_\mathbf{a} f} = \{\mathbf{b} \in \mathbb{F}_2^n : D_\mathbf{b} D_\mathbf{a} f(x) = \epsilon_{\mathbf{a},\mathbf{b}} (\textit{constant})\}.$$

Proof. The autocorrelation of any $f \in \mathcal{B}_n$ at $\mathbf{a} \in \mathbb{F}_2^n$ is given by

$$C_f(\mathbf{a}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) + f(\mathbf{x}+\mathbf{a})} = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{D_\mathbf{a} f(\mathbf{x})}.$$

Therefore,

$$\begin{aligned} |C_f(\mathbf{a})|^2 &= \sum_{\mathbf{x} \in \mathbb{F}_2^n} \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{D_\mathbf{a} f(\mathbf{x})} (-1)^{D_\mathbf{a} f(\mathbf{y})} \\ &= \sum_{\mathbf{x} \in \mathbb{F}_2^n} \sum_{\mathbf{y} = \mathbf{x} + \mathbf{b} \in \mathbb{F}_2^n} (-1)^{D_\mathbf{a} f(\mathbf{x})} (-1)^{D_\mathbf{a} f(\mathbf{y})} \\ &= \sum_{\mathbf{b} \in \mathbb{F}_2^n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{D_\mathbf{a} f(\mathbf{x}) + D_\mathbf{a} f(\mathbf{x}+\mathbf{b})} \\ &= \sum_{\mathbf{b} \in \mathbb{F}_2^n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{D_\mathbf{b} D_\mathbf{a} f(\mathbf{x})}. \end{aligned} \tag{6.4.1}$$

Further, if f is cubic, then the derivative $D_\mathbf{a} f$ of f at any $\mathbf{a} \in \mathbb{F}_2^n$ is at most quadratic, and $D_\mathbf{b} D_\mathbf{a} f(\mathbf{x})$ is at most affine function for any $\mathbf{b} \in \mathbb{F}_2^n$. This implies that $D_\mathbf{b} D_\mathbf{a} f(\mathbf{x})$ is either constant function or balanced function. The function $D_\mathbf{b} D_\mathbf{a} f(\mathbf{x})$ is balanced if $\mathbf{b} \notin \mathcal{E}_{D_\mathbf{a} f}$,

otherwise $D_{\mathbf{b}}D_{\mathbf{a}}f(\mathbf{x})$ is a constant function. Using this result in (6.4.1), we get

$$\begin{aligned}|C_f(\mathbf{a})|^2 &= \sum_{\mathbf{b}\in\mathcal{E}_{D_{\mathbf{a}}f}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{\epsilon_{\mathbf{a},\mathbf{b}}} + \sum_{\mathbf{b}\notin\mathcal{E}_{D_{\mathbf{a}}f}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{D_{\mathbf{b}}D_{\mathbf{a}}f(\mathbf{x})} \\ &= 2^n\sum_{\mathbf{b}\in\mathcal{E}_{D_{\mathbf{a}}f}}(-1)^{\epsilon_{\mathbf{a},\mathbf{b}}}.\end{aligned}$$

Therefore,

$$|C_f(\mathbf{a})|^2 \leq 2^n|\mathcal{E}_{D_{\mathbf{a}}f}|.$$

■

In the following subsections, we use above result to obtain the non-trivial bounds on $\triangle f$ and σ_f for some well-known highly nonlinear and non-bent cubic Boolean functions.

6.4.1 For Welch and modified-Welch functions

The vectorial Welch function $F_{welch} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined by $x \mapsto x^{2^\ell+3}$, where ℓ is a positive integer and $n = 2\ell+1$. These functions are maximally nonlinear (with $nl(F_{welch}) = 2^{n-1} - 2^{\frac{n-1}{2}}$) [9]. Let $f_\lambda(x) = tr_1^n(\lambda x^{2^\ell+3})$ ($tr_1^n(.)$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$) be a Welch Boolean function. The function $f_\lambda(x)$ corresponding to $n = 2\ell - 1$ is said to be modified-Welch function. Both Welch and modified-Welch functions also have very good lower bounds on second order nonlinearity [15]. For more details on these functions we refer to [15, 44].

In the following theorem, we deduce the upper bounds on the two indicators $\triangle f$ and σ_f for Welch and Modified-Welch functions.

Theorem 6.4.4. *Let ℓ is an positive integer. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function defined by $f(x) = tr_1^n(x^{2^\ell+3})$. Then*

(a) *if $n = 2\ell + 1$, then $\triangle_f \leq 2^{\frac{n+3}{2}}$ and $\sigma_f = 2^{2n+1}$.*

(b) *if $n = 2\ell - 1$, then $\triangle_f \leq 2^{\frac{n+3}{2}}$ and $\sigma_f \leq 2^{2n+2} + 2^{2n+1}$ if $\gcd(n, 3) = 1$, otherwise, $\sigma_f \leq 2^{2n+2} + 2^{2n+1} + 7\sqrt{6}\cdot 2^{\frac{3n}{2}-1}$.*

Proof. (a) If $n = 2\ell+1$, then the dimension $k(a)$ of the kernel $\mathcal{E}_{D_af}$ of D_af is at most 3 for all $a \in \mathbb{F}_{2^n} \setminus \{0\}$ [15]. Using Lemma 6.4.3 and Theorem 6.3.1 with $q = 2$, we get $\triangle_f \leq 2^{\frac{n+3}{2}}$ and $\sigma_f = 2^{2n+1}$.

(b) If $n = 2\ell - 1$, then the dimension $k(a)$ of the kernel $\mathcal{E}_{D_af}$ is at most 3 for any $a \in \mathbb{F}_{2^n} \setminus \{0\}$ [15, pp 1269]. Moreover, if $\gcd(n, 3) = 1$, then $N(a)$, the number of a's for which $k(a) = 1$, is 2^{n-1}, i.e., $N(a) = 2^{n-1}$, otherwise, $N(a) \geq 2^{n-1} - 2^{\frac{n}{2}-1}\sqrt{6}$. Using these results in Lemma 6.4.3, we get the desired result. ∎

Remark 6.4.5. *It is well known that $2^{2n} \leq \sigma_f \leq 2^{3n}$ and $0 \leq \triangle_f \leq 2^n$. From Theorem 6.4.4, we observe that the upper bounds on the indicators $\triangle_f$ and σ_f for both Welch and modified-Welch functions are much better than these bounds.*

6.4.2 For semi-bent Boolean functions in [146] on even n

Sun and Wu [146] have obtained the lower bounds on second-order nonlinearities of two well known classes of cubic semi-bent Boolean functions [35] of the form $f(x) = tr_1^n(x^d)$, for all $x \in \mathbb{F}_2^n$, where (i) $d = 2^{r+1} + 3$ and $n = 2r$, and (ii) $d = 2^{2r} + 2^{r+1} + 1$, $n = 2r$, and r is odd. The obtained bounds are very good. In particular, for $n = 8$, these functions achieve the maximum possible second-order nonlinearity: $nl_2(f) = 84$ [146, Section 4].

In the following theorem, we deduce the upper bounds of the two indicators: $\triangle_f$ and σ_f for the semi-bent Boolean functions of these classes.

Theorem 6.4.6. *Let $f \in \mathcal{B}_n$ be a cubic Boolean function of the form $f(x) = tr_1^n(x^d)$, where*

(a) *$d = 2^{r+1} + 3$ and $n = 2r$, or*

(b) *$d = 2^{2r} + 2^{r+1} + 1$, $n = 2r$, and r is odd.*

Then $\triangle_f \leq 2^{\frac{3n+4}{4}}$ and $\sigma_f = 2^{2n+2}$.

Proof. For both of the cases, the dimension of the kernel $\mathcal{E}_{D_af}$ is $k(a) = 2$ if $a \notin \mathbb{F}_{2^r}$, and

$k(a) = r + 2$ if $a \in \mathbb{F}_{2^r}$ [146]. Now, by Lemma 6.4.3, we get

$$\begin{aligned} \triangle_f &= \max_{a \in \mathbb{F}_{2^n} \setminus \{0\}} |C_f(a)| \\ &\leq 2^{\frac{n+r+2}{2}} \\ &= 2^{\frac{3n+4}{4}}. \end{aligned}$$

In either case f is semi-bent, and so, the second part follows from Theorem 6.3.1. ■

Chapter 7

The SSMI of some q-ary functions

7.1 Introduction

In this chapter, we further continue our study on q-ary functions in terms of the indicators: the SSMI and the MI as introduced in Chapter 5. It is well known that the crosscorrelation between two functions indicates that statistically how far they are from each other. The low crosscorrelation between the functions shows that they are very different from each other, and such functions when used in any cryptosystem provide best confusion. For last few decades, it has been a problem of great interest in the literature to construct cryptographic functions with low values of crosscorrelation and the autocorrelation. The crosscorrelation and the autocorrelation of the functions have been studied by researchers in many different forms. As stated in Chapter 5 that the two indicators: the SSMI and the MI are closely related to the crosscorrelation (or autocorrelation) of the functions. The lower value of the indicators for the cryptographic functions correspond to low correlation between them. Therefore, it is important to investigate the bounds on these indicators.

In this chapter, we turn our attention especially to the study of the behavior of the indicator the SSMI of q-ary functions. We provide some results representing relationships among $\sigma_{f,g}$, σ_f (the SSMI of f) and σ_g for arbitrary two q-ary functions. Also, we obtain some upper bounds on the indicators, the SSMI and the MI for two q-ary functions one of which is an s-plateaued function. We present a construction of ternary functions and investigate a link of the SSMI between an $(n+1)$-variable ternary function and its n-variable

decomposition functions. We present a construction of m-plateaued ternary functions with disjoint WHS. Further, we use these m-plateaued functions to construct some ternary functions with smaller value of the SSMI.

7.2 Preliminaries

Recall that the following result is Theorem 5.2.1, which provides a relationship between the crosscorrelation of two q-ary functions and their WHS.

Lemma 7.2.1. *Let $f, g \in \mathcal{B}_{n,q}$, and $\mathbf{u}, \mathbf{x} \in \mathbb{Z}_q^n$, then*

$$\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{x}) \overline{\mathcal{W}_g(\mathbf{x})} \xi^{\langle \mathbf{u}, \mathbf{x} \rangle}.$$

Two functions f and g are said be *perfectly uncorrelated* if $\mathcal{C}_{f,g}(\mathbf{u}) = 0$ for every $\mathbf{u} \in \mathbb{Z}_q^n$ [128]. It is clear from Lemma 7.2.1 that $\mathcal{W}_f(\mathbf{u})\mathcal{W}_g(\mathbf{u}) = 0$ for every $\mathbf{u} \in \mathbb{Z}_q^n$ implies that $\mathcal{C}_{f,g}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n$, i.e., the functions f and g are perfectly uncorrelated if they are disjoint spectra functions.

Further, we recall following result, which is Corollary 5.4.6.

Lemma 7.2.2. *Let $f, g \in \mathcal{B}_{n,q}$ and $\mathbf{u} \in \mathbb{Z}_q^n$. Then the SSMI of f and g is given by*

$$\sigma_{f,g} = q^n \sum_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u})|^2 |\mathcal{W}_g(\mathbf{u})|^2.$$

Further, for $f = g$, the SSMI of f is given by

$$\sigma_f = q^n \sum_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u})|^4.$$

7.3 Bounds on the SSMI of two q-ary functions

In this section, we provide a relationship among $\sigma_{f,g}$, σ_f and σ_g of two q-ary functions f and g. The results are generalization of the results appeared in [165, 167] obtained for $q = 2$.

Theorem 7.3.1. *Let $f, g \in \mathcal{B}_{n,q}$. Then the SSMI of f and g satisfies the relation*

$$\sigma_{f,g}^2 \leq \sigma_f \sigma_g.$$

Further, we have $\sigma_{f,g}^2 = \sigma_f \sigma_g$ if and only if $|\mathcal{W}_f(\mathbf{u})| = |\mathcal{W}_g(\mathbf{u})|$ for every $\mathbf{u} \in \mathbb{Z}_q^n$.

Proof. By Lemma 7.2.2, we have

$$\sigma_{f,g}^2 = q^{2n} \left(\sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 |\mathcal{W}_g(\mathbf{x})|^2 \right)^2 \tag{7.3.1}$$

and

$$\sigma_f = q^n \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^4, \text{ and } \sigma_g = q^n \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\mathcal{W}_g(\mathbf{x})|^4. \tag{7.3.2}$$

Now, using Cauchy-Schwarz's inequality, i.e., $(\sum_{i=1}^n a_i b_i)^2 \leq \sum_{i=1}^n a_i^2 \sum_{i=1}^n b_i^2$, in (7.3.1) and (7.3.2), we get

$$\left(\sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 |\mathcal{W}_g(\mathbf{x})|^2 \right)^2 \leq \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^4 \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\mathcal{W}_g(\mathbf{x})|^4,$$

from which follows that $\sigma_{f,g}^2 \leq \sigma_f \sigma_g$. Further, it is easy to verify that $\sigma_{f,g}^2 = \sigma_f \sigma_g$ if and only if $|\mathcal{W}_f(\mathbf{u})| = |\mathcal{W}_g(\mathbf{u})|$ for every $\mathbf{u} \in \mathbb{Z}_q^n$. ∎

Theorem 7.3.2. *Let $f, g \in \mathcal{B}_{n,q}$. Then the SSMI of f and g satisfies*

$$0 \leq \sigma_{f,g} \leq \frac{1}{2}(\sigma_f + \sigma_g).$$

Further, $\sigma_{f,g} = 0$ if and only if f and g are disjoint spectra functions, and $\sigma_{f,g} = \frac{1}{2}(\sigma_f + \sigma_g)$ if and only if $|\mathcal{W}_f(\mathbf{u})| = |\mathcal{W}_g(\mathbf{u})|$ for every $\mathbf{u} \in \mathbb{Z}_q^n$.

Proof. Using Lemma 7.2.2, we have

$$\sigma_{f,g} = q^n \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 |\mathcal{W}_g(\mathbf{x})|^2 \tag{7.3.3}$$

$$\begin{aligned}
&= q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 \left(|\mathcal{W}_g(\mathbf{x})|^2 - |\mathcal{W}_f(\mathbf{x})|^2 + |\mathcal{W}_f(\mathbf{x})|^2\right) \\
&= q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^4 + q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 \left(|\mathcal{W}_g(\mathbf{x})|^2 - |\mathcal{W}_f(\mathbf{x})|^2\right) \\
&= \sigma_f + q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 \left(|\mathcal{W}_g(\mathbf{x})|^2 - |\mathcal{W}_f(\mathbf{x})|^2\right).
\end{aligned} \tag{7.3.4}$$

By using similar computation, we obtain

$$\sigma_{f,g} = \sigma_g + q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_g(\mathbf{x})|^2 \left(|\mathcal{W}_f(\mathbf{x})|^2 - |\mathcal{W}_g(\mathbf{x})|^2\right). \tag{7.3.5}$$

On combining (7.3.4) and (7.3.5), we get

$$\begin{aligned}
\sigma_{f,g} &= \frac{1}{2}(\sigma_f + \sigma_g) + \frac{q^n}{2} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 \left(|\mathcal{W}_g(\mathbf{x})|^2 - |\mathcal{W}_f(\mathbf{x})|^2\right) \\
&\qquad + \frac{q^n}{2} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_g(\mathbf{x})|^2 \left(|\mathcal{W}_f(\mathbf{x})|^2 - |\mathcal{W}_g(\mathbf{x})|^2\right) \\
&= \frac{1}{2}(\sigma_f + \sigma_g) - \frac{q^n}{2} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \left(|\mathcal{W}_f(\mathbf{x})|^2 - |\mathcal{W}_g(\mathbf{x})|^2\right)^2.
\end{aligned} \tag{7.3.6}$$

Thus, from the definition of SSMI and (7.3.6), we obtain

$$0 \le \sigma_{f,g} \le \frac{1}{2}(\sigma_f + \sigma_g).$$

Now, from (7.3.6), it is clear that $\sigma_{f,g} = 0$ if and only if

$$\begin{aligned}
(\sigma_f + \sigma_g) &= q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \left(|\mathcal{W}_f(\mathbf{x})|^2 - |\mathcal{W}_g(\mathbf{x})|^2\right)^2 \\
&= q^n \left(\sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^4 + \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_g(\mathbf{x})|^4\right),
\end{aligned} \tag{7.3.7}$$

if and only if $\mathcal{W}_f(\mathbf{x})\mathcal{W}_g(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{Z}_q^n$, i.e., if and only if f and g are disjoint spectra functions.

On the other hand, it also follows from (7.3.6) that $\sigma_{f,g} = \frac{1}{2}(\sigma_f + \sigma_g)$ if and only if $|\mathcal{W}_f(\mathbf{x})| = |\mathcal{W}_g(\mathbf{x})|$ for all $\mathbf{x} \in \mathbb{Z}_q^n$. ■

Recall that a function $f \in \mathcal{B}_{n,q}$ is called *s-plateaued* if for some s, with $0 \leq s \leq n$, $|W_f(\mathbf{a})| \in \{0, q^{\frac{s}{2}}\}$ for all $\mathbf{a} \in \mathbb{Z}_q^n$ [24]. The case $s = 0$ corresponds to bent functions and $s = n$ to affine or constant functions. In the following result, we deduce upper bounds on the indicators, the SSMI and the MI of two q-ary functions, one of which is s-plateaued.

Theorem 7.3.3. *Let $f, g \in \mathcal{B}_{n,q}$. Suppose f is an s-plateaued q-ary function for $0 \leq s \leq n$, and $M_g = \max_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u})|$. Then, we have*

1. $\triangle_{f,g} \leq q^{n+\frac{s}{2}} M_g$, *and*

2. $\sigma_{f,g} \leq q^{2n+s}$.

Proof. Since f is an s-plateaued q-ary function, therefore, $|W_f(\mathbf{x})| \in \{0, q^{\frac{s}{2}}\}$ $\forall \mathbf{x} \in \mathbb{Z}_q^n$.

(1) By using the result in Lemma 7.2.1, for every $\mathbf{u} \in \mathbb{Z}_q^n$, we have

$$\begin{aligned}
\mathcal{C}_{f,g}(\mathbf{u}) &= \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{x}) \overline{\mathcal{W}_g(\mathbf{x})} \xi^{\langle \mathbf{u}, \mathbf{x} \rangle} \\
&\leq \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})| |\overline{\mathcal{W}_g(\mathbf{x})}| \\
&= q^{\frac{s}{2}} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\mathcal{W}_g(\mathbf{x})| \\
&\leq q^{\frac{s}{2}} \cdot q^n M_g \\
&= q^{n+\frac{s}{2}} M_g.
\end{aligned}$$

From which it follows that $\triangle_{f,g} = \max_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\mathbf{u})| \leq q^{n+\frac{s}{2}} M_g$.

(2) From the Parseval's identity and Lemma 7.2.2, we have

$$\begin{aligned}
\sigma_{f,g} &= q^n \sum_{\mathbf{x} \in \mathbb{Z}_q^n} | W_f(\mathbf{x}) |^2 | W_g(\mathbf{x}) |^2 \\
&\leq q^n q^s \sum_{\mathbf{x} \in \mathbb{Z}_q^n} | W_g(\mathbf{x}) |^2 \\
&= q^{n+s} \cdot q^n = q^{2n+s}.
\end{aligned}$$

■

7.4 Construction of a ternary functions and bounds on their SSMI

In the following result, we construct a ternary function f on $n+1$ variables in terms of its subfunctions f_1, f_2 and f_3 on n variables. We investigate a relationship between SSMI of f and its subfunctions f_1, f_2 and f_3.

Theorem 7.4.1. *Let a function $f \in \mathcal{B}_{n+1,3}$ expressed as*

$$f(\mathbf{x}, x_{n+1}) = \frac{1}{2}\left((1+x_{n+1})(2+x_{n+1})f_1(\mathbf{x}) + x_{n+1}(1+x_{n+1})f_2(\mathbf{x}) + x_{n+1}(2+x_{n+1})f_3(\mathbf{x})\right), \tag{7.4.1}$$

where $f_1, f_2, f_3 \in \mathcal{B}_{n,3}$ such that $\mathcal{C}_{f_i,f_j}(\mathbf{u})\mathcal{C}_{f_j,f_k}(\mathbf{u}) = 0$ for all $i \neq j, j \neq k$, $i, j, k \in \{1, 2, 3\}$. Then the SSMI of f is given by

$$\sigma_f = \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} + 4(\sigma_{f_1,f_2} + \sigma_{f_2,f_3} + \sigma_{f_1,f_3}).$$

Proof. The autocorrelation of f at $(\mathbf{u}, u_{n+1}) \in \mathbb{Z}_3^n \times \mathbb{Z}_3$ is given by

$$\mathcal{C}_f(\mathbf{u}, u_{n+1}) = \sum_{\mathbf{x}\in\mathbb{Z}_3^n} \sum_{x_{n+1}\in\mathbb{Z}_3} \omega^{f(\mathbf{x},x_{n+1}) - f(\mathbf{x}+\mathbf{u},x_{n+1}+u_{n+1})}, \tag{7.4.2}$$

where $f(\mathbf{x}, x_{n+1}) = \frac{1}{2}(1+x_{n+1})(2+x_{n+1})f_1(\mathbf{x}) + \frac{1}{2}\left(x_{n+1}(1+x_{n+1})f_2(\mathbf{x}) + x_{n+1}(2+x_{n+1})f_3(\mathbf{x})\right)$, and

$$\begin{aligned} f(\mathbf{x}+\mathbf{u}, x_{n+1}+u_{n+1}) = {} & \frac{1}{2}(1+x_{n+1}+u_{n+1})(2+x_{n+1}+u_{n+1})f_1(\mathbf{x}+\mathbf{u}) + \frac{1}{2}(x_{n+1}+u_{n+1}) \\ & \times (1+x_{n+1}+u_{n+1})f_2(\mathbf{x}+\mathbf{u}) + \frac{1}{2}(x_{n+1}+u_{n+1})(2+x_{n+1}+u_{n+1})f_3(\mathbf{x}+\mathbf{u}). \end{aligned}$$

Now, since $u_{n+1}, x_{n+1} \in \mathbb{Z}_3$, therefore, from (7.4.2), we get the following expression

$$\mathcal{C}_f(\mathbf{u}, 0) = \sum_{\mathbf{x}\in\mathbb{Z}_3^n} \sum_{x_{n+1}\in\mathbb{Z}_3} \omega^{f(\mathbf{x},x_{n+1}) - f(\mathbf{x}+\mathbf{u},x_{n+1})}$$

$$\begin{aligned}
&= \sum_{\mathbf{x}\in\mathbb{Z}_3^n}\sum_{x_{n+1}\in\mathbb{Z}_3} \omega^{\frac{1}{2}(1+x_{n+1})(2+x_{n+1})(f_1(\mathbf{x})-f_1(\mathbf{x}+\mathbf{u}))+\frac{1}{2}x_{n+1}(1+x_{n+1})(f_2(\mathbf{x})+f_2(\mathbf{x}+\mathbf{u}))} \\
&\qquad \times\omega^{\frac{1}{2}x_{n+1}(2+x_{n+1})(f_3(\mathbf{x})+f_3(\mathbf{x}+\mathbf{u}))} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_3^n,x_{n+1}=0} \omega^{f_1(\mathbf{x})-f_1(\mathbf{x}+\mathbf{u})} + \sum_{\mathbf{x}\in\mathbb{Z}_3^n,x_{n+1}=1} \omega^{f_2(\mathbf{x})-f_2(\mathbf{x}+\mathbf{u})} + \sum_{\mathbf{x}\in\mathbb{Z}_3^n,x_{n+1}=2} \omega^{f_3(\mathbf{x})-f_3(\mathbf{x}+\mathbf{u})} \\
&= \mathcal{C}_{f_1}(\mathbf{u})+\mathcal{C}_{f_2}(\mathbf{u})+\mathcal{C}_{f_3}(\mathbf{u}). \qquad (7.4.3)
\end{aligned}$$

In the similar way, we can compute the following

$$\begin{aligned}
\mathcal{C}_f(\mathbf{u},1) &= \mathcal{C}_{f_1,f_2}(\mathbf{u})+\mathcal{C}_{f_2,f_3}(\mathbf{u})+\mathcal{C}_{f_3,f_1}(\mathbf{u}), \text{ and} \\
\mathcal{C}_f(\mathbf{u},2) &= \mathcal{C}_{f_2,f_1}(\mathbf{u})+\mathcal{C}_{f_1,f_3}(\mathbf{u})+\mathcal{C}_{f_3,f_2}(\mathbf{u}).
\end{aligned} \qquad (7.4.4)$$

In the view of (7.4.3) and (7.4.4), the SSMI of $f\in\mathcal{B}_{n,3}$ is given by

$$\begin{aligned}
\sigma_f &= \sum_{(\mathbf{u},u_{n+1})\in\mathbb{Z}_3^n\times\mathbb{Z}_3} |\mathcal{C}_f(\mathbf{u},u_{n+1})|^2 \\
&= \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_f(\mathbf{u},0)|^2 + \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_f(\mathbf{u},1)|^2 + \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_f(\mathbf{u},2)|^2 \\
&= \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_{f_1}(\mathbf{u})+\mathcal{C}_{f_2}(\mathbf{u})+\mathcal{C}_{f_3}(\mathbf{u})|^2 + \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_{f_1,f_2}(\mathbf{u})+\mathcal{C}_{f_2,f_3}(\mathbf{u})+\mathcal{C}_{f_3,f_1}(\mathbf{u})|^2 \\
&+ \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_{f_2,f_1}(\mathbf{u})+\mathcal{C}_{f_1,f_3}(\mathbf{u})+\mathcal{C}_{f_3,f_2}(\mathbf{u})|^2 \\
&= R+S+T, \qquad (7.4.5)
\end{aligned}$$

where

$$\begin{aligned}
R &= \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_{f_1}(\mathbf{u})+\mathcal{C}_{f_2}(\mathbf{u})+\mathcal{C}_{f_3}(\mathbf{u})|^2, \\
S &= \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_{f_1,f_2}(\mathbf{u})+\mathcal{C}_{f_2,f_3}(\mathbf{u})+\mathcal{C}_{f_3,f_1}(\mathbf{u})|^2, \text{ and} \\
T &= \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_{f_2,f_1}(\mathbf{u})+\mathcal{C}_{f_1,f_3}(\mathbf{u})+\mathcal{C}_{f_3,f_2}(\mathbf{u})|^2.
\end{aligned}$$

Now, we compute

$$R = \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_{f_1}(\mathbf{u})+\mathcal{C}_{f_2}(\mathbf{u})+\mathcal{C}_{f_3}(\mathbf{u})|^2$$

$$= \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} + \sum_{\mathbf{u}\in\mathbb{Z}_3^n} \Big(\mathcal{C}_{f_1}(\mathbf{u})\overline{\mathcal{C}_{f_2}(\mathbf{u})} + \mathcal{C}_{f_2}(\mathbf{u})\overline{\mathcal{C}_{f_3}(\mathbf{u})} + \mathcal{C}_{f_3}(\mathbf{u})\overline{\mathcal{C}_{f_1}(\mathbf{u})} + \mathcal{C}_{f_2}(\mathbf{u})\overline{\mathcal{C}_{f_1}(\mathbf{u})} + \mathcal{C}_{f_3}(\mathbf{u})\overline{\mathcal{C}_{f_2}(\mathbf{u})} + \mathcal{C}_{f_1}(\mathbf{u})\overline{\mathcal{C}_{f_3}(\mathbf{u})} \Big). \tag{7.4.6}$$

For any two ternary functions $g, h \in \mathcal{B}_{n,3}$, we have

$$\begin{aligned}
\sum_{\mathbf{u}\in\mathbb{Z}_3^n} \mathcal{C}_g(\mathbf{u})\overline{\mathcal{C}_h(\mathbf{u})} &= \sum_{\mathbf{u}\in\mathbb{Z}_3^n}\sum_{\mathbf{x}\in\mathbb{Z}_3^n} \omega^{g(\mathbf{x})-g(\mathbf{x}+\mathbf{u})}\overline{\sum_{\mathbf{y}\in\mathbb{Z}_3^n} \omega^{h(\mathbf{y})-h(\mathbf{y}+\mathbf{u})}} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_3^n}\sum_{\mathbf{y}\in\mathbb{Z}_3^n} \omega^{g(\mathbf{x})-h(\mathbf{y})} \sum_{\mathbf{u}\in\mathbb{Z}_3^n} \omega^{-g(\mathbf{x}+\mathbf{u})+h(\mathbf{y}+\mathbf{u})} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_3^n}\sum_{\mathbf{y}\in\mathbb{Z}_3^n} \omega^{g(\mathbf{x})-h(\mathbf{y})} \sum_{\mathbf{z}\in\mathbb{Z}_3^n} \omega^{-g(\mathbf{z})+h(\mathbf{y}+\mathbf{z}-\mathbf{x})} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_3^n}\sum_{\mathbf{y}\in\mathbb{Z}_3^n} \omega^{g(\mathbf{x})-h(\mathbf{y})}\overline{\mathcal{C}_{g,h}(\mathbf{y}-\mathbf{x})} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_3^n}\sum_{\mathbf{e}\in\mathbb{Z}_3^n} \omega^{g(\mathbf{x})-h(\mathbf{x}+\mathbf{e})}\overline{\mathcal{C}_{g,h}(\mathbf{e})} \\
&= \sum_{\mathbf{e}\in\mathbb{Z}_3^n} \mathcal{C}_{g,h}(\mathbf{e})\overline{\mathcal{C}_{g,h}(\mathbf{e})} \\
&= \sum_{\mathbf{e}\in\mathbb{Z}_3^n} |\mathcal{C}_{g,h}(\mathbf{e})|^2 = \sigma_{f_1,f_2}.
\end{aligned} \tag{7.4.7}$$

Also,

$$\sum_{\mathbf{u}\in\mathbb{Z}_3^n} \mathcal{C}_h(\mathbf{u})\overline{\mathcal{C}_g(\mathbf{u})} = \sigma_{f_1,f_2}. \tag{7.4.8}$$

On combining (7.4.6), (7.4.7) and (7.4.8), we obtain

$$R = \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} + 2\left(\sigma_{f_1,f_2} + \sigma_{f_2,f_3} + \sigma_{f_3,f_1}\right). \tag{7.4.9}$$

Now, we compute

$$\begin{aligned}
S &= \sum_{\mathbf{u}\in\mathbb{Z}_3^n} |\mathcal{C}_{f_1,f_2}(\mathbf{u}) + \mathcal{C}_{f_2,f_3}(\mathbf{u}) + \mathcal{C}_{f_3,f_1}(\mathbf{u})|^2 \\
&= \sigma_{f_1,f_2} + \sigma_{f_2,f_3} + \sigma_{f_3,f_1} + \sum_{\mathbf{u}\in\mathbb{Z}_3^n} \Big(\mathcal{C}_{f_1,f_2}(\mathbf{u})\overline{\mathcal{C}_{f_2,f_3}(\mathbf{u})} + \mathcal{C}_{f_2,f_3}(\mathbf{u})\overline{\mathcal{C}_{f_1,f_2}(\mathbf{u})} + \mathcal{C}_{f_1,f_2}(\mathbf{u})\overline{\mathcal{C}_{f_3,f_1}(\mathbf{u})} \\
&\qquad + \mathcal{C}_{f_3,f_1}(\mathbf{u})\overline{\mathcal{C}_{f_1,f_2}(\mathbf{u})} + \mathcal{C}_{f_2,f_3}(\mathbf{u})\overline{\mathcal{C}_{f_3,f_1}(\mathbf{u})} + \mathcal{C}_{f_1,f_3}(\mathbf{u})\overline{\mathcal{C}_{f_2,f_3}(\mathbf{u})} \Big).
\end{aligned} \tag{7.4.10}$$

The functions f_1, f_2 and f_3 involved in the constructed function f satisfy the property that for every $\mathbf{u} \in \mathbb{Z}_3^n$, $\mathcal{C}_{f_i,f_j}(\mathbf{u})\overline{\mathcal{C}_{f_j,f_k}(\mathbf{u})} = 0$ for every $i \neq j, j \neq k$ and $i, j, k \in \{1, 2, 3\}$. Using this property of f_1, f_2 and f_3 in (7.4.10), we get

$$S = \sigma_{f_1,f_2} + \sigma_{f_2,f_3} + \sigma_{f_3,f_1}. \tag{7.4.11}$$

By proceeding in similar way, we obtain

$$T = \sigma_{f_1,f_2} + \sigma_{f_2,f_3} + \sigma_{f_3,f_1}. \tag{7.4.12}$$

On substituting the values of R, S and T from (7.4.9), (7.4.11) and (7.4.12) in (7.4.5), we obtain

$$\sigma_f = \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} + 4(\sigma_{f_1,f_2} + \sigma_{f_2,f_3} + \sigma_{f_1,f_3}).$$

This completes the proof. ■

As noted earlier, the smaller value of σ_f correspond to low autocorrelation of f and hence to better GAC of f [162]. It is clear from Theorem 7.4.1 that the decomposition functions f_1, f_2 and f_3 play an important role in the construction of a function $f \in \mathcal{B}_{n,3}$ with good GAC.

Note that if $\mathcal{W}_{f_i}(\mathbf{u})\overline{\mathcal{W}_{f_j}(\mathbf{u})} = 0$ for every $\mathbf{u} \in \mathbb{Z}_3^n$, $i \neq j$, $i, j \in \{1, 2, 3\}$, then it follows from Lemma 7.2.1 that $\mathcal{C}_{f_i,f_j}(\mathbf{u}) = 0$ for every $\mathbf{u} \in \mathbb{Z}_3^n$, $i \neq j$, $i, j \in \{1, 2, 3\}$. The functions f_1, f_2 and f_3 are then known as pairwise disjoint spectra functions. In case of Boolean functions, disjoint spectra functions are very useful as they can be used to construct highly nonlinear resilient functions [121]. Therefore, it is important to obtain the functions f_1, f_2 and f_3 with the property such that $\mathcal{C}_{f_i,f_j}(\mathbf{u}) = 0$ for every $\mathbf{u} \in \mathbb{Z}_3^n$, $i \neq j$, $i, j \in \{1, 2, 3\}$. If the functions f_i and f_j for $i \neq j$, $i, j \in \{1, 2, 3\}$ in Theorem 7.4.1 are pairwise perfectly uncorrelated functions, then the SSMI of $f \in \mathcal{B}_{n,3}$ reduces to $\sigma_f = \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3}$.

It is observed that, for the ternary function f as constructed in Theorem 7.4.1, the following statements hold:

(1) $\sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} \leq \sigma_f \leq \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3} + 4(\sigma_{f_1,f_2} + \sigma_{f_2,f_3} + \sigma_{f_1,f_3})$ if $\mathcal{C}_{f_i,f_j}(\mathbf{u})\mathcal{C}_{f_j,f_k}(\mathbf{u}) = 0$

for all $i \neq j, j \neq k$, $i, j, k \in \{1, 2, 3\}$, and

(2) $\sigma_f = \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3}$ if for every $\mathbf{u} \in \mathbb{Z}_3^n$, $\mathcal{C}_{f_i, f_j}(\mathbf{u}) = 0$ for all $i \neq j$, $i, j \in \{1, 2, 3\}$.

7.5 Construction of m-plateaued ternary functions

In this section, first we construct m-plateaued ternary functions with disjoint WHS by using ternary bent functions. Further, we use these functions to construct ternary functions with smaller value of the indicator, the SSMI.

Lemma 7.5.1. *Let $f(\mathbf{x}, \mathbf{y}) = g(\mathbf{x}) + \langle \mathbf{a}, \mathbf{y} \rangle$, where $\mathbf{x} \in \mathbb{Z}_3^{n-m}$, $\mathbf{a}, \mathbf{y} \in \mathbb{Z}_3^m$, and $g(\mathbf{x})$ is a ternary bent function. Then for every $\mathbf{u} \in \mathbb{Z}_3^{n-m}$, $\mathbf{v} \in \mathbb{Z}_3^m$, we have*

$$|\mathcal{W}_f(\mathbf{u}, \mathbf{v})| = \begin{cases} 3^{\frac{m}{2}}, & \text{if } \mathbf{v} = -\mathbf{a}, \\ 0, & \text{if } \mathbf{v} \neq -\mathbf{a}. \end{cases}$$

Therefore, f is a m-plateaued ternary functions and hence $\sigma_f = 3^{2n+m}$.

Proof. For $\mathbf{u} \in \mathbb{Z}_3^{n-m}$ and $\mathbf{v} \in \mathbb{Z}_3^m$, we have

$$\begin{aligned} \mathcal{W}_f(\mathbf{u}, \mathbf{v}) &= \frac{1}{3^{\frac{n}{2}}} \sum_{\mathbf{x} \in \mathbb{Z}_3^{n-m}} \sum_{\mathbf{y} \in \mathbb{Z}_3^m} \omega^{f(\mathbf{x}, \mathbf{y}) + \langle \mathbf{u}, \mathbf{x} \rangle + \langle \mathbf{v}, \mathbf{y} \rangle} \\ &= \frac{1}{3^{\frac{n}{2}}} \sum_{\mathbf{x} \in \mathbb{Z}_3^{n-m}} \omega^{g(\mathbf{x}) + \langle \mathbf{u}, \mathbf{x} \rangle} \sum_{\mathbf{y} \in \mathbb{Z}_3^m} \omega^{\langle \mathbf{a} + \mathbf{v}, \mathbf{y} \rangle} \\ &= 3^{\frac{m}{2}} \mathcal{W}_g(\mathbf{u}) \delta_{\mathbf{0}}(\mathbf{a} + \mathbf{v}) \end{aligned} \tag{7.5.1}$$

$$\begin{aligned} &= \begin{cases} 3^{\frac{m}{2}} \mathcal{W}_g(\mathbf{u}), & \text{if } \mathbf{v} = -\mathbf{a}, \\ 0, & \text{if } \mathbf{v} \neq -\mathbf{a}, \text{ (from Lemma 5.1.1)} \end{cases} \\ \text{i.e., } |\mathcal{W}_f(\mathbf{u}, \mathbf{v})| &= \begin{cases} 3^{\frac{m}{2}}, & \text{if } \mathbf{v} = -\mathbf{a}, \\ 0, & \text{if } \mathbf{v} \neq -\mathbf{a}, \text{ (as } g \text{ is a ternary bent function),} \end{cases} \end{aligned} \tag{7.5.2}$$

which implies that f is a m-plateaued functions. Therefore, it follows from Theorem 6.3.1 that the SSMI of f is $\sigma_f = 3^{2n+m}$. This completes the proof.

■

The following result presents a construction of ternary functions with good value of the SSMI by using m-plateaued ternary functions.

Theorem 7.5.2. *Let* $f_i(\mathbf{x},\mathbf{y}) = g_i(\mathbf{x}) + \langle \mathbf{a}_i, \mathbf{y}\rangle$, $i \in \{1,2,3\}$, *where* $\mathbf{x} \in \mathbb{Z}_3^{n-m}$, $\mathbf{a}_i, \mathbf{y} \in \mathbb{Z}_3^m$, $\mathbf{a}_1 \neq \mathbf{a}_2 \neq \mathbf{a}_3$, *and* $g_i(\mathbf{x})$*'s are ternary bent functions. We construct a function* $f : \mathbb{Z}_3^{n-m} \times \mathbb{Z}_3^m \times \mathbb{Z}_3 \to \mathbb{Z}_3$ *expressed by*

$$f(\mathbf{x},\mathbf{y},x_{n+1}) = \frac{1}{2}\left((1+x_{n+1})(2+x_{n+1})f_1(\mathbf{x},\mathbf{y}) + x_{n+1}(1+x_{n+1})f_2(\mathbf{x},\mathbf{y}) + x_{n+1}(2+x_{n+1})f_3(\mathbf{x},\mathbf{y})\right), \tag{7.5.3}$$

then the SSMI of f *is* $\sigma_f = 3^{2n+m+1}$.

Proof. From Lemma 7.5.1, it follows that the functions f_i, $i \in \{1,2,3\}$ are m-plateaued functions. Further, from Lemma 7.5.1, it follows that $\mathcal{W}_{f_i}(\mathbf{u},\mathbf{v})\mathcal{W}_{f_j}(\mathbf{u},\mathbf{v}) = 0$ for every $\mathbf{u} \in \mathbb{Z}_3^{n-m}$, $\mathbf{v} \in \mathbb{Z}_3^m$, $\mathbf{a}_1 \neq \mathbf{a}_2 \neq \mathbf{a}_3$, and for all $i \neq j, i, j \in \{1,2,3\}$. This implies that for $i \neq j, i, j \in \{1,2,3\}$, f_i and f_j are pairwise disjoint spectra functions and hence pairwise perfectly uncorrelated.

Therefore, by using Theorem 7.4.1 and Lemma 7.5.1, we have

$$\begin{aligned}\sigma_f &= \sigma_{f_1} + \sigma_{f_2} + \sigma_{f_3}\\ &= 3^{2n+m+1}.\end{aligned}$$

This completes the proof. ∎

Chapter 8

Generalized nega-Hadamard transform and negabent functions

8.1 Introduction

Parker and Riera have extended the concept of bent functions to some generalized bent criteria, where Boolean functions are required to have flat spectra with respect to one or more unitary transformations [118,123]. The transforms they have chosen are n-fold tensor products of the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the Walsh-Hadamard matrix $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and the nega-Hadamard matrix $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$ with $i^2 = -1$.

The *nega-Hadamard transform* (NHT) of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is a complex-valued function on $\mathbb{Z}_2^n$ defined as

$$N_f(\mathbf{u}) = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + \langle \mathbf{x}, \mathbf{u} \rangle} i^{w_H(\mathbf{x})}.$$

A function $f \in \mathcal{B}_n$ is said to be *negabent* if $|N_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. The multiset $\{N_f(\mathbf{u}) : \mathbf{u} \in \mathbb{Z}_2^n\}$ is called *nega-Hadamard spectrum* of f.

The sum

$$C_{f,g}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) + g(\mathbf{x}+\mathbf{u})} (-1)^{\langle \mathbf{x}, \mathbf{u} \rangle}$$

is called the *nega-crosscorrelation* between Boolean functions f and g at $\mathbf{u} \in \mathbb{Z}_2^n$. For

$f = g, C_{f,f} = C_f = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{x})+f(\mathbf{x}+\mathbf{u})}(-1)^{\langle \mathbf{x},\mathbf{u}\rangle}$ is called the *nega-autocorrelation* of f at $\mathbf{u}$.

The functions which are both bent and negabent are called *bent-negabent* functions and have got special attention in the literature [119, 123, 132]. In recent years, the constructions of bent-negabent Boolean functions of maximum possible degree have been considered as an important problem. Recently, Parker and Pott [119], Schmidt et al. [132], Stănică et al. [144] and Su et al. [145] have presented several properties and constructions of bent-negabent functions in the Boolean context. For more constructions and various properties of bent-negabent Boolean functions we refer to [86, 118, 123, 132, 144, 145].

In this chapter, we propose a new generalization of negabent functions by considering the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. Let $\mathcal{NB}_{n,q}$ be the set of all such functions. Let $f : \mathbb{Z}_q^n \to \mathbb{Z}_{2q}$ be a function, ξ a primitive q-th root of unity and ω a primitive $2q$-th root of unity. Then, we define the *generalized nega-Hadamard transform* (GNHT) $\mathcal{N}_f(\mathbf{u})$ of f at $\mathbf{u} \in \mathbb{Z}_q^n$ as

$$\mathcal{N}_f(\mathbf{u}) = \frac{1}{q^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})} \xi^{\langle \mathbf{x},\mathbf{u}\rangle} \omega^{\Sigma x_i}.$$

A function $f \in \mathcal{NB}_{n,q}$ is said to be *generalized negabent function* if $|\mathcal{N}_f(\mathbf{u})| = 1$ for every $\mathbf{u} \in \mathbb{Z}_q^n$. The multiset $\{N_f(\mathbf{u}) : \mathbf{u} \in \mathbb{Z}_q^n\}$ is called the generalized *nega-Hadamard spectrum* of f.

We remark that the definition of a negabent function given here is different from the one that is used in the binary case [123]. Our motivation to use this definition stems mainly from the fact that if we define generalized (q-ary) negabent functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ as a natural looking generalization of binary negabent functions as

$$\mathcal{N}'_f(\mathbf{u}) = \frac{1}{q^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})} \xi^{\langle \mathbf{x},\mathbf{u}\rangle} \omega^{\Sigma x_i},$$

then we find it extremely difficult to get functions with flat spectra for $q > 2$ in this setup. In fact, it is an open problem to us whether such functions exist at all for $q > 2$. On the other hand, in the new setup we have proposed, we get many interesting examples of generalized negabent functions for various values of q and n. Also, in this setup affine functions are not

in general negabent, which is a good characteristic from cryptographic point of view, as we require functions as far as possible from the class of affine functions. It may be noted that in the binary case all affine functions are negabent [119].

The sum

$$\mathcal{C}^q_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})}(-1)^{n_q(\mathbf{x},\mathbf{u})},$$

where $n_q(\mathbf{x},\mathbf{u}) = \sum_{i=1}^n \lfloor \frac{x_i+u_i}{q} \rfloor = |\{i : \ x_i + u_i \geq q\}|$, is defined as the *generalized nega-crosscorrelation* between two functions $f, g \in \mathcal{NB}_{n,q}$ at $\mathbf{u} \in \mathbb{Z}_q^n$. The identity $\sum_{i=1}^n \lfloor \frac{x_i+u_i}{q} \rfloor = |\{i : \ x_i + u_i \geq q\}|$ holds in the present case as $x_i + u_i < 2q$ for all $x_i, u_i \in \mathbb{Z}_q$. For $f = g$, the quantity

$$\mathcal{C}^q_f(\mathbf{u}) = \mathcal{C}^q_{f,f}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})-f(\mathbf{x}+\mathbf{u})}(-1)^{n_q(\mathbf{x},\mathbf{u})}$$

is called the *generalized nega-autocorrelation* of f at $\mathbf{u}$.

In the present chapter we investigate several properties of generalized nega-Hadamard transform and its behavior on various combinations of functions. We provide the inverse of nega-Hadamard transform of a function and the nega-Parseval identity in the current setup. Several results regarding generalized negabent functions are provided. We establish a connection between the GNHT of the functions and their nega-autocorrelation spectra. We generalize a result of Schmidt et al. [132, Lemma 1] (obtained for binary case) to $\mathbb{Z}_q$. We present a characterization of generalized (for $q = 4$) negabent functions on $n+1$ variables in terms of their subfunctions on n-variables. Further, some examples of generalized negabent functions for different values of q and n are presented.

8.2 Main results

The following lemma is an important property and will be used frequently in this chapter.

Lemma 8.2.1. *Let* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{Z}_q^n$ *such that* $\mathbf{z} = \mathbf{x} + \mathbf{y}$. *Then*

$$\Sigma z_i = \Sigma x_i + \Sigma y_i - q n_q(\mathbf{x}, \mathbf{y}).$$

Proof. Write $\mathbf{z} = (z_n, \ldots, z_1)$. Then we have

$$\begin{aligned} z_i &= x_i + y_i \pmod{\text{q}} \\ &= (x_i + y_i) - q\lfloor \frac{x_i + y_i}{q} \rfloor \\ \Sigma z_i &= \Sigma x_i + \Sigma y_i - q\Sigma\lfloor \frac{x_i + y_i}{q} \rfloor. \end{aligned}$$

Since $x_i + y_i < 2q$, for $i = 1, 2, \ldots, n$, therefore, we have

$$\lfloor \frac{x_i + y_i}{q} \rfloor = \begin{cases} 1, & \text{if } x_i + y_i \geq q, \\ 0, & \text{otherwise .} \end{cases}$$

Therefore, $\Sigma\lfloor \frac{x_i+y_i}{q} \rfloor = |\{i \ : \ x_i + y_i \geq q\}| = n_q(\mathbf{x}, \mathbf{y})$. The result follows. ∎

The following theorem generalizes a result of Schmidt et al. [132, Lemma 1] (obtained for binary case) over $\mathbb{Z}_q$.

Theorem 8.2.2. *For any $\mathbf{u} \in \mathbb{Z}_q^n$, we have*

$$\sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{\langle \mathbf{u},\ \mathbf{x} \rangle} \omega^{\Sigma x_j} = \frac{1}{\prod_{j=1}^{n} \sin(2u_j + 1)\frac{\pi}{2q}} \eta^{n(q-1) - 2\Sigma u_j},$$

where ξ is a q-th, ω is a $2q$-th and η is a $4q$-th primitive complex roots of unity.

Proof. We compute the sum

$$\begin{aligned} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{\langle \mathbf{u},\ \mathbf{x} \rangle} \omega^{\Sigma x_j} &= \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{\Sigma u_j x_j} \omega^{\Sigma x_j} \\ &= \prod_{j=1}^{n} \sum_{x_j \in \mathbb{Z}_q} \xi^{u_j x_j} \omega^{x_j} \\ &= \prod_{j=1}^{n} \frac{1 - (\omega \xi^{u_j})^q}{1 - \omega \xi^{u_j}} \\ &= \prod_{j=1}^{n} \frac{2}{1 - \omega \xi^{u_j}}. \end{aligned} \tag{8.2.1}$$

Since ξ and ω are q-th and $2q$-th roots of unity respectively, therefore, we obtain

$$\begin{aligned}
1-\omega\xi^{u_j} &= 1-e^{(2u_j+1)\frac{\pi i}{q}} \\
&= 1-\cos(2u_j+1)\frac{\pi}{q}-i\sin(2u_j+1)\frac{\pi}{q} \\
&= 2\sin(2u_j+1)\frac{\pi}{2q}\left[\sin(2u_j+1)\frac{\pi}{2q}-i\cos(2u_j+1)\frac{\pi}{2q}\right] \\
&= 2\sin(2u_j+1)\frac{\pi}{2q}\left[\cos\left(\frac{\pi}{2}-(2u_j+1)\frac{\pi}{2q}\right)-i\sin\left(\frac{\pi}{2}-(2u_j+1)\frac{\pi}{2q}\right)\right] \\
&= 2\sin(2u_j+1)\frac{\pi}{2q}\left[\cos\left((q-1-2u_j)\frac{\pi}{2q}\right)-i\sin\left((q-1-2u_j)\frac{\pi}{2q}\right)\right] \\
&= 2e^{-(q-1-2u_j)\frac{\pi i}{2q}}\sin(2u_j+1)\frac{\pi}{2q}. \qquad (8.2.2)
\end{aligned}$$

It follows from (8.2.2) that

$$\begin{aligned}
\frac{2}{1-\omega\xi^{u_j}} &= \frac{1}{\sin(2u_j+1)\frac{\pi}{2q}}e^{(q-1-2u_j)\frac{\pi i}{2q}} \\
&= \frac{1}{\sin(2u_j+1)\frac{\pi}{2q}}\eta^{(q-1-2u_j)}. \qquad (8.2.3)
\end{aligned}$$

Hence, from (8.2.1) and (8.2.3), we have

$$\begin{aligned}
\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\xi^{\langle \mathbf{u},\ \mathbf{x}\rangle}\omega^{\Sigma x_j} &= \prod_{j=1}^{n}\frac{2}{1-\omega\xi^{u_j}} \\
&= \prod_{j=1}^{n}\frac{1}{\sin(2u_j+1)\frac{\pi}{2q}}\eta^{(q-1-2u_j)} \\
&= \frac{1}{\prod_{j=1}^{n}\sin(2u_j+1)\frac{\pi}{2q}}\eta^{n(q-1)-2\Sigma u_j}.
\end{aligned}$$

Hence the result. ∎

Remark 8.2.3. *In the binary case ($q=2$), $\prod_{j=1}^{n}\sin(2u_j+1)\frac{\pi}{2q}=\prod_{j=1}^{n}\sin(2u_j+1)\frac{\pi}{4}=\frac{1}{2^{n/2}}$, as $\sin(2u_j+1)\frac{\pi}{4}=\frac{1}{\sqrt{2}}$ for $u_j\in\{0,1\}$. However, for $q>2$, the product $\prod_{j=1}^{n}\sin(2u_j+1)\frac{\pi}{2q}$ depends on the values of u_j and in general not a constant.*

8.3 Properties of generalized nega-Hadamard transform

In this section, we have presented several properties of generalized nega-Hadamard transform regarding its behavior on various combinations of the functions in $\mathcal{NB}_{n,q}$.

Like in the Boolean case [119], the generalized nega-Hadamard transformation is also an unitary transformation. In the following result, we provide the inverse of generalized nega-Hadamard transform of a function $f \in \mathcal{NB}_{n,q}$.

Lemma 8.3.1. *Let $f \in \mathcal{NB}_{n,q}$. Then for all $\mathbf{x} \in \mathbb{Z}_q^n$, we have*

$$\omega^{f(\mathbf{x})} = q^{\frac{-n}{2}} \omega^{-\Sigma x_i} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \mathcal{N}_f(\mathbf{u}) \xi^{\langle -\mathbf{u}, \mathbf{x} \rangle}.$$

Proof. By using Lemma 5.1.1, we have

$$\begin{aligned}
\sum_{\mathbf{u} \in \mathbb{Z}_q^n} \mathcal{N}_f(\mathbf{u}) \xi^{\langle -\mathbf{u}, \mathbf{x} \rangle} &= q^{\frac{-n}{2}} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{f(\mathbf{y})} \xi^{\langle \mathbf{u}, \mathbf{y} \rangle} \omega^{\Sigma y_i} \xi^{\langle -\mathbf{u}, \mathbf{x} \rangle} \\
&= q^{\frac{-n}{2}} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{f(\mathbf{y})} \omega^{\Sigma y_i} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \xi^{\langle \mathbf{u}, -\mathbf{x} + \mathbf{y} \rangle} \\
&= q^{\frac{n}{2}} \omega^{\Sigma x_i} \omega^{f(\mathbf{x})}, \\
\text{which implies that, } \omega^{f(\mathbf{x})} &= q^{\frac{-n}{2}} \omega^{-\Sigma x_i} \sum_{\mathbf{u} \in \mathbb{Z}_q^n} \mathcal{N}_f(\mathbf{u}) \xi^{\langle -\mathbf{u}, \mathbf{x} \rangle}.
\end{aligned}$$

■

In the next result, we show that the conservation law for the GNHT values of $f \in \mathcal{NB}_{n,q}$ holds, which we call the *generalized nega-Parseval's identity* in the current setup, according to which the sum of squares of GNHT values is constant.

Theorem 8.3.2. *Let $f \in \mathcal{NB}_{n,q}$. Then*

$$\sum_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{N}_f(\mathbf{u})|^2 = q^n.$$

Proof. We have

$$\begin{aligned}
\sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{N}_f(\mathbf{u})|^2 &= \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_f(\mathbf{u})} \\
&= \frac{1}{q^n} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})} \xi^{\langle \mathbf{u},\mathbf{x}\rangle} \omega^{\Sigma x_i} \overline{\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{y})} \xi^{\langle \mathbf{u},\mathbf{y}\rangle} \omega^{\Sigma y_i}} \\
&= \frac{1}{q^n} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})-f(\mathbf{y})} \xi^{\langle \mathbf{u},\mathbf{x}-\mathbf{y}\rangle} \omega^{\Sigma x_i - \Sigma y_i} \\
&= \frac{1}{q^n} \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})-f(\mathbf{y})} \omega^{\Sigma x_i - \Sigma y_i} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{\langle \mathbf{u},\mathbf{x}-\mathbf{y}\rangle} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})-f(\mathbf{x})} = q^n.
\end{aligned}$$

■

In the following result, we investigate a relationship between generalized nega-Hadamard transforms of $f, g \in \mathcal{NB}_{n,q}$ and their generalized nega-crosscorrelation.

Theorem 8.3.3. *If $f, g \in \mathcal{NB}_{n,q}$ and $\mathbf{u}, \mathbf{z} \in \mathbb{Z}_q^n$, then*

$$\sum_{\mathbf{z}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}^q(\mathbf{z}) \omega^{-\Sigma z_i} \xi^{\langle -\mathbf{u},\mathbf{z}\rangle} = q^n \mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_g(\mathbf{u})}, \text{ and}$$

$$\mathcal{C}_{f,g}^q(\mathbf{z}) = \omega^{\Sigma z_i} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_g(\mathbf{u})} \ \ \xi^{\langle \mathbf{u},\ \mathbf{z}\rangle}.$$

Proof. By the definition of generalized nega-Hadamard transform, we have

$$\begin{aligned}
\mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_g(\mathbf{u})} &= \frac{1}{q^n} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})} \xi^{\langle \mathbf{u},\mathbf{x}\rangle} \omega^{\Sigma x_i} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \omega^{-g(\mathbf{y})} \xi^{-\langle \mathbf{u},\mathbf{y}\rangle} \omega^{-\Sigma y_i} \\
&= \frac{1}{q^n} \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})-g(\mathbf{y})} \xi^{\langle \mathbf{u},\mathbf{x}\rangle - \langle \mathbf{u},\mathbf{y}\rangle} \omega^{\Sigma x_i - \Sigma y_i} \\
&= \frac{1}{q^n} \sum_{\mathbf{x},\mathbf{z}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{z})} \xi^{\langle \mathbf{u},\mathbf{x}\rangle - \langle \mathbf{u},\mathbf{x}+\mathbf{z}\rangle} \omega^{-\Sigma z_i + q n_q(\mathbf{x},\mathbf{z})} \\
&= \frac{1}{q^n} \sum_{\mathbf{x},\mathbf{z}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{z})} (-1)^{n_q(\mathbf{x},\mathbf{z})} \xi^{\langle -\mathbf{u},\mathbf{z}\rangle} \omega^{-\Sigma z_i} \\
&= \frac{1}{q^n} \sum_{\mathbf{z}\in\mathbb{Z}_q^n} \omega^{-\Sigma z_i} \mathcal{C}_{f,g}^q(\mathbf{z}) \xi^{\langle -\mathbf{u},\mathbf{z}\rangle}.
\end{aligned}$$

Then it follows that

$$\begin{aligned}\omega^{\Sigma z_i}\sum_{\mathbf{u}\in\mathbb{Z}_q^n}\mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_g(\mathbf{u})}\xi^{\langle\mathbf{u},\mathbf{z}\rangle} &= \frac{1}{q^n}\omega^{\Sigma z_i}\sum_{\mathbf{u}\in\mathbb{Z}_q^n}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\omega^{-\Sigma x_i}\mathcal{C}_{f,g}^q(\mathbf{x})\xi^{\langle\mathbf{u},-\mathbf{x}+\mathbf{z}\rangle}\\ &= \frac{1}{q^n}\omega^{\Sigma z_i}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\omega^{-\Sigma x_i}\mathcal{C}_{f,g}^q(\mathbf{x})\sum_{\mathbf{u}\in\mathbb{Z}_q^n}\xi^{\langle\mathbf{u},-\mathbf{x}+\mathbf{z}\rangle}\\ &= \mathcal{C}_{f,g}^q(\mathbf{z}). \qquad (8.3.1)\end{aligned}$$

■

In particular, if $f = g$ in (8.3.1), then we have

$$\mathcal{C}_f^q(\mathbf{z}) = \omega^{\Sigma z_i}\sum_{\mathbf{u}\in\mathbb{Z}_q^n}|\mathcal{N}_f(\mathbf{u})|^2\xi^{\langle\mathbf{u},\ \mathbf{z}\rangle}. \qquad (8.3.2)$$

By putting $\mathbf{z} = \mathbf{0}$ in (8.3.2), we obtain $\sum_{\mathbf{u}\in\mathbb{Z}_q^n}|\mathcal{N}_f(\mathbf{u})|^2 = q^n$, which is the generalized nega-Parseval's identity.

Corollary 8.3.4. *A function $f \in \mathcal{NB}_{n,q}$ is generalized negabent if and only if $\mathcal{C}_f^q(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n \setminus \{0\}$.*

Proof. The proof follows from Lemma 5.1.1 and (8.3.2). ■

8.4 Characterizations of generalized negabent functions

Recall that, for any fixed $\mathbf{v} = (v_r, \ldots, v_1)$ with $1 \le r \le n$ and $f \in \mathcal{NB}_{n,q}$, the restriction $f_{\mathbf{v}}$ of f is

$$f_{\mathbf{v}}(x_{n-r}, \ldots, x_1) = f(v_r, \ldots, v_1, x_{n-r}, \ldots, x_1).$$

Also recall that the concatenation of two vectors $\mathbf{u} = (u_r, \ldots, u_1) \in \mathbb{Z}_q^r$ and $\mathbf{w} = (w_{n-r}, \ldots, w_1) \in \mathbb{Z}_q^{n-r}$ the vector $\mathbf{uw} = (\mathbf{u}, \mathbf{w}) = (u_r, \ldots, u_1, w_{n-r}, \ldots, w_1)$.

Lemma 8.4.1. *Let* $\mathbf{u} \in \mathbb{Z}_q^r$, $\mathbf{w} \in \mathbb{Z}_q^{n-r}$ *and* $f \in \mathcal{NB}_{n,q}$. *Then the generalized nega-autocorrelation of* f *is given by*

$$\mathcal{C}_f^q(\mathbf{uw}) = \sum_{\mathbf{v}\in\mathbb{Z}_q^r} \mathcal{C}^q_{f_\mathbf{v}, f_{\mathbf{v}+\mathbf{u}}}(\mathbf{w})(-1)^{n_q(\mathbf{u},\mathbf{v})}.$$

Proof. We have

$$\begin{aligned}\mathcal{C}_f^q(\mathbf{uw}) &= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \omega^{f(\mathbf{x})-f(\mathbf{x}+\mathbf{uw})}(-1)^{n_q(\mathbf{uw},\mathbf{x})} \\ &= \sum_{\mathbf{v}\in\mathbb{Z}_q^r}\sum_{\mathbf{z}\in\mathbb{Z}_q^{n-r}} \omega^{f(\mathbf{vz})-f(\mathbf{vz}+\mathbf{uw})}(-1)^{n_q(\mathbf{uw},\mathbf{vz})},\end{aligned}$$

where $\mathbf{x} \in \mathbb{Z}_q^n$ can be considered as the vector concatenation of $\mathbf{v} \in \mathbb{Z}_q^r$ and $\mathbf{z} \in \mathbb{Z}_q^{n-r}$. Also, for a fixed $\mathbf{v}$, we have $f(\mathbf{vz}) = f_\mathbf{v}(\mathbf{z})$ and $f(\mathbf{vz}+\mathbf{uw}) = f_{\mathbf{v}+\mathbf{u}}(\mathbf{z}+\mathbf{w})$. Then

$$\begin{aligned}\mathcal{C}_f^q(\mathbf{uw}) &= \sum_{\mathbf{v}\in\mathbb{Z}_q^r}\sum_{\mathbf{z}\in\mathbb{Z}_q^{n-r}} \omega^{f_\mathbf{v}(\mathbf{z})-f_{\mathbf{v}+\mathbf{u}}(\mathbf{z}+\mathbf{w})}(-1)^{n_q(\mathbf{u},\mathbf{v})+n_q(\mathbf{w},\mathbf{z})} \\ &= \sum_{\mathbf{v}\in\mathbb{Z}_q^r}(-1)^{n_q(\mathbf{u},\mathbf{v})}\sum_{\mathbf{z}\in\mathbb{Z}_q^{n-r}} \omega^{f_\mathbf{v}(\mathbf{z})-f_{\mathbf{v}+\mathbf{u}}(\mathbf{z}+\mathbf{w})}(-1)^{n_q(\mathbf{w},\mathbf{z})} \\ &= \sum_{\mathbf{v}\in\mathbb{Z}_q^r} \mathcal{C}^q_{f_\mathbf{v}, f_{\mathbf{v}+\mathbf{u}}}(\mathbf{w})(-1)^{n_q(\mathbf{u},\mathbf{v})}.\end{aligned}$$

■

Two functions $f, g \in \mathcal{NB}_{n,q}$ are said to have *complementary generalized nega-autocorrelation* if for all $\mathbf{u} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}\}$, $\mathcal{C}_f^q(\mathbf{u}) + \mathcal{C}_g^q(\mathbf{u}) = 0$.

In the following theorem, we provide a relationship between the GNHT of $f, g \in \mathbb{Z}_q^n$ and their generalized nega-autocorrelations.

Theorem 8.4.2. *The functions* $f, g \in \mathcal{NB}_{n,q}$ *have complementary generalized nega-autocorrelation if and only if*

$$|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2 \quad \textit{for all } \mathbf{u} \in \mathbb{Z}_q^n.$$

Proof. Let the functions $f, g \in \mathbb{Z}_q^n$ have complementary generalized nega-autocorrelation.

Then by taking $f = g$ in (8.3.1), we get

$$q^n(|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2) = \sum_{\mathbf{z}\in\mathbb{Z}_q^n} (\mathcal{C}_f^q(\mathbf{z}) + \mathcal{C}_g^q(\mathbf{z}))\omega^{-\Sigma z_i}\xi^{\langle -\mathbf{u},\mathbf{z}\rangle} = 2q^n,$$

which implies, $|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{Z}_q^n$.

Conversely, suppose that $|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{Z}_q^n$. Then

$$\begin{aligned}\mathcal{C}_f^q(\mathbf{z}) + \mathcal{C}_g^q(\mathbf{z}) &= \omega^{\Sigma z_i} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} (|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2)\xi^{\langle \mathbf{u},\mathbf{z}\rangle} \\ &= 2\omega^{\Sigma z_i} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{\langle \mathbf{u},\mathbf{z}\rangle} \\ &= 2q^n\delta_{\mathbf{0}}(\mathbf{z}).\end{aligned}$$

Therefore, for all $\mathbf{z} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}\}$ we have, $\mathcal{C}_f^q(\mathbf{z}) + \mathcal{C}_g^q(\mathbf{z}) = 0$. Hence, the functions f and g have complementary generalized nega-autocorrelations. ■

In the following result, we show that for arbitrary positive integers r, s and q the direct sum of two generalized negabent functions is generalized negabent.

Theorem 8.4.3. *Let $f_1 \in \mathcal{NB}_{r,q}$ and $f_2 \in \mathcal{NB}_{s,q}$. Then a function $f \in \mathcal{NB}_{r+s,q}$ expressed as*

$$f(x_{r+s}, \ldots, x_{r+1}, x_r, \ldots, x_1) = f_1(x_r, \ldots, x_1) + f_2(x_{r+s}, \ldots, x_{r+1}),$$

is generalized negabent if and only if f_1 and f_2 both are generalized negabent functions.

Proof. Let $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^r \times \mathbb{Z}_q^s$. Then

$$\begin{aligned}\mathcal{N}_f(\mathbf{u}, \mathbf{v}) &= \frac{1}{q^{\frac{(r+s)}{2}}} \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{Z}_q^r\times\mathbb{Z}_q^s} \omega^{f(\mathbf{x},\mathbf{y})}\xi^{\langle \mathbf{u},\mathbf{x}\rangle+\langle \mathbf{v},\mathbf{y}\rangle}\omega^{\Sigma x_i+\Sigma y_i} \\ &= \frac{1}{q^{\frac{r}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_q^r} \omega^{f_1(\mathbf{x})}\xi^{\langle \mathbf{u},\mathbf{x}\rangle}\omega^{\Sigma x_i} \frac{1}{q^{\frac{s}{2}}} \sum_{\mathbf{y}\in\mathbb{Z}_q^s} \omega^{f_2(\mathbf{y})}\xi^{\langle \mathbf{v},\mathbf{y}\rangle}\omega^{\Sigma y_i} \\ &= \mathcal{N}_{f_1}(\mathbf{u})\mathcal{N}_{f_2}(\mathbf{v}).\end{aligned}$$

Suppose f_1 and f_2 both are generalized negabent. Then $|\mathcal{N}_{f_1}(\mathbf{u})| = 1$ and $|\mathcal{N}_{f_2}(\mathbf{v})| = 1$. This implies that, $|\mathcal{N}_f(\mathbf{u}, \mathbf{v})| = |\mathcal{N}_{f_1}(\mathbf{u})||\mathcal{N}_{f_2}(\mathbf{v})| = 1$ for all $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^r \times \mathbb{Z}_q^s$. Hence f is a

generalized negabent function.

Conversely, suppose that f is a generalized negabent function. We claim that f_1 and f_2 are generalized negabent functions. Let us suppose that f_1 is not generalized negabent function. Then there exists $\mathbf{u} \in \mathbb{Z}_q^r$ such that $|\mathcal{N}_{f_1}(\mathbf{u})| > 1$. This implies that $|\mathcal{N}_{f_2}(\mathbf{v})| < 1$ for every $\mathbf{v} \in \mathbb{Z}_q^s$, as $|\mathcal{N}_{f_1}(\mathbf{u})||\mathcal{N}_{f_2}(\mathbf{v})| = 1$. This contradicts the fact that $\sum_{\mathbf{v}\in\mathbb{Z}_q^s} |\mathcal{N}_{f_2}(\mathbf{v})|^2 = q^s$. Therefore f_1 is a generalized negabent function. Similarly, f_2 is also a generalized negabent function. ∎

8.4.1 Characterization of generalized negabent functions in $\mathcal{NB}_{n+1,4}$ from the functions in $\mathcal{NB}_{n,4}$

In this subsection we provide a characterization of generalized negabent functions for $q = 4$ on $n + 1$ variables in terms of its subfunctions on n variables.

Theorem 8.4.4. *A function $h \in \mathcal{NB}_{n+1,4}$ expressed as*

$$h(x_{n+1}, x_n, \ldots, x_1) = (1 + x_{n+1})f(x_n, \ldots, x_1) + x_{n+1}g(x_n, \ldots, x_1),$$

where $f, g \in \mathcal{NB}_{n,4}$, is generalized negabent if and only if

(i) $|\sum_{j=0}^{3} \omega^j \mathcal{N}_{h_j}(\mathbf{u})| = 2$ *for all* $\mathbf{u} \in \mathbb{Z}_4^n$, *where* $\omega = (1+\imath)/\sqrt{2}$ *is a primitive 8-th root of unity.*

(ii) $\frac{\mathcal{N}_{h_0}(\mathbf{u})-\omega^2\mathcal{N}_{h_2}(\mathbf{u})}{\omega\mathcal{N}_{h_1}(\mathbf{u})-\omega^3\mathcal{N}_{h_3}(\mathbf{u})} = \phi(\mathbf{u})$ *and* $\frac{\mathcal{N}_{h_0}(\mathbf{u})+\omega^2\mathcal{N}_{h_2}(\mathbf{u})}{\omega\mathcal{N}_{h_1}(\mathbf{u})+\omega^3\mathcal{N}_{h_3}(\mathbf{u})} = \imath\psi(\mathbf{u})$, $\phi(\mathbf{u}), \psi(\mathbf{u}) \in \mathbb{R}$.

(iii) $\sum_{j=0}^{3} |\mathcal{N}_{h_j}(\mathbf{u})|^2 = 4$ *for all* $\mathbf{u} \in \mathbb{Z}_4^n$, *and* $\overline{\mathcal{N}_{h_0}(\mathbf{u})}\mathcal{N}_{h_2}(\mathbf{u}) - \mathcal{N}_{h_0}(\mathbf{u})\overline{\mathcal{N}_{h_2}(\mathbf{u})} + \overline{\mathcal{N}_{h_1}(\mathbf{u})}\mathcal{N}_{h_3}(\mathbf{u}) - \mathcal{N}_{h_1}(\mathbf{u})\overline{\mathcal{N}_{h_3}(\mathbf{u})} = 0$.

Proof. We identify $(x_{n+1}, x_n, \ldots, x_1) \in \mathbb{Z}_4^{n+1}$ with $(x_{n+1}, \mathbf{x}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$. Let

$$h(x_{n+1}, \mathbf{x}) = (1 + x_{n+1})f(\mathbf{x}) + x_{n+1}g(\mathbf{x})$$

is a generalized negabent function. The GNHT of h at $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$ is given by

$$\begin{aligned}\mathcal{N}_h(a,\mathbf{u}) &= \frac{1}{4^{\frac{n+1}{2}}} \sum_{(x_{n+1},\mathbf{x})\in\mathbb{Z}_4\times\mathbb{Z}_4^n} \omega^{h(x_{n+1},\mathbf{x})} \imath^{ax_{n+1}+\langle \mathbf{u},\ \mathbf{x}\rangle} \omega^{\Sigma x_i + x_{n+1}} \\ &= \frac{1}{2^{n+1}} \sum_{j=0}^{3} \sum_{\mathbf{x}\in\mathbb{Z}_4^n} \omega^{h_j(\mathbf{x})} \imath^{aj+\langle \mathbf{u},\ \mathbf{x}\rangle} \omega^{\Sigma x_i + j} \\ &= \frac{1}{2} \sum_{j=0}^{3} \imath^{aj} \omega^j \mathcal{N}_{h_j}(\mathbf{u}) \\ &= \frac{1}{2}(\mathcal{N}_{h_0}(\mathbf{u}) + \imath^a \omega \mathcal{N}_{h_1}(\mathbf{u}) + (-1)^a \omega^2 \mathcal{N}_{h_2}(\mathbf{u}) + (-\imath)^a \omega^3 \mathcal{N}_{h_3}(\mathbf{u})),\end{aligned} \tag{8.4.1}$$

where $h_j(x_n, \cdots, x_1) = h(j, x_n, \cdots, x_1)$ for every $j \in \mathbb{Z}_4$.

Since h is a generalized negabent function so, $|\mathcal{N}_h(a, \mathbf{u})| = 1$ for all $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$. This implies that

$$|\mathcal{N}_{h_0}(\mathbf{u}) + \omega\mathcal{N}_{h_1}(\mathbf{u}) + \omega^2\mathcal{N}_{h_2}(\mathbf{u}) + \omega^3\mathcal{N}_{h_3}(\mathbf{u})| = 2. \tag{8.4.2}$$

$$|\mathcal{N}_{h_0}(\mathbf{u}) - \omega^2\mathcal{N}_{h_2}(\mathbf{u}) + \imath(\omega\mathcal{N}_{h_1}(\mathbf{u}) - \omega^3\mathcal{N}_{h_3}(\mathbf{u}))| = 2. \tag{8.4.3}$$

$$|\mathcal{N}_{h_0}(\mathbf{u}) - \omega\mathcal{N}_{h_1}(\mathbf{u}) + \omega^2\mathcal{N}_{h_2}(\mathbf{u}) - \omega^3\mathcal{N}_{h_3}(\mathbf{u})| = 2. \tag{8.4.4}$$

$$|\mathcal{N}_{h_0}(\mathbf{u}) - \omega^2\mathcal{N}_{h_2}(\mathbf{u}) - \imath(\omega\mathcal{N}_{h_1}(\mathbf{u}) - \omega^3\mathcal{N}_{h_3}(\mathbf{u}))| = 2. \tag{8.4.5}$$

Let $\frac{\mathcal{N}_{h_0}(\mathbf{u})+\omega^2\mathcal{N}_{h_2}(\mathbf{u})}{\omega\mathcal{N}_{h_1}(\mathbf{u})+\omega^3\mathcal{N}_{h_3}(\mathbf{u})} = \rho(\mathbf{u})$ (say), where $\omega\mathcal{N}_{h_1}(\mathbf{u}) + \omega^3\mathcal{N}_{h_3}(\mathbf{u}) \neq 0$.

On combining (8.4.2) and (8.4.4), we get $\rho(\mathbf{u}) = -\overline{\rho(\mathbf{u})}$, which implies that $\rho(\mathbf{u})$ is purely imaginary, i.e.,

$$\rho(\mathbf{u}) = \imath\psi(\mathbf{u}), \text{ where } \psi(\mathbf{u}) \in \mathbb{R}. \tag{8.4.6}$$

Similarly, on combining (8.4.3) and (8.4.5), we obtain that

$$\frac{\mathcal{N}_{h_0}(\mathbf{u}) - \omega^2\mathcal{N}_{h_2}(\mathbf{u})}{\omega\mathcal{N}_{h_1}(\mathbf{u}) - \omega^3\mathcal{N}_{h_3}(\mathbf{u})} = \phi(\mathbf{u}), \text{where } \phi(\mathbf{u}) \in \mathbb{R}. \tag{8.4.7}$$

On solving (8.4.3) and (8.4.7), we get

$$\begin{aligned} |\omega\mathcal{N}_{h_1}(\mathbf{u}) - \omega^3\mathcal{N}_{h_3}(\mathbf{u})|^2 \,|(\imath + \phi(\mathbf{u}))|^2 &= 4 \\ i.e., |\omega\mathcal{N}_{h_1}(\mathbf{u}) - \omega^3\mathcal{N}_{h_3}(\mathbf{u})|^2 \left(1 + \phi(\mathbf{u})^2\right) &= 4 \\ i.e., \left|\mathcal{N}_{h_0}(\mathbf{u}) - \omega^2\mathcal{N}_{h_2}(\mathbf{u})\right|^2 + \left|\omega\mathcal{N}_{h_1}(\mathbf{u}) - \omega^3\mathcal{N}_{h_3}(\mathbf{u})\right|^2 &= 4. \end{aligned} \tag{8.4.8}$$

Similarly, from (8.4.4) and (8.4.6), we obtain

$$\left|\mathcal{N}_{h_0}(\mathbf{u}) + \omega^2\mathcal{N}_{h_2}(\mathbf{u})\right|^2 + \left|\omega\mathcal{N}_{h_1}(\mathbf{u}) + \omega^3\mathcal{N}_{h_3}(\mathbf{u})\right|^2 = 4. \tag{8.4.9}$$

On combing (8.4.8) and (8.4.9), we obtain

$$\overline{\mathcal{N}_{h_0}(\mathbf{u})}\mathcal{N}_{h_2}(\mathbf{u}) - \mathcal{N}_{h_0}(\mathbf{u})\overline{\mathcal{N}_{h_2}(\mathbf{u})} + \overline{\mathcal{N}_{h_1}(\mathbf{u})}\mathcal{N}_{h_3}(\mathbf{u}) - \mathcal{N}_{h_1}(\mathbf{u})\overline{\mathcal{N}_{h_3}(\mathbf{u})} = 0,$$

and $\sum_{j=0}^{3} |\mathcal{N}_{h_j}(\mathbf{u})|^2 = 4$.

Conversely, we assume that the conditions (i), (ii) and (iii) are true. Condition (ii) implies that the terms $\mathcal{N}_{h_0}(\mathbf{u}) - \omega^2\mathcal{N}_{h_2}(\mathbf{u})$ and $\omega\mathcal{N}_{h_1}(\mathbf{u}) - \omega^3\mathcal{N}_{h_3}(\mathbf{u})$ (as well as $\mathcal{N}_{h_0}(\mathbf{u}) + \omega^2\mathcal{N}_{h_2}(\mathbf{u})$ and $\omega\mathcal{N}_{h_1}(\mathbf{u}) + \omega^3\mathcal{N}_{h_3}(\mathbf{u})$) cannot be zero simultaneously. If $\mathcal{N}_{h_0}(\mathbf{u}) - \imath\mathcal{N}_{h_2}(\mathbf{u}) = 0$, then $|\mathcal{N}_{h_1}(\mathbf{u}) - \imath\mathcal{N}_{h_3}(\mathbf{u})| = 2$ (resp. if $\mathcal{N}_{h_0}(\mathbf{u}) + \imath\mathcal{N}_{h_2}(\mathbf{u}) = 0$, then $|\mathcal{N}_{h_1}(\mathbf{u}) + \imath\mathcal{N}_{h_3}(\mathbf{u})| = 2$). Now consider the case when $|\mathcal{N}_{h_0}(\mathbf{u}) - \imath\mathcal{N}_{h_2}(\mathbf{u})|\,|\mathcal{N}_{h_1}(\mathbf{u}) - \imath\mathcal{N}_{h_3}(\mathbf{u})| = 0$ and $|\mathcal{N}_{h_0}(\mathbf{u}) + \imath\mathcal{N}_{h_2}(\mathbf{u})|\,|\mathcal{N}_{h_1}(\mathbf{u}) + \imath\mathcal{N}_{h_3}(\mathbf{u})| = 0$.

Let $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$ be arbitrary. Condition (i) implies that $|\mathcal{N}_h(0, \mathbf{u})| = 1$.

Using condition (ii) and (iii) we have

$$\begin{aligned} 4\,|\mathcal{N}_h(1, \mathbf{u})|^2 &= |\mathcal{N}_{h_0}(\mathbf{u}) - \omega^2\mathcal{N}_{h_2}(\mathbf{u}) + \imath(\omega\mathcal{N}_{h_1}(\mathbf{u}) - \omega^3\mathcal{N}_{h_3}(\mathbf{u}))|^2 \\ &= |\mathcal{N}_{h_1}(\mathbf{u}) - \imath\mathcal{N}_{h_3}(\mathbf{u})|^2|\phi(\mathbf{u}) + \imath|^2 = |\mathcal{N}_{h_1}(\mathbf{u}) - \imath\mathcal{N}_{h_3}(\mathbf{u})|^2 \left(1 + \phi^2(\mathbf{u})\right) \\ &= \left(|\mathcal{N}_{h_0}(\mathbf{u}) - i\mathcal{N}_{h_2}(\mathbf{u})|^2 + |\mathcal{N}_{h_1}(\mathbf{u}) - i\mathcal{N}_{h_3}(\mathbf{u})|^2\right) \\ &= \sum_{j=1}^{3} |\mathcal{N}_{h_j}(\mathbf{u})|^2 - \Big(\overline{\mathcal{N}_{h_0}(\mathbf{u})}\mathcal{N}_{h_2}(\mathbf{u}) - \mathcal{N}_{h_0}(\mathbf{u})\overline{\mathcal{N}_{h_2}(\mathbf{u})} + \overline{\mathcal{N}_{h_1}(\mathbf{u})}\mathcal{N}_{h_3}(\mathbf{u}) \\ &\quad -\mathcal{N}_{h_1}(\mathbf{u})\overline{\mathcal{N}_{h_3}(\mathbf{u})}\Big) = 4, \end{aligned}$$

which implies that $|\mathcal{N}_h(1, \mathbf{u})| = 1$.

Similarly for $a = 2, 3$ it follows from condition (ii) and (iii) that $|\mathcal{N}_h(a, \mathbf{u})| = 1$. Therefore, $|\mathcal{N}_h(a, \mathbf{u})| = 1$ for all $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$. Hence the result. ∎

8.5 Examples

In this section, we present some examples of generalized negabent functions.

Example 8.5.1. *Let $f \in \mathcal{NB}_{2,3}$ such that $f(x_2, x_1) = 2x_1x_2 + x_1$. Then the GNHT of f at $(u_2, u_1) \in \mathbb{Z}_3^2$ is*

$$\begin{aligned}\mathcal{N}_f(u_2, u_1) &= \frac{1}{3^{1/2}} \sum_{(x_2,x_1)\in\mathbb{Z}_3^2} \omega^{2x_1x_2+x_1} \xi^{u_1x_1+u_2x_2} \omega^{x_1+x_2} \\ &= \frac{1}{3^{1/2}} \sum_{x_1,x_2\in\mathbb{Z}_3} \omega^{2x_1x_2+2x_1+x_2+2u_1x_1+2u_2x_2} \\ &= \frac{1}{3^{1/2}} \left(1 + \omega^{1+2u_2} + \omega^{2+4u_2} + \omega^{2+2u_1} + \omega^{5+2u_1+2u_2} + \omega^{8+2u_1+4u_2} + \omega^{4+4u_1}\right. \\ &\quad \left. + \omega^{9+4u_1+u_2} + \omega^{14+4u_1+4u_2}\right).\end{aligned} \tag{8.5.1}$$

Since $u_1, u_2 \in \mathbb{Z}_3$, therefore, from (8.5.1)*, we obtain*

$$\mathcal{N}_f(u_2, u_1) = \frac{1}{3^{1/2}} \text{ for every } (u_2, u_1) \in \mathbb{Z}_3^2.$$

Therefore, f is a generalized negabent function.

Given below are some more examples of generalized negabent functions.

1. $f(x_3, x_2, x_1) = x_1^2 + x_2^2 + x_3^2$ is a generalized negabent function on 3 variables for q an odd integer.

2. $f(x_4, x_3, x_2, x_1) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is a generalized negabent function on 4 variables for q an odd integer.

3. $f(x_4, x_3, x_2, x_1) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2x_1x_2 + 2x_3x_4 + 2x_2x_4$ is a generalized negabent function on 4 variables for $q = 2, 3, 5, 7, 9, \ldots$.

4. $f(x) = x^2 + x$ is a generalized negabent function on one variable for $q = 2, 4, 6, 8, \ldots$.

5. $f(x) = 2x^2 + x$ is a generalized negabent function on one variable for $q = 3, 5, 7, \ldots$.

6. $f(x) = 2x^4 + x^2$ is a generalized negabent function on one variable for $q = 9, 27, 81, \ldots$.

7. $f(x) = 2x^4 + 2x^3 + 2x^2 + x$ is a generalized negabent function on one variable for $q = 3, 4, 12$.

8. $f(x_2, x_1) = x_1^3 + 2x_1x_2 + 2x_2^2$ is a generalized negabent function on two variables for $q = 2$ and 3.

9. $f(x_2, x_1) = x_1^3 + 2x_1x_2 + x_2^2$ is a generalized negabent function on two variables for $q = 2, 3, 9, 27, 81, \ldots$.

10. $f(x_2, x_1) = 2x_1x_2^2 + 2x_1^2x_2 + 2x_1^2 + 2x_2^2 + x_1 + x_2$ is generalized negabent function on two variable for $q = 4$.

Chapter 9

Conclusion

In this thesis, we investigate several cryptographic properties of Boolean functions, q-ary functions defined from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, and the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. Using Carlet's recursive approach [15] we identify some classes of Boolean functions with high nonlinearity whose lower bounds on second order nonlinearities are better than some existing general bounds. We investigate several properties of q-ary functions in terms of their WHT, autocorrelation and crosscorrelation spectra. Several primary as well as secondary constructions of q-ary balanced functions which satisfy various important cryptographic criteria are presented. We propose a new generalization of negabent functions for the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. We present various properties of generalized negabent functions and provide several examples of generalized negabent functions.

In **Chapter** 3 we consider the problem of computing lower bounds on second order nonlinearities of cubic monomial functions of the form (i) $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$, where $n = 3r,\ 5r$ and $\lambda \in \mathbb{Z}_{2^n} \setminus \{0\}$, (ii) $f(x) = tr_1^n(\lambda x^{2^{2r}+2^r+1})$, where $n = 3r$ and $\lambda \in \mathbb{Z}_{2^r} \setminus \{0\}$.

Boolean functions in the above classes possess no affine derivative. It is observed that the bounds obtained by us for the above classes of functions are better than Carlet's [15] general bounds and the bounds of some other classes of functions which are recently studied [50,53,147]. Further, we obtain lower bounds on second-order nonlinearities for some classes of cubic Boolean functions based on secondary constructions.

In **Chapter 4** using the approach proposed by Gao et al. [52], we provide some new constructions of highly nonlinear resilient Boolean functions on large number of variables

with disjoint spectra by concatenating disjoint spectra functions on small number of variables. We observe that in some cases the nonlinearity bounds of the constructed functions are better than the bounds obtained in [52].

Chapter 5 through Chapter 7 are devoted to the study of various cryptographic properties and constructions of q-ary functions.

In **Chapter 5** we compute the crosscorrelation of a subclass of Maiorana-McFarland (MM) type q-ary bent functions. We provide a characterization of quaternary (4-ary) bent functions on $(n+1)$-variables in terms of their subfunctions on n-variables. Several results on q-ary functions in terms of their WHTs and crosscorrelations spectra are presented. Analogous to the indicators sum-of-squares indicator and absolute indicator in Boolean case, we define two similar indicators: the sum-of-squares-of-modulus indicator (SSMI) $\sigma_{f,g}$ and the modulus indicator (MI) $\triangle_{f,g}$ to measure the global avalanche characteristics (GAC) of two q-ary functions. We study q-ary functions in terms of these two indicators and derive some lower and upper bounds on these indicators. Also, we provide a construction of balanced quaternary functions with high $\mathbb{Z}_4$-nonlinearity under the Lee metric.

In **Chapter 6** we present construction of two classes of q-ary balanced functions which have good GAC measured in terms of two indicators SSMI and MI, and propagation criterion (PC). We show that the cryptographic criteria the SSMI, MI, and PC of q-ary functions are invariant under affine transformations. Also, we give a construction of q-ary s-plateaued functions and obtain their SSMI. We provide a relationship between the autocorrelation spectrum of a cubic Boolean function and the dimension of the kernel of the bilinear form associated with the derivative of the function. Using this result, we identify several classes of cubic semi-bent Boolean functions which have good bounds on their SSMI and MI, and hence show good behavior with respect to the GAC.

In **Chapter 7**, we provide a method for the construction of ternary functions on $(n+1)$ variables by using decomposition functions f_1, f_2, f_3 on n-variables, and investigate a link between their SSMIs. Also, we provide a construction of ternary functions with low value of SSMI by using perfectly uncorrelated ternary functions and modified ternary bent functions. We investigate a relationship among the SSMI $\sigma_{f,g}$ of two q-ary functions f and g, and their individual SSMIs, σ_f and σ_g. Further, we deduce some upper bounds for the indicators the

SSMI and the MI of two q-ary functions for the case that one of them is s-plateaued q-ary function.

In **Chapter 8** we propose a new generalization of negabent functions by considering the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. We investigate several properties of generalized nega-Hadamard transform (GNHT) and its behavior on various combinations of functions. We present some results describing the properties of generalzed negabent functions. We have established a connection between the generalized nega-autocorrelation spectra of functions and their GNHT. A characterization of generalized negabent (for $q = 4$) functions on $n + 1$ variables in terms of its subfunctions on n-variables is presented. We provide several examples of generalized negabent functions for various values of q and n.

It is expected that the results presented in this thesis will be useful in choosing cryptographically significant functions. The future work may be to compute the crosscorrelation of all q-ary functions in Maiorana-McFarland class. Also, the tight lower and upper bounds on two indicators as proposed in Chapter 5 may be obtained. The construction of q-ary balanced functions with optimal values of the indicators, the SSMI and the MI, and satisfying some other important cryptographic criteria remains an open problem. The problem of getting general construction methods for generalized negabent functions remains as future work.

Bibliography

[1] Ambrosimov, A.C.: Properties of the bent functions of q-ary logic over finite fields, *Discrete Mathematics and Applications*, Vol. 4(4), pp. 341–350, 1994.

[2] Biham, E. and Shamir, A.: Differential cryptanalysis of DES-like cryptosystems, *Journal of Cryptology.*, Vol. 4(1), pp. 3–72, 1991.

[3] Boztas, S. and Kumar P.V.: Binary sequences with Gold-like correlation but larger linear span, *IEEE Trans. Inform. Theory*, Vol. 40(2), pp. 532–537, 1994.

[4] Bracken, C., Byrne, E., Markin N. and McGuire G.: Determining the nonlinearity of a new family of APN functions, In Proc. AAECC-2007, LNCS, Springer-Verlag, Vol. 4851, pp. 72–79, 2007.

[5] Budaghyan, L., Carlet, C. Helleseth, T., Kholosha A. and Mesnager, S.: Further results on Niho bent functions, *IEEE Trans. Inform Theory*, Vol. 58(11), pp. 6979–6985, 2012.

[6] Budaghyan, L., Carlet, C., Helleseth, T. and Kholosha, A.: Generalized bent functions and their relation to Maiorana-McFarland class, In Proc. IEEE Inter. Symp. on Inform. Theory 2012, pp. 1212–1215, 2012.

[7] Canteaut, A., Carlet, C., Charpin, P. and Fontaine, C.: On cryptographic properties of the cosets of R(1; m), *IEEE Trans. Inform. Theory*, Vol. 47, pp. 1494–1513, 2001.

[8] Canteaut, A. and Charpin, P.: Decomposing bent functions, *IEEE Trans. Inform. Theory*, Vol. 49(8), pp. 2004–2019, 2003.

[9] Canteaut, A., Charpin, P. and Dobbertin, H.: Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture, *IEEE Trans. Inform. Theory*, Vol. 46(1), pp. 4–8, 2000.

[10] Canteaut, A., Charpin, P. and Kyureghyan, G.M.: A new class of monomial bent functions, *Finite Fields Appl.*, Vol. 14, pp. 221–241, 2008.

[11] Camion, P., Carlet, C., Charpin, P. and Sendrier, N.: On correlation-immune functions, in Advances in Cryptology CRYPTO'91, LNCS, Springer-Verlag, Vol. 547, pp. 86–100, 1992.

[12] Carlet, C.: Two new classes of bent functions, In EUROCRYPT 1993, LNCS, Springer-Verlag, Vol. 765, pp. 77–101, 1994.

[13] Carlet, C.: A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland constructions, in Advances in Cryptology CRYPTO'2002, LNCS, Springer-Verlag, Vol. 2442, pp. 549–564, 2002.

[14] Carlet, C.: On bent and highly nonlinear balanced/resilient functions and their algebraic immunities, In Proc. AAECC 2006, LNCS, Springer-Verlag, Vol. 3857, pp. 1–28, 2006.

[15] Carlet, C.: Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, *IEEE Trans. Inform. Theory*, Vol. 54(3), pp. 1262–1272, 2008.

[16] Carlet, C.: On the nonlinearity profile of the Dillon function, Available at: http://eprint.iacr.org/2009/577.pdf.

[17] Carlet, C.: Boolean functions for cryptography and error correcting codes, In *Boolean Models and Methods in Mathematics, Computer Science and Engineering*, Cambridge Univ. Press, Y. Crama, P. Hammer (eds.), pp. 257–397, 2010.

[18] Carlet, C. and Charpin, P.: Cubic Boolean functions with highest resiliency, *IEEE Trans. Inform. Theory*, Vol. 51(2), pp. 562–571, 2005.

[19] Carlet, C., Dalai, D.K., Gupta, K.C. and Maitra, S.: Algebraic immunity for cryptographically significant Boolean functions: Analysis and Construction, *IEEE Trans. Inform. Theory*, Vol. 52(7), pp. 3105–3121, 2006.

[20] Carlet, C. and Dubuc, S.: On generalized bent and q-ary perfect nonlinear functions, in Proc. Fq5, D. Jungnickel, H. Niederreiter (Eds.), *Finite Fields Appl.*, Springer-Verlag, pp. 81–94, 2000.

[21] Carlet, C. and Feng, K.: An infinite class of balanced vectorial Boolean functions with optimum algebraic immunity and good nonlinearity, In Proc. IWCC'2009, Coding and Cryptology, LNCS, Springer-Verlag, Vol. 5557, pp. 1–11, 2009.

[22] Carlet, C. and Mesnager, S.: Improving the upper bounds on the covering radii of binary Reed-Muller codes, *IEEE Trans. Inform. Theory*, Vol. 53(1), pp. 162–173, 2007.

[23] Carlet, C. and Mesnager, S.: A note on semi-bent Boolean functions, In Cryptology ePrint Archive, http://eprint.iacr.org/2010/486.

[24] Çeşmelioğlu, A. and Meidl, W.: Bent functions of maximal degree, *IEEE Trans. Inform. Theory*, Vol. 58(2), pp. 1186–1190, 2012.

[25] Çeşmelioğlu, A. and Meidl, W.: A construction of bent functions from plateaued functions, *Des. Codes Cryptogr.*, Vol. 66, pp. 231–242, 2013.

[26] Çeşmelioğlu, A., Meidl, W. and Pott, A.: Generalized Maiorana-McFarland class and normality of p-ary bent functions, *Finite Fields Appl.*, Vol. 24, pp. 105–117, 2013.

[27] Çeşmelioğlu, A., Meidl, W. and Pott, A.: On the dual of (non)-weakly regular bent functions and self-dual bent functions, *Advances in Mathematics of Communications*, Vol. 7(4), pp. 425–440, 2013.

[28] Chang, A., Gaal, P., Golomb, S.W., Gong, G., Helleseth, T. and Kumar, P.V.: On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code, *IEEE Trans. Inform. Theory*, Vol. 46(2), pp. 680–687, 2000.

[29] Charpin, P., Pasalic, E. and Tavernier, C.: On bent and semi-bent quadratic Boolean functions, *IEEE Trans. Inform. Theory*, Vol. 51(12), pp. 4286–4298, 2005.

[30] Chee, S., Lee, S. and Kim, K.: Semi-bent Functions, In Advance in Cryptology ASIACRYPT'1994, In Proc. 4-th International Conference on the Theory and Appl. Cryptology, Australia, Pieprzyk, J. and Safavi-Naini, R. (eds.), LNCS, Springer-Verlag, Vol. 917, pp. 107–118, 1994.

[31] Chee, S., Lee, S., Lee, D. and Sung, S.H.: On the correlation immune functions and their nonlinearity, in Advances in Cryptology ASIACRYPT'96, LNCS, Springer-Verlag, Vol. 1163, pp. 232–243, 1997.

[32] Courtois, N.: Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt, In: Proc. of the ICISC'02, LNCS, Springer-Verlag, Vol. 2587, pp. 182–199, 2002.

[33] Courtois, N.: Fast algebraic attacks on stream ciphers with linear feedback, In Advance in Cryptology CRYPTO'2003, LNCS, Springer-Verlag, Vol. 2729, pp. 176–194, 2003.

[34] Courtois, N. and Meier, W.: Algebraic attacks on stream ciphers with linear feedback, In Advance in Cryptology EUROCRYPT'2003, LNCS, Springer-Verlag, Vol. 2656, pp. 346–359, 2003.

[35] Cusick, T.W. and Dobbertin, H.: Some new three-valued crosscorrelation functions for binary m-sequences, *IEEE Trans. Inform. Theory*, Vol. 42(4), pp. 1238–1240, 1996.

[36] Cusick, T.W. and Stănică, P.: Cryptographic Boolean Functions and Applications, Academic Press, Elsevier, 2009.

[37] Dalai, D.K. and Maitra, S.: Balanced Boolean functions with (more than) maximum algebraic immunity, Available at: IACR Cryptology ePrint Archive 01/2006; 2006:434.

[38] Dalai, D.K., Maitra, S. and Sarkar, S.: Results on rotation symmetric bent functions, *Discrete Mathematics*, Vol. 309(8), pp. 2398–2409, 2009.

[39] Dillon, J.F.: A survey of bent functions, *NSA Technical Journal*, Special Issue, pp. 191–215, 1972.

[40] Dillon, J.F.: Elementary Hadamard Difference Sets, Ph.D. Thesis, University of Maryland, 1974.

[41] Dillon, J.F. and McGuire, G.: Near bent functions on a hyperplane, *Finite Fields Appl.* Vol. 14, pp. 715–20, 2008.

[42] Ding, C., Xiao, G.Z. and Shan, W.: The stability theory of stream ciphers, LNCS, Springer-Verlag, Vol. 561, 1991.

[43] Dobbertin, H.: Construction of bent functions and balanced Boolean functions with high nonlinearity, in Proc. Workshop on Fast Software Encryption, FES'1994 , LNCS, Springer-Verlag, Vol. 1008, pp. 61–74, 1995.

[44] Dobbertin, H.: Almost perfect nonlinear power functions on GF(2^n): The Welch case, *IEEE Trans. Inform. Theory*, Vol. 45(4), pp. 1271–1275, 1999.

[45] Dobbertin, H., Helleseth, T., Kumar, P.V. and Martinsen, H.: Ternary m sequences with three-valued crosscorrelation function: new decimations of Welch and Niho type, *IEEE Trans. Inform. Theory*, Vol. 47(4), pp. 1473–1481, 2001.

[46] Fedorova, M. and Tarannikov, Y.V.: On the constructing of highly nonlinear resilient Boolean functions by means of special matrices, In Progress in Cryptology INDOCRYPT'2001, LNCS, Springer-Verlag, Vol. 2247, pp. 254–266, 2001.

[47] Fourquet, R. and Tavernier, C.: An improved list decoding algorithm for the second-order Reed Muller codes and its applications, *Des. Codes Cryptogr.*, Vol. 49, pp. 323–340, 2008.

[48] Gangopadhyay, S., Keskar, P.H. and Maitra, S.: Patterson-Wiedmann construction revisited, *Discrete Mathematics*, Vol. 306. pp. 1540–1556, 2006.

[49] Gangopadhyay, S. and Maitra, S.: Crosscorrelation spectra of Dillon and Patterson-Wiedemann type Boolean functions, Available at http://eprint.iacr.org/2004/014.pdf

[50] Gangopadhyay, S., Sarkar, S. and Telang, R.: On the lower bounds of the second-order nonlinearities of some Boolean functions, *Information Sciences*, Vol. 180, pp. 266–273, 2010.

[51] Gangopadhyay, S. and Singh, B.K.: On second-order nonlinearities of some D_0 type bent functions, *Fundamenta Informaticae*, Vol. 114(3-4), pp. 271–285, 2012.

[52] Gao, S., Ma, W., Zhao, Y. and Zhuo, Z.: Walsh spectrum of cryptographically concatenating functions and its application in constructing resilient Boolean functions, *Journal of Computational Information Systems*, Vol. 7(4), pp. 1074–1081, 2011.

[53] Gode, R. and Gangopadhyay, S.: On second order nonlinearities of cubic monomial Boolean functions, Available at http://eprint.iacr.org/2009/502.pdf

[54] Gode, R. and Gangopadhyay, S.: On lower bounds of second order nonlinearities of cubic bent functions constructed by concatenating Gold functions. *International Journal of Computer Mathematics*, Vol. 88(15), pp. 3125–3135, 2011.

[55] Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions, *IEEE Trans. Inform. Theory*, Vol. 14, pp. 154-156, 1968.

[56] Golić, J.: Fast low order approximation of cryptographic functions, In Proc. EUROCRYPT'96, LNCS, Springer-Verlag, Vol. 1070, pp. 268–282, 1996.

[57] Golić, J. and Mihaljevic, M.J.: A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance, *Journal of Cryptology*, Vol. 3(3), pp. 201–212, 1991.

[58] Golomb, S.W. and Gong, G.: Signal design for good correlation: for wireless communication, cryptography and radar, Cambridge Uni. Press, ISBN 0521821045, 2005.

[59] Gong, G. and Khoo, K.: Additive autocorrelation of resilient Boolean functions, In Selected Areas in Cryptography 2003, LNCS, Springer-Verlag, pp. 275–290, 2004.

[60] Gong, G., Rønjom, S., Helleseth, T. and Hu, H.: Fast discrete Fourier spectra attacks on stream ciphers, *IEEE Trans. Inform. Theory*, Vol. 57(8), pp. 5555–5565, 2011.

[61] Gong, G. and Youssef, A.M.: Cryptographic properties of the Welch-Gong transformation sequence generators, *IEEE Trans. Inform. Theory*, Vol. 48(11), pp. 2837–2846, 2002.

[62] Gupta, K.C., Nawaz, Y. and Gong, G.: Upper bound for algebraic immunity on a subclass of Maiorana-McFarland class of bent functions, *Information Processing Letters*, Vol. 111, pp. 247–249, 2011.

[63] Gupta, K.C. and Sarkar, P.: Construction of perfect nonlinear and maximally nonlinear multiple-output Boolean functions satisfying higher order strict avalanche criteria, *IEEE Trans. Inform. Theory*, Vol. 50(11), pp. 2886–2893, 2004.

[64] Helleseth, T.: Some results about the crosscorrelation function between two maximal linear sequences, *Discrete Mathematics*, Vol. 16, pp. 209–232, 1976.

[65] Helleseth, T.: Correlation of m-sequences and related topics, In Proc. SETA-1998, Discrete Mathematics and Theoretical Computer Science, C. Ding, T. Helleseth, and H. Niederreiter, (eds.), London, Springer-Verlag, pp. 49–66, 1999.

[66] Helleseth, T. and Kholosha, A.: New monomial bent functions over the finite fields of odd characteristic, In Proc. IEEE ISOC ITW-2005 on Coding and Complexity, M.J. Dinneen (ed.), co-chairs U. Speidel and D. Taylor, pp. 72–76, 2005.

[67] Helleseth, T. and Kholosha, A.: On the dual of monomial quadratic p- ary bent functions, In Proc. SSC 2007, S.W. Golomb et al. (eds.), LNCS, Springer-Verlag, Vol. 4893, pp. 50–61, 2007.

[68] Helleseth, T. and Kumar, P.V.: Sequences with low correlation, Chapter in Handbook of Coding Theory, North-Holland, 1998.

[69] Helleseth, T., Lahtonen, J. and Rosendahl, P.: On Niho type crosscorrelation functions of m-sequences, *Finite Fields Appl.*, Vol. 13, pp. 305–317, 2007.

[70] Hou, X.: q-ary bent functions constructed from chain rings, *Finite Fields Appl.*, Vol. 4, pp. 55–61, 1998.

[71] Hou, X.: Bent functions, partial difference sets and quasi-Frobenius rings, *Des. Codes Cryptogr.*, Vol. 20, pp. 251–268, 2000.

[72] Hou, X.: p-ary and q-ary versions of certain results about bent functions and resilient functions, *Finite Fields Appl.*, Vol. 10, pp. 566–582, 2004.

[73] Hu, Z., Li, X., Mills, D., Müller, E., Sun, W., Williems, W., Yang, Y. and Zhang Z.: On the crosscorrelation of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$, *Appl. Algebra Engrg. Comm. Comput.*, Vol. 12, pp. 255-263, 2001.

[74] Iwata, T. and Kurosawa, K.: Probabilistic higher order differential attack and higher order bent functions, In Proc. ASIACRYPT'1999, LNCS, Springer-Verlag, Vol. 1716, pp. 62–74, 1999.

[75] Jadda, Z. and Parraud, P.: $\mathbb{Z}_4$-nonlinearity of a constructed quaternary cryptographic functions class, C. Carlet and A. Pott (eds.), SETA-2010, LNCS, Springer-Verlag, Vol. 6338, pp. 270–283, 2010.

[76] Jakobsen, T. and Knudsen, L.R.: Attacks on block ciphers of low algebraic degree, *Journal of Cryptology*, Vol. 14, pp. 197–210, 2001.

[77] Kabatiansky, G. and Tavernier, C.: List decoding of second order Reed-Muller codes, In Proc. 8th Inter'l Symp. Communi. Theory and Appli., Ambleside, UK, 2005.

[78] Kasami, T.: Weight enumerators for several classes of subcodes of the 2nd order Reed-Muller codes, *Information and Control*, Vol. 18, pp. 369–394, 1971.

[79] Kavut, S., Maitra, S., Sarkar, S. and Yücel, M.D.: Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity > 240, In INDOCRYPT'2006, LNCS, Springer-Verlag, pp. 266–279, 2006.

[80] Kavut, S. and Yücel, M.D.: Generalized rotation symmetric and dihedral symmetric Boolean functions 9 variable Boolean functions with nonlinearity 242, In Proc. AAECC-2007, Springer-Verlag, pp. 321-329, 2007.

[81] Khoo, K., Gong, G. and Stinson, D.R.: A new characterization of semi-bent and bent functions on finite fields, *Des. Codes Cryptogr.*, Vol. 38, pp. 279–295, 2006.

[82] Khoo, Y.S., Jang, J.W., No, J.S. and Helleseth, T.: On p-ary bent functions defined on finite fields, In Mathematical Properties of Sequences and Combinatorial Structures, Kluwer Academic, Dordrecht, pp. 65–76, 2002.

[83] Kim, S.H. and No, J.S.: New families of binary sequences with low correlation, *IEEE Trans. Inform. Theory*, Vol. 49(11), pp. 3059–3065, 2003.

[84] Knudsen, L.R. and Robshaw, M.J.B.: Nonlinear approximations in linear cryptanalysis, In Proc. EUROCRYPT'1996, LNCS, Springer-Verlag, Vol. 1070, pp. 224–236, 1996.

[85] Kolokotronis, N. and Limniotis, K.: Maiorana-McFarland functions with high second order nonlinearity. Available at http://eprint.iacr.org/2011/212.pdf

[86] Kumar, P.V., Hellesth, T., Calderbank, A.R. and Hammons, A.R.: Large families of quaternary sequences with low correlation. *IEEE Trans. Inform. Theory*, Vol. 42(2), pp. 579–592, 1996.

[87] Kumar, P.V., Scholtz, R.A. and Welch, L.R.: Generalized bent functions and their properties, *Journal of Combinatorial Theory*, Ser. A (40), pp. 90–107, 1985.

[88] Langevin, P. and Leander, G.: Monomial bent functions and Stickelberger's theorem, *Finite Fields Appl.*, Vol. 14(3), pp. 727–742, 2008.

[89] Leander, G.: Monomial bent functions, *IEEE Trans. Inform. Theory*, Vol. 52(2), pp. 738–743, 2006.

[90] Li, N., Helleseth, T., Tang, X. and Kholosha, A.: Several new classes of bent functions from Dillon exponents, *IEEE Trans. Inform. Theory*, Vol. 59(3), pp. 1818–1831, 2013.

[91] Li, X., Hu, Y. and Gao, J.: Lower bounds on the second-order nonlinearity of Boolean functions, *International Journal of Foundations of Computer Science*, Vol. 22(6), pp. 1331–1349, 2011.

[92] Li, X., Hu, Y. and Gao, J.: Autocorrelation coefficient of two classes of semi-bent functions, *Applied Mathematics & Information Sciences*, Vol. 5(1), pp. 85–97, 2011.

[93] Li, S., Hu, L. and Zeng, X.: Constructions of p-ary quadratic bent functions, *Acta Applicandae Mathematicae*, Vol. 100, pp. 227–245, 2008.

[94] Lidl, R. and Niederreiter, H.: Introduction to Finite Fields and Their Applications, Cambridge University Press, 1994.

[95] Ma, W. and Lee, M.: A new family of generalized bent functions, SETA-04, Seoul, Korea, pp. 24–28, 2004.

[96] MacWilliams, F.J. and Sloane, N.J.A.: The Theory of Error Correcting Codes, North-Holland, Amsterdam, 1977.

[97] Maitra, S.: Highly nonlinear balanced Boolean functions with good local and global avalanche characteristics, *Information Processing Letters*, Vol. 83, pp. 281–286, 2002.

[98] Maitra, S. and Pasalic, E.: Further constructions of resilient Boolean functions with very high nonlinearity, *IEEE Trans. Inform. Theory*, Vol. 48(7), pp. 1825–1834, 2002.

[99] Maitra, S. and Pasalic, E.: A Maiorana-McFarland type construction for resilient Boolean functions on variables (n even) with nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{\frac{n}{2}-2}$, *Discrete Applied Mathematics*, Vol. 154, pp. 357–369, 2006.

[100] Maitra, S. and Pasalic, E.: Further constructions of resilient Boolean functions with very high nonlinearity, *IEEE Trans. on Inform. Theory*, Vol. 52(5), pp. 2269–2270, 2006.

[101] Maitra, S. and Sarkar, P.: Highly nonliear resilient functions optimizing Siegenthaler's inequality, In Pro. of CRYPTO'99, LNCS, Springer Verlag, Vol. 1666, pp. 198–215, 1999.

[102] Maitra, S. and Sarkar, P.: Modifications of Patterson-Wiedemann functions for cryptographic applications, *IEEE Trans. Inform. Theory*, Vol. 48(1), pp. 278–284, 2002.

[103] Matsui, M.: Linear cryptanalysis method for DES cipher, In Advances in Cryptology-EUROCRYPT'93, LNCS, Springer-Verlag, PP. 386–397, 1994.

[104] Maximov, A.: Some words on cryptanalysis of stream ciphers, Ph.D. Thesis, Lund University, Lund, Sweden, 2006.

[105] Meier, W., Pasalic, E. and Carlet, C.: Algebraic attacks and decomposition of Boolean functions, In Advances in Cryptology EUROCRYPT'2004, LNCS, Springer-Verlag, Vol. 3027, pp. 474–491, 2004.

[106] Meier, W. and Staffelbach, O.: Nonlinearity criteria for cryptographic functions, In Advance in Cryptology EUROCRYPT 1989, LNCS, Springer-Verlag, Vol. 434, pp. 549–562, 1990.

[107] Menezes, A.J., Oorschot, P.C. and Vanstone, S.A.: Handbook of Applied Cryptography, CRC Press, 2001.

[108] Mesnager, S.: Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials, *IEEE Trans. Inform. Theory*, Vol 57(11), pp. 7443–7458, 2011.

[109] Millan, W.: Low order approximation of cipher functions, In cryptographic policy and algorithms, LNCS, Springer-Verlag, Vol. 1029, pp. 144–155, 1996.

[110] Müller, E.N.: On the cross-correlation of sequences over $GF(p)$ with short periods, *IEEE Trans. Inform. Theory*, Vol. 45(1), pp. 289–295, 1999.

[111] Niho, Y.: Multi-valued crosscorrelation functions between two maximal linear recursive sequences, Ph.D. dissertation, Univ. Sothern Calif., Loss Angeles, 1972.

[112] No, J.S., Golomb, S.W., Gong, G., Lee, H.K. and Gaal, P.: Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation, *IEEE Trans. Inform. Theory*, Vol. 44(2), pp. 814–817, 1998.

[113] Nyberg, K.: New bent mapping suitable for fast implementation, In Fast Software Encryption, FSE'1993, LNCS, Springer-Verlag, Vol. 809, pp. 179–184, 1994.

[114] Nyberg, K. and Knudsen, L.R.: Provable security against a differential attack, *Journal of Cryptology*, Vol. 8(1), pp. 27–38, 1995.

[115] Olsen, J.D., Scholtz, R.A. and Welch, L.R.: Bent-function sequences, *IEEE Trans. Inform. Theory*, Vol. 28, pp. 858–864, 1982.

[116] Palit, S., Roy, B.K. and De, A.: A fast correlation attack for LFSR-based stream ciphers, In ACNS'2003, Vol. 2846, pp. 331–342, 2003.

[117] Palit, S. and Roy, B.K.: Cryptanalysis of LFSR-encrypted codes with unknown combining function, K.Y. Lam, E. Okamoto and C. Xing (Eds.), ASIACRYPT'99, LNCS, Springer-Verlag, Vol. 1716, pp. 306–320, 1999.

[118] Parker, M.G.: The constabent properties of Golay-Davis-Jedwab sequences, in Proc. IEEE Int. Symp. Information Theory, Sorrento, Italy, pp. 302, 2000.

[119] Parker, M.G. and Pott, A.: On Boolean functions which are bent and negabent, in Proc. Int. Conf. Sequences, Subsequences, Consequences, LNCS, Springer-Verlag, Vol. 4893, pp. 9–23, 2007.

[120] Pasalic, E. and Johannson, T.: Further results on the relation between nonlinearity and resiliency of Boolean functions, In Proc. of IMA conference cryptography and coding, New York, LNCS, Springer-Verlag, Vol. 1746, pp. 35–45, 1999.

[121] Pasalic, E., Maitra, S., Johannson, T. and Sarkar, P.: New constructions of resilient and correlation immune Boolean functions achieving upper bound on nonlinearity, In Proc. of WCC-2001, Electronic Notes Discrete Mathematics, Vol. 6, pp. 158–167, 2001.

[122] Preneel, B., Leekwijck, W.V., Linden, L.V., Govaerts, R. and Vandewalle, J.: Propagation characteristics of Boolean functions. In Advances in Cryptology-EUROCRYPT'90, LNCS, Springer-Verlag, Vol. 437, pp. 155–165, 1991.

[123] Riera, C. and Parker, M.G.: Generalized bent criteria for Boolean functions (I), *IEEE Trans. Inform. Theory*, Vol. 52(9), pp. 4142–4159, 2006.

[124] Rothaus, O.S.: On bent functions, *Journal of Combinatorial Theory*, Ser. A, Vol. 20, pp. 300–305, 1976.

[125] Roy, B.K.: A brief outline of research on correlation immune functions, L. Batten and J. Seberry (Eds.), ACISP-2002, LNCS, Springer-Verlag, Vol. 2384, pp. 379–394, 2002.

[126] Sarkar, P. and Maitra, S.: Nonlinearity bounds and constructions of resilient Boolean functions, In Advances in Cryptology-CRYPTO'2000, LNCS, Springer-Verlag, Vol. 1880, pp. 515–532, 2000.

[127] Sarkar, P. and Maitra, S.: Construction of nonlinear Boolean functions with important cryptographic properties, in Advances in Cryptology, EUROCRYPT'2000, LNCS, Springer-Verlag, Vol. 1807, pp. 485–506, 2000.

[128] Sarkar, P. and Maitra, S.: Cross-correlation analysis of cryptographically useful Boolean functions. *Theory of Computing Systems*, Vol. 35, pp. 39–57, 2002.

[129] Sarkar, P. and Maitra, S.: Efficient implementation of cryptographically useful large Boolean functions, *IEEE Trans. Comput.*, Vol. 52(4), pp. 410–417, 2003.

[130] Sarkar, P. and Maitra, S.: Construction of nonlinear resilient Boolean functions using small affine functions, *IEEE Trans. Inform. Theory*, Vol. 50(9), pp. 2185–2193, 2004.

[131] Schmidt, KU.: Quaternary constant-amplitude codes for multicode CDMA. *IEEE Trans. Inform. Theory*, Vol. 55(4), pp. 1824–1832, 2009.

[132] Schmidt, K.U., Parker, M.G. and Pott, A.: Negabent functions in the Maiorana-McFarland class, in Proc. Inter. Conf. Seq. Appl. SETA-2008, LNCS-5203 Springer-Verlag, pp. 390–402, 2008.

[133] Seberry, J., Zhang, X.M. and Zheng, Y.: Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion. In Advances in Cryptology, AUSCRYPT'92, LNCS, Springer-Verlag, Vol. 718, pp. 145–155, 1993.

[134] Seberry, J., Zhang, X.M. and Zheng, Y.: Nonlinearly balanced Boolean functions and their propagation characteristics, in Advances in Cryptology, CRYPTO'93, LNCS, Springer-Verlag, Vol. 773, pp. 49–60, 1994.

[135] Seberry, J., Zhang, X.M. and Zheng, Y.: Nonlinearity and propagation characteristics of balanced Boolean functions, *Information and Computation*, Vol. 119(1), pp. 1-13, 1995.

[136] Seo, E., Kim, Y., No, J.S. and Shin, D.: Crosscorrelation distribution of p-ary m-Sequence and its $p+1$ decimated sequences with shorter period, *IEICE Trans. Fundamentals*, Vol. E90-A(11), pp. 2568–2574, 2007.

[137] Shannon, C.: Communication theory of secrecy systems, *Bell System Technical Journal*, Vol. 28, pp. 656–715, 1949.

[138] Shimoyama, T. and Kaneko, T.: Quadratic relation of S-box and its application to the linear attack of full round DES, In Proc. CRYPTO-1998, LNCS, Springer-Verlag, Vol. 1462, pp. 200–211, 1998.

[139] Sidelnikov, V.M.: On the mutual correlation of sequences, *Soviet Math. Dokl.*, Vol. 12, pp. 197–201, 1971.

[140] Siegenthaler, T.: Correlation immunity of nonlinear combining functions for cryptographic applications, *IEEE Trans. Inform. Theory*, Vol. 30(5), pp. 776–780, 1984.

[141] Siegenthaler, T.: Decrypting a class of stream ciphers using ciphertexts only, *IEEE Transactions on Computers*, Vol. C34 (1), pp. 81–85, 1985.

[142] Solé, P. and Tokareva, N.: Connections between quaternary and binary bent functions. Available at: http://www.eprint.iacr.org/2009/544.

[143] Son, J.J., Lima, J.I., Chee, S. and Sung, S.H.: Global avalanche characteristics and nonlinearity of balanced Boolean functions, *Information Processing Letters*, Vol. 65, pp. 139–144, 1998.

[144] Stănică, P., Gangopadhyay, S., Chaturvedi, A., Gangopadhyay, A. and Maitra, S.: Investigations on bent and negabent functions via the nega-Hadamard transform, *IEEE Trans. Inform Theory*, Vol. 58(6), pp. 4064–4072, 2012.

[145] Su, W., Pott, A. and Tang, X.: Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree, 2012. Available at: arXiv:1205.6568v1 [cs.IT].

[146] Sun, G. and Wu, C.: The lower bounds on the second order nonlinearity of three classes of Boolean functions with high nonlinearity, *Information Sciences*, Vol. 179(3), pp. 267–278, 2009.

[147] Sun, G. and Wu, C.: The lower bounds on the second-order nonlinearity of a class of Boolean functions with high nonlinearity, *Appl. Algebra Engrg. Comm. Comput.* Vol. 22, pp. 37–45 2011.

[148] Sung, S.H., Chee, S. and Park, C.: Global avalanche characteristics and propagation criterion of balanced Boolean functions, *Information Processing Letters*, Vol. 69, pp. 21–24, 1999.

[149] Tarannikov, Y.: On resilient Boolean functions with maximum nonlinearity, In Proc. INDOCRYPT'2000, LNCS, Springer-Verlag, Vol. 2248, pp. 460–479, 2001.

[150] Telang, R.G. and Gangopadhyay, S.: On higher-order nonlinearity of monomial partial-spreads type Boolean functions, *Journal of Combinatorics, Information and System Sciences*, Vol. 35(3-4), pp. 341–360, 2010.

[151] Tokareva, N.: Generalizations of bent functions: A survey, *Journal of Applied and Industrial Mathematics*, Vol. 5(1), pp. 110–129, 2011.

[152] Trachtenberg, H.M.: On the cross-correlation functions of maximal recurring sequences, Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, 1970.

[153] Udaya, P.: Polyphase and Frequency Hopping Sequences Obtained from Finite Rings, Ph.D dissertation, Dept. Elec. Eng., Indian Inst. Techno., Kanpur, 1992.

[154] Wang, Z.W. and Zhang, W.: A new construction of leakage-resilient signature, *Journal of Computational Information Systems*, Vol. 6(2), pp. 387–393, 2010.

[155] Webster, A.F.: Plaintext/ciphertext bit Dependencies in Cryptographic System. Master's Thesis, Department of Electrical Engineering, Queen's University, Ontario, Cannada, 1985.

[156] Webster, A.F. and Tavares, S.E.: On the design of S-boxes. In Advances in Cryptology, CRYPTO'85, LNCS, Springer-Verlag, Vol. 219, pp. 523–534, 1986.

[157] Welch, L.R.: Lower bounds on the maximum cross correlation of the signals, *IEEE Trans. Inform. Theory*, IT-20, pp. 397–399, 1974.

[158] Xiao, G.Z. and Messey, J.L.: A spectral characterization of correlation-immune comb-ing functions, *IEEE Trans. Inform. Theory*, Vol. 34(3), pp. 569–571, 1988.

[159] Youssef, A.M.: Generalized hyper-bent functions, *Discrete Applied Mathematics*, Vol. 155, pp. 1066–1070, 2007.

[160] Youssef, A.M. and Gong, G.: Hyper-bent functions, in Advanced Cryptology, EUROCRYPT'2001, Austria, LNCS, Springer-Verlag, Vol. 2045, pp. 406–419, 2001.

[161] Zhang, W.G. and Xiao, G.Z.: Constructions of almost optimal resilient Boolean functions on large even number of variables, *IEEE Trans. Inform. Theory*, Vol. 55(12), pp. 5822–5831, 2009.

[162] Zhang, X.M. and Zheng, Y.: GAC-the criterion for global acalanche criteria of cryptographic functions, *Journal of Universal Computer Science*, Vol. 1(5), pp. 316–333, 1995.

[163] Zheng, Y. and Zhang, X.M.: Plateaued functions, In Advance in Cryptography, ICICS'1999, LNCS, Springer-Verlag, Vol. 1726, pp. 284–300, 1999.

[164] Zhou, Y.: On the distribution of auto-correlation value of balanced Boolean functions, *Advances in Mathematics of Communications*, Vol. 7(3), pp. 335–347, 2013.

[165] Zhou, Y., Dong X., Zhang W. and Zeng, B.: New bounds on the sum-of-squares indicator, 7th International ICST Conference on Communications and Networking in China (CHINACOM), pp. 173–178, 2012.

[166] Zhou, Y., Xie, M. and Xiao, G.Z.: On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, *Information Sciences*, Vol. 180, pp. 256–265, 2010.

[167] Zhou, Y., Zhang, W., Zhu, S. and Xiao, G.Z.: The global avalanche characteristics of two Boolean functions and algebraic immunity, *International Journal Computer Mathematics*, Vol. 89(16), pp. 2165–2179, 2012.

[168] Zhuo, Z.: On cross-correlation properties of Boolean functions, *International Journal Computer Mathematics*, Vol. 88(10), pp. 2035-2041, 2011.

[169] Zhuo, Z., Chong, J., Cao, H. and Xiao, G.Z.: Spectral analysis of two Boolean functions and their derivatives, *Chinese Journal of Electronics*, Vol. 20(4), pp. 747–749, 2011.

BIBLIOGRAPHY

[1] Agievich S.V., Bent rectangles, NATO Advanced Study Inst. on Boolean Functions in Cryptology and Inform. Security, Zvenigorod, Russia, Proc: Netherlands, IOS Press, pp. 3-22, 2008. Available at http://arxiv.org/abs/0804.0209.

[2] Ambrosimov A.C., Properties of the bent functions of q-ary logic over finite fields, Discrete Math., Vol. 6(3), pp. 5060, 1994.

[3] Biham E., Shamir A., Differential cryptanalysis of DES-like cryptosystems, J. of Cryptology, Vol. 4(1), pp. 372, 1991.

[4] Budaghyan L., Carlet C., Helleseth T., Kholosha A., Generalized bent functions and their relation to Maiorana-McFarland class, In Proc. IEEE Inter. Symp. on Inform. Theory 2012, pp. 1212-1215, 2012.

[5] Budaghyan L., Carlet C., Helleseth T., Kholosha A., Mesnager S., Further results on Niho bent functions, IEEE Trans. Inform. Theory, Vol. 58(11), pp. 6979-6985, 2012.

[6] Butson A., Generalized Hadamard matrices, Proc. Amer. Math. Soc., Vol. 13, pp. 894-898, 1962.

[7] Camion P., Carlet C., Charpin P., Sendrier N., On correlation-immune functions, in Advances in Cryptology-CRYPTO'91, LNCS, Berlin, Germany, Springer-Verlag, Vol. 547, pp. 86100, 1992.

[8] Canteaut A., Charpin P., Dobbertin H., Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture, IEEE Trans. Inform. Theory, Vol. 46(1), pp. 4-8, 2000.

[9] Canteaut A., Charpin P., Kyureghyan G.M.: A new class of monomial bent functions, Finite Fields and Applications, Vol. 14, pp. 221-241, 2008.

[10] Carlet C., A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland constructions, in Advances in Cryptology-CRYPTO'2002, LNCS, Berlin, Germany, Springer-Verlag, Vol. 2442, pp. 549-564, 2002.

[11] Carlet C., Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, IEEE Trans. Inform. Theory, Vol. 54 (3), pp. 1262-1272, 2008.

[12] Carlet C., On the nonlinearity profile of the Dillon function, Available at: http://eprint.iacr.org/2009/577.pdf.

[13] Carlet C., Boolean functions for cryptography and error correcting codes, Chapter of the monograph, Boolean Models and Methods in Mathematics, Computer Science and Engineering, Cambridge Univ. Press, Y. Crama, P. Hammer (eds.), pp. 257-397, 2010.

[14] Carlet C., Charpin P., Cubic Boolean functions with highest resiliency, IEEE Trans. Inform. Theory, Vol. 51(2), pp. 562-571, 2005.

[15] Carlet C., Dalai D.K., Gupta K.C., Maitra S., Algebraic immunity for cryptographically significant Boolean functions: analysis and construction, IEEE Trans. Inform. Theory,, Vol. 52(7), pp. 3105-3121, 2006.

[16] Carlet C., Dubuc S., On generalized bent and q-ary perfect nonlinear functions, in: D. Jungnickel, H. Niederreiter (Eds.), Finite Fields and Appli., Proc. of Fq5, Springer, Berlin, pp. 81-94, 2000.

[17] Carlet C., Mesnager S., Improving the upper bounds on the covering radii of binary Reed-Muller codes, IEEE Trans. Inform. Theory, Vol. 53 (1), pp. 162-173, 2007.

[18] Çeşmelioğlu A., Meidl W., Bent functions of maximal degree, IEEE Trans. Inform. Theory, Vol. 58(2), pp. 1186-1190, 2012.

[19] Çeşmelioğlu A., Meidl W., A construction of bent functions from plateaued functions, Design Codes Crypto., Vol. 66, pp. 231-242, 2013.

[20] Çeşmelioğlu A., Meidl W., Pott A., Generalized Maiorana-McFarland class and normality of p-ary bent functions, Finite Fields Appli., Vol. 24, pp. 105-117, 2013.

[21] Chee S., Lee S., Lee D., Sung S.H., On the correlation immune functions and their nonlinearity, in Advances in Cryptology-Asiacrypt'96, LNCS, Berlin, Germany, Springer-Verlag, Vol. 1163, pp. 232-243, 1997.

[22] Cohen G., Honkala I., Litsyn S., Lobstein A., Covering codes, Amsterdam, The Netherlands: North- Holland, 1977.

[23] Courtois N., Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt, In: Proc. of ICISC'02, LNCS, Springer-Verlag, Vol. 2587, pp. 182-199, 2002.

[24] Courtois N., Fast algebraic attacks on stream ciphers with linear feedback, In Advance in Cryptology-CRYPTO'2003, LNCS, Springer-Verlag, Vol. 2729, pp. 176-194, 2003.

[25] Courtois N., Meier, W., Algebraic attacks on stream ciphers with linear feedback, Advance in Cryptology-EUROCRYPT'2003, LNCS, Springer-Verlag, Vol. 2656, pp. 346-359, 2003.

[26] Cusick T.W., Dobbertin H., Some new three-valued crosscorrelation functions for binary m-sequences, IEEE Trans. Inform. Theory, Vol. 42(4), pp. 1238-1240, 1996.

[27] Dalai D.K., Maitra S., Balanced Boolean functions with (more than) maximum algebraic immunity, Available at:

[28] Dalai D.K., Maitra S., Sarkar S., Results on rotation symmetric bent functions, Discrete Math., Vol. 309, pp. 2398-2409, 2009.

[29] Dillon J. F., McGuire G., Near bent functions on a hyperplane, Finite Fields Appli. Vol. 14, 715720, 2008.

[30] Dobbertin H., Construction of bent functions and balanced Boolean functions with high nonlinearity, in Proc. Workshop on Fast Software Encryption, FES-1994 , Berlin, Germany, Vol. 1008, pp. 6174, 1995.

[31] Dobbertin H., Almost perfect nonlinear power functions on GF(2^n): The Welch case, IEEE Trans. Inform. Theory, Vol. 45(4), pp. 1271-1275, 1999.

[32] Dobbertin H., Helleseth T., Kumar P.V., Martinsen H., Ternary m-sequences with three-valued crosscorrelation function: new decimations of Welch and Niho type, IEEE Trans. Inform. Theory, Vol. 47(4), pp. 14731481, 2001.

[33] Dobbertin H., Leander G., Cryptographers toolkit for construction of 8-bit bent functions, Cryptology ePrint Archive, Report 2005/089 (http://eprint.iacr.org/).

[34] Eleuch H., Quantum trajectories and autocorrelation function in semiconductor microcavity, Appl. Math. Inf. Sci, Vol. 3(2), pp. 185-196, 2009.

[35] Fedorova M., Tarannikov Y.V., On the constructing of highly nonlinear resilient Boolean functions by means of special matrices, in Progress in Cryptology-INDOCRYPT'2001, LNCS, Berlin, Germany, Springer-Verlag, Vol. 2247, pp. 254-266, 2001.

[36] Fourquet R., Tavernier C., An improved list decoding algorithm for the second-order Reed-Muller codes and its applications, Designs Codes and Crypto., Vol. 49, pp. 323-340, 2008.

[37] Gangopadhyay S., Sarkar S., Telang R., On the lower bounds of the second-order nonlinearities of some Boolean functions, Inform. Sci., Vol. 180, pp. 266-273, 2010.

[38] Gangopadhyay S., Singh B.K., On Second-order nonlinearities of some D_0 type bent functions, Funda. Inform., Vol. 114(3-4), pp. 271-285, 2012.

[39] Gao S., Ma W., Zhao Y., Zhuo Z., Walsh spectrum of cryptographically concatenating functions and its application in constructing resilient Boolean functions. J. of Comput. Inform. Syst., Vol. 7(4), pp. 1074-1081, 2011.

[40] Gode R., Gangopadhyay S., On second order nonlinearities of cubic monomial Boolean functions, Available at: http://eprint.iacr.org/2009/502.pdf

[41] Gode R., Gangopadhyay, S., On lower bounds of second order nonlinearities of cubic bent functions constructed by concatenating Gold functions. Inter. J. Comput. Math., Vol. 88(15), pp. 3125-3135, 2011.

[42] Gold R., Maximal recursive sequences with 3-valued recursive crosscorrelation functions, IEEE Trans. Inform. Theory, Vol. 14, pp. 154-156, 1968.

[43] Golić, J., Fast low order approximation of cryptographic functions, In: Proc. of the EUROCRYPT'96, LNCS, Springer-Verlag, Vol. 1070, pp. 268-282, 1996.

[44] Golić, J., Mihaljevic M. J., A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance, J. of Crypto., Vol. 3(3), pp. 201-212, 1991.

[45] Gong G., Khoo K., Additive autocorrelation of resilient Boolean functions, In Selected Areas in Cryptography-2003, LNCS, Springer-Verlag, pp. 275-290, 2004.

[46] Gong G., Rønjom S., Helleseth T., Hu H., Fast discrete Fourier spectra attacks on stream ciphers, IEEE Trans. Inform. Theory, Vol. 57(8), pp. 5555-5565, 2011.

[47] Gong G., Youssef A.M., Cryptographic properties of the Welch-Gong transformation sequence generators, IEEE Trans. Inform. Theory, Vol. 48(11), pp. 2837-2846, 2002.

[48] Gupta K.C., Nawaz Y., Gong G., Upper bound for algebraic immunity on a subclass of Maiorana-McFarland class of bent functions, Inform. Proc. Letters, Vol. 111, pp. 247-249, 2011.

[49] Gupta K.C., Sarkar P., Construction of perfect nonlinear and maximally nonlinear multiple-output Boolean functions satisfying higher order strict avalanche criteria, IEEE Trans. Inform. Theory, Vol. 50(11), pp. 2886-2893, 2004.

[50] Helleseth T., Some results about the cross-correlation function between two maximal linear sequences, Discrete Math., Vol. 16, pp. 209-232, 1976.

[51] Helleseth T., Kholosha A., New monomial bent functions over the finite fields of odd characteristic, In Proc. of IEEE, ISOC-ITW'2005 on Coding and Complexity, M.J. Dinneen (edi), pp. 72-76, 2005.

[52] Helleseth T., Kholosha A., On the dual of monomial quadratic p- ary bent functions, In Proc. SSC-2007, S.W. Golomb et al. (Eds.), LNCS, Springer-Verlag, Berlin, Heidelberg, Vol. 4893, pp. 50-61, 2007.

[53] Helleseth T., Lahtonen J., Rosendahl P., On Niho type crosscorrelation functions of m-sequences, Finite Fields Appli., Vol. 13, pp. 305-317, 2007.

[54] Hou X., q-ary bent functions constructed from chain rings, Finite Fields Appli., Vol. 4, pp. 55-61, 1998.

[55] Hou X., Bent functions, partial difference sets and quasi-Frobenius rings, Designs Codes Crypto., Vol. 20, pp. 251-268, 2000.

[56] Hou X., p-ary and q-ary versions of certain results about bent functions and resilient functions, Finite Fields Appli., Vol. 10, pp. 566-582, 2004.

[57] Hu Z., Li X., Mills D., Müller E., Sun W., Williems W., Yang Y., Zhang Z., On the crosscorrelation of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$, Appli. Alg. in Engi, Communi. Comput., Vol. 12, pp. 255-263, 2001.

[58] Iwata T., Kurosawa K., Probabilistic higher order differential attack and higher order bent functions, In Pro. of ASIACRYPT'1999, LNCS, Springer, Heidelberg, Vol. 1716, pp. 62-74, 1999.

[59] Jadda Z., Parraud P., $\mathbb{Z}_4$-nonlinearity of a constructed quaternary cryptographic functions class, C. Carlet and A. Pott (Eds.), SETA-2010, LNCS, Springer-Verlag, Heidelberg, Vol. Vol. 6338, pp. 270-283, 2010.

[60] Jakobsen T., Knudsen L.R., Attacks on block ciphers of low algebraic degree, J. of Crypto., Vol. 14, pp. 197-210, 2001.

[61] Kabatiansky G., Tavernier C., List decoding of second order Reed-Muller codes, In Proc. of eighth Inter'l Symp. of Commun. Theory and Appli., Ambleside, UK, 2005.

[62] Kasami T., Weight enumerators for several classes of subcodes of the 2nd order Reed-Muller codes, Inform. Control, Vol. 18, pp. 369-394, 1971.

[63] Khoo K., Gong G., Stinson D.R., A new characterization of semi-bent and bent functions on finite fields. Designs, Codes Crypto., Vol. 38, pp. 279295, 2006.

[64] Khoo Y.S., Jang J.W., No J.S., Helleseth T., On p-ary bent functions defined on finite fields, In: Mathematical Properties of Sequences and Combinatorial Structures, pp. 65-76. Kluwer Academic, Dordrecht, 2002.

[65] Kim S.H., No J.S., New families of binary sequences with low correlation, IEEE Trans. Inform. Theory, Vol. 49(11), pp. 3059-3065, 2003.

[66] Knudsen L.R., Robshaw M.J.B., Nonlinear approximations in linear cryptanalysis, In Proc. of EUROCRYPT'1996, LNCS, Springer, Vol. 1070, pp. 224-236, 1996.

[67] Kolokotronis N., Limniotis K., Maiorana-McFarland functions with high second order nonlinearity. Available at http://eprint.iacr.org/2011/212.pdf

[68] Kumar P.V., Hellesth T., Calderbank A.R., Hammons A.R, Large families of quaternary sequences with low correlation. IEEE Trans. Inform. Theory, Vol. 42(2), pp. 579-592, 1996.

[69] Kumar P.V., Scholtz R.A., Welch L.R., Generalized bent functions and their properties. J. of Combinatirial Theory, Ser. A 1(40), pp. 90-107, 1985.

[70] Langevin P., Leander G., Monomial bent functions and Stickelberger's theorem, Finite Fields Appli., Vol. 14(3), pp. 727-742, 2008.

[71] Li N., Helleseth T., Tang X., Kholosha A., Several new classes of bent functions from Dillon exponents, IEEE Trans. Inform. Theory, Vol. 59(3), pp. 1818-1831, 2013.

[72] Li X., Hu Y., Gao J., Autocorrelation coefficient of two classes of semi-bent functions, App. Math. Inform. Sci., Vol. 5(1), pp. 85-97, 2011.

[73] Li X., Hu Y., Gao J., Lower bounds on the second-order nonlinearity of Boolean functions, Inter. J. of Found. of Comp. Sci., Vol. 22(6), pp. 1331-1349, 2011.

[74] Li S., Hu L., Zeng X., Constructions of p-ary quadratic bent functions, Acta Appl. Math., Vol. 100, pp. 227-245, 2008.

[75] Lidl R., Niederreiter H., Introduction to finite fields and their applications, Cambridge University Press, 1994.

[76] Logachev O.A., Sal'nikov A.A., Yashchenko V.V., Bent functions over a finite Abelian group, Discrete Math., Vol. 9(4), pp. 320, 1997.

[77] Ma W., Lee M., A new family of generalized bent functions, SETA-04, Seoul, Korea, pp. 2428, 2004.

[78] MacWilliams F.J., Sloane N.J.A., The Theory of Error Correcting Codes, North-Holland, Amsterdam, 1977.

[79] Maitra S., Highly nonlinear balanced Boolean functions with good local and global avalanche characteristics, Inform. Proc. Lett., Vol. 83, pp. 281-286, 2002.

[80] Maitra S., Pasalic E., Further constructions of resilient Boolean functions with very high nonlinearity, IEEE Trans. Inform. Theory, Vol. 48(7), pp. 1825-1834, 2002.

[81] Maitra S., Pasalic E., Further constructions of resilient Boolean functions with very high nonlinearity, IEEE Trans. Inform. Theory, Vol. 52(5), pp. 2269-2270, 2006.

[82] Maitra S., Sarkar P., Highly nonliear resilient functions optimizing Siegenthaler's inequality, In Pro. of Crypto'99, LNCS, Springer Verlag, Vol. 1666, pp. 198-215, 1999.

[83] Matsui M., Linear cryptanalysis method for DES cipher, In Advances in Cryptology-EUROCRYPT'93, LNCS, Springer, Berlin, PP. 386-397, 1994.

[84] Meier W., Pasalic E., Carlet C., Algebraic attacks and decomposition of Boolean functions, In Advances in Cryptology-EUROCRYPT'2004, LNCS, Berlin, Germany, Springer-Verlag, Vol. 3027, pp. 474-491, 2004.

[85] Meier W., Staffelbach O., Nonlinearity criteria for cryptographic functions, In Advance in Cryptology EUROCRYPT'1989, LNCS, Springer-Verlag, Vol. 434, pp. 549-562, 1990.

[86] Menezes A.J., Oorschot P.C., Vanstone S.A., Handbook of Applied Cryptography, CRC Press, 2001,

[87] Mesnager, S., Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity, IEEE Trans. Inform. Theory, Vol 54(8), pp. 3656-3662, 2008.

[88] Millan W., Low order approximation of cipher functions, In cryptographic policy and algorithms, LNCS, Springer-Verlag, Vol. 1029, pp. 144-155, 1996.

[89] Müller E. N., On the cross-correlation of sequences over $GF(p)$ with short periods, IEEE Trans. Inform. Theory, Vol. 45(1), pp. 289-295, 1999.

[90] No J.S., Golomb S.W., Gong G., Lee H.K., Gaal P., Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation, IEEE Trans. Inform. Theory, Vol. 44(2), pp. 814-817, 1998.

[91] Nyberg, K., New bent mapping suitable for fast implementation. In Fast Software Encryption (FSE 1993), LNCS, Springer-Verlag, Vol. 809, pp. 179-184, 1994.

[92] Nyberg K., Knudsen L.R., Provable security against a differential attack, J. of Crypto., Vol. 8(1), pp. 27-38, 1995.

[93] Palit S., Roy B.K., Cryptanalysis of LFSR-encrypted codes with unknown combining function, K.Y. Lam, E. Okamoto and C. Xing (Eds.), ASIACRYPT'99, LNCS, Springer-Verlag, Berlin, Heidelberg, Vol. 1716, pp. 306-320, 1999.

[94] Palit S., Roy B.K., De A., A fast correlation attack for LFSR-based stream ciphers, In ACNS-2003, Vol. 2846, pp. 331-342, 2003.

[95] Parker M.G., The constabent properties of Golay-Davis-Jedwab sequences, in Proc. IEEE Inter. Symp. Inform. Theory, Sorrento, Italy, pp. 302, 2000.

[96] Pasalic E., Johannson T., Further results on the relation between nonlinearity and resiliency of Boolean functions, In Proc. of IMA conference cryptography and coding, New York, LNCS, Springer-Verlag, Vol. 1746, pp. 35-45, 1999.

[97] Pasalic E., Maitra S., Johannson T., Sarkar P., New constructions of resilient and correlation immune Boolean functions achieving upper bound on nonlinearity, In Proc. of WCC-2001, Electronic Notes Discrete Math., Vol. 6, pp. 158-167, 2001.

[98] Poinsot L., Harari S., Generalized Boolean bent functions, in Progress in Cryptology-INDOCRYPT'2004, Chennai, India, Dec. 2022, 2004, Proc. LNCS, Springer, Berlin, Vol. 3348, pp. 107-119, 2005.

[99] Preneel B., Leekwijck W.V., Linden L.V., Govaerts R., Vandewalle J., Propagation characteristics of Boolean functions, In Advances in Cryptology- EUROCRYPT'90, LNCS, Springer-Verlag, Berlin, Heidelberg, New York, Vol. 437, pp. 155-165, 1991.

[100] Riera C., Parker M.G., Generalized bent criteria for Boolean functions (I), IEEE Trans. Inform. Theory, Vol. 52(9), pp. 4142-4159, 2006.

[101] Rothaus O.S., On Bent functions. J. of Combinatorial Theory, Ser. A, Vol. 20, pp. 300-305, 1976.

[102] Roy B., A brief outline of research on correlation immune functions, L. Batten and J. Seberry (Eds.), ACISP-2002, LNCS, Springer-Verlag, Berlin, Heidelberg, Vol. 2384, pp. 379-394, 2002.

[103] Rueppel R.A., Analysis and Design of Stream Ciphers, Springer Verlag, 1986.

[104] Sarkar P., Maitra S., Nonlinearity bounds and constructions of resilient Boolean functions, In Advances in Cryptology-CRYPTO'2000, LNCS, Springer, Heidelberg, Vol. 1880, pp. 515-532, 2000.

[105] Sarkar P., Maitra S., Cross-correlation analysis of cryptographically useful Boolean functions, Theory of Computing Systems, Vol. 35, pp. 39-57, 2002.

[106] Schmidt K.U., Quaternary constant-amplitude codes for multicode CDMA. IEEE Trans. Infor. Theory, Vol. 55(4), pp. 1824-1832, 2009.

[107] Schmidt K.U., Parker M.G., Pott A., Negabent functions in the Maiorana-McFarland class, in S.W. Golomb, M.G. Parker, A. Pott, A. Winterhof (eds.), in Proc. Inter. Conf. Seq. Appl. SETA-2008, LNCS, Springer, Vol. 5203, pp. 390-402. 2008.

[108] Seberry J., Zhang Y., Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion, In Advances in Cryptology-AUSCRYPT'92, LNCS, Berlin, Germany, Springer-Verlag, Vol. 718, pp. 145-155, 1993.

[109] Seberry J., Zhang X.M., Zheng Y., Nonlinearly balanced Boolean functions and their propagation characteristics, in Advances in Cryptology-CRYPTO'93, LNCS, Berlin, Germany, Springer-Verlag, Vol. 773, pp. 49-60, 1994.

[110] Seberry J., Zhang X.M., Zheng Y., Nonlinearity and propagation characteristics of balanced Boolean functions, Inform. Comput., Vol. 119, pp. 113, 1995.

[111] Seo E., Kim Y., No J.S., Shin D., Crosscorrelation distribution of p-ary m-sequence and its $(p+1)$ decimated sequences with shorter period, IEICE Trans. Funda, Vol. E90A (11), 2007.

[112] Shannon C., Communication theory of secrecy systems, Bell System Technical Journal Vol. 28, pp. 656-715, 1949.

[113] Shimoyama T., Kaneko T., Quadratic relation of S-box and its application to the linear attack of full round DES, In Proc. of the CRYPTO'1998, LNCS, Springer, Vol. 1462, pp. 200-211, 1998.

[114] Siegenthaler T., Correlation immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. on Infor. Theory, Vol. 30(5), pp. 776-780, 1984.

[115] Siegenthaler T., Decrypting a class of stream ciphers using ciphertexts only, IEEE Trans. Comput., Vol. C34(1), pp. 81-85, 1985.

[116] Solé P., Tokareva N., Connections between quaternary and binary bent functions. Cryptology ePrint Archives, http://www.eprint.iacr.org/2009/544.

[117] Son J.J., Lima J.I., Chee S., Sung S.H., Global avalanche characteristics and nonlinearity of balanced Boolean functions, Inform. Proc. Lett., Vol. 65, pp. 139-144, 1998.

[118] Stănică P., Gangopadhyay S., Chaturvedi A., Gangopadhyay A., Maitra S., Investigations on bent and negabent functions via the nega-Hadamard transform, IEEE Trans. Inform. Theory, Vol. 58(6), pp. 4064-4072, 2012.

[119] Su W., Pott A., Tang X., Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree. Available at: arXiv:1205.6568v1 [cs.IT] 2012.

[120] Sun G., Wu C., The lower bounds on the second order nonlinearity of three classes of Boolean functions with high nonlinearity, Inform. Sci., Vol. 179 (3), pp. 267-278, 2009.

[121] Sun G., Wu C., The lower bounds on the second-order nonlinearity of a class of Boolean functions with high nonlinearity, Appli. Alg. in Eng. Commu. Comp., Vol. 22, pp. 37-45, 2011.

[122] Sung S.H., Chee S., Park C., Global avalanche characteristics and propagation criterion of balanced Boolean functions, Inform. Proc. Lett., Vol. 69, pp. 21-24, 1999.

[123] Tarannikov Y., On resilient Boolean functions with maximum nonlinearity, In Pro. of INDOCRYPT'2000, LNCS, Springer-Verlag, Vol. 2248, pp. 460-479, 2001.

[124] Tarannikov Y., Korolev P., Botev A., Autocorrelation coefficients and correlation immunity of Boolean functions, In: Advances in Cryptology-Asiacrypt'01, Springer, Berlin, pp. 460479, 1994.

[125] Telang R., Gangopadhyay S., On higher-order nonlinearity of monomial partial-spreads type Boolean functions, IMST 2009- FIM XVIII, Jaypee Uni. Inform. Tech., Waknaghat, Solan, H.P., India. Aug. 2-4, 2009.

[126] Tokareva N.N., Bent functions with stronger nonlinear properties: k-bent functions, J. Appl. Indust. Math. 2 (4), 566584, 2008.

[127] Tokareva N., Generalizations of bent functions: A survey. J. Appl. Indust. Math., Vol. 5(1), pp. 110-129, 2011.

[128] Trachtenberg H.M., On the crosscorrelation functions of maximal recurring sequences, Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, 1970.

[129] Udaya P., Polyphase and frequency hopping sequences obtained from finite rings, Ph.D dissertation, Dept. Elec. Eng., Indian Inst. Techno., Kanpur, 1992.

[130] Wang Z.W., Zhang W., A new construction of leakage-resilient signature, J. of Computat. Inform. Systems, Vol. 6(2), pp. 387-393, 2010.

[131] Webster A.F., Plaintext/ciphertext bit dependencies in cryptographic system, Master's Thesis, Dept. of Elect. Eng., Queen's University, Ontario, Cannada, 1985.

[132] Webster A.F. Tavares S.E., On the design of S-boxes. In Advances in Cryptology-CRYPTO'85, LNCS, Springer-Verlag, Berlin, Heidelberg, New York, Vol. 219, pp. 523-534, 1986.

[133] Welch L.R., Lower bounds on the maximum crosscorrelation of the signals, IEEE Trans. Inform. Theory, IT-20, pp. 397-399, 1974.

[134] Xiao G.Z., Massey J.L., A spectral characterization of correlation-immune combing functions, IEEE Trans. Inform. Theory, Vol. 34(3), pp. 569-571, 1988.

[135] Youssef A.M., Generalized hyper-bent functions, Discrete Appl. Math., Vol. 155, pp. 1066-1070, 2007.

[136] Youssef A.M., Gong G., Hyper-bent functions, in Advanced Cryptology - EUROCRYPT'2001, Austria, LNCS, Berlin, Springer, Vol. 2045, pp. 406-419, 2001.

[137] Zhang W.G., Xiao G.Z., Constructions of almost optimal resilient Boolean functions on large even number of variables, IEEE Trans. on Inform. Theory, Vol. 55(12), pp. 5822-5831, 2009.

[138] Zhang X.M., Zheng Y., GAC-The criterion for global acalanche criteria of cryptographic functions, J. Univ. Comput. Sci., Vol. 1(5), pp. 316-333, 1995.

[139] Zhou Y., On the distribution of autocorrelation value of balanced Boolean functions, Advances in Math. Communi., Vol. 7(3), pp. 335-347, 2013.

[140] Zhou Y., Xie M., Xiao G.Z., On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, Inform. Sci., Vol. 180, pp. 256-265, 2010.

[141] Zhou Y., Zhang W., Zhu S., Xiao G., The global avalanche characteristics of two Boolean functions and algebraic immunity, Inter. J. Comput. Math., Vol. 89(16), pp. 2165-2179, 2012.

[142] Zhuo Z., On cross-correlation properties of Boolean functions, Inter. J. Comput. Math., Vol. 88(10), pp. 2035-2041, 2011.

[143] Zhuo Z., Chong J., Cao H., Xiao G.Z., Spectral analysis of two Boolean functions and their derivatives, Chi. J. Electro., Vol. 20(4), pp. 747-749, 2011.

(a) Panel of Examiners from India

1.	Name:	**Dr. Kishan Chand Gupta**	Telephone No.
	Designation:	**Assistant Professor**	Fax No.
	Address:	**Applied Statistical Unit, Indian Statistical Institute, 203 Barrackpore Trunk Road, Kolkata 700108, India**	Email Address: **kishan@isical.ac.in**
			Publication/Reference of Bibliography: **[15], [48], [49]**

2.	Name:	**Dr. Deepak Kumar Dalai**	Telephone No. (**0674) 2304060**
	Designation:	**Assistant Professor**	Fax No.
	Address:	**School of Mathematical Sciences, National Institute of Science Education and Research, Institute of Physics Campus, P.O.: Sainik School, Bhubaneswar – 751005, India**	Email Address: **deepakkumardalai@gmail.com**
			Publication/Reference of Bibliography: **[15], [27], [28]**

3.	Name:	**Dr. Bimal Kumar Roy**	Telephone No. **(033) 2575-2809**
	Designation:	**Professor and Director**	Fax No.
	Address:	**Indian Statistical Institute, 203 Barrackpore Trunk Road, Kolkata 700108, India**	Email Address: **bimal@isical.ac.in**
			Publication/Reference of Bibliography: **[93], [94], [102]**

4.	Name:	**Dr. P. Vijay Kumar**	Telephone No. **(080) 22933155**
	Designation:	**Professor**	Fax No.
	Address:	**Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012, India**	Email Address: **pvk1729@gmail.com**
			Publication/Reference of Bibliography: **[32], [68], [69]**

5.	Name:	**Dr. Palash Sarkar**	Telephone No.
	Designation:	**Professor**	Fax No.
	Address:	**Applied Statistical Unit, Indian Statistical Institute, 203 Barrackpore Trunk Road, Kolkata 700108, India**	Email Address: **palash@isical.ac.in**
			Publication/Reference of Bibliography: **[49], [82], [97], [104], [105]**

Member, SRC (External Expert) **Member, SRC (Internal Expert)**

Supervisor **Supervisor** **Supervisor** **Chairman, DR C/CRC**

DATED : **HEAD OF THE DEPARTMENT/CENTRE**

(b) Panel of Foreign Examiners

1.	Name:	**Dr. Wilfried Meidl**	Telephone No.
	Designation:	**Associate Professor**	Fax No.
	Address:	**Sabanci University, MDBF, Orhanli, 34956 Tuzla, Istanbul, Turkey**	Email Address: **wmeidl@sabanciuniv.edu**
			Publication/Reference of Bibliography: **[18], [19], [20]**

2.	Name:	**Dr. Yu Zhou**	Telephone No.
	Designation:	**Senior Engineer**	Fax No.
	Address:	**Science and Technology on Communication Security Laboratory, Southwest Communication Institute, Chengdu, 610041, China**	Email Address: **zhouyu.zhy@tom.com**
			Publication/Reference of Bibliography: **[139], [140], [141]**

3.	Name:	**Dr. Yuliang Zheng**	Telephone No. **704-687-8666**
	Designation:	**Professor**	Fax No.
	Address:	**Department of Software Information Systems, University of North Carolina at Charlotte, 9201 University City Blvd, Charlotte, NC 28223, USA**	Email Address: **yzheng@uncc.edu**
			Publication/Reference of Bibliography: **[109], [110], [138]**

4.	Name:	**Dr. Amr M. Youssef**	Telephone No. **(514) 848-2424 - ext 5441**
	Designation:	**Professor**	Fax No.
	Address:	**Concordia Institute of Information Systems Engineering, Concordia University, Montreal, Quebec, Canada H3G 1MG**	Email Address: **youssef@ciise.concordia.ca**
			Publication/Reference of Bibliography: **[47], [135], [136]**

5.	Name:	**Dr. Guozhen Xiao**	Telephone No.
	Designation:	**Professor**	Fax No.
	Address:	**State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China**	Email Address: **gzxiao@xidian.edu.cn**
			Publication/Reference of Bibliography: **[134], [137], [140], [141], [143]**

Member, SRC (External Expert) **Member, SRC (Internal Expert)**

Supervisor **Supervisor** **Supervisor** **Chairman, DR C/CRC**

DATED : **HEAD OF THE DEPARTMENT/CENTRE**

A STUDY OF SOME CRYPTOGRAPHICALLY SIGNIFICANT BOOLEAN FUNCTIONS AND THEIR GENERALIZATIONS

SYNOPSIS

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

of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

by

DEEP SINGH

Under the Supervision of

Dr. MAHESHANAND
Department of Mathematics, I.I.T. Roorkee

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE - 247667 (INDIA)
MAY, 2014

Synopsis

Cryptography is a key technology in providing the secure transmission of information over public channels. It is a branch of science which mainly deals with the design and construction of protocols related to various aspects of secure communication through an insecure channel. The goal of secure communication can be achieved by using suitable encryption algorithms for generating secure cipher texts. In 1949, Shannon [25] established the foundation of modern cryptography by deriving the notion of product ciphers in terms of two basic transformations: substitutions and permutations. Both these transformations extensively use Boolean functions with certain desirable cryptographic properties.

According to Shannon [25], to achieve secure encryption algorithms, it is sufficient to design the elementary blocks: S-boxes and P-boxes. Boolean functions and S-boxes with desirable cryptographic properties have many applications in designing of symmetric key cryptosystem: *stream ciphers* and *block ciphers*. In stream ciphers a pseudorandom keystream of bits is generated which on XOR-ing with plaintext bits provides the cipher text. The cipher text is transmitted over the channel and at receiver end, deciphering is done by XOR-ing cipher bits with the same random bit sequence used for ciphering. Several linear feedback shift registers (LFSRs) based stream ciphers use Boolean functions as *combiner* functions or *filter* functions. LFSRs are important building block in the stream ciphers, but they are linear, so, by using nonlinear Boolean functions, some form of nonlinearity can be introduced [21]. The nonlinear combiner Boolean function and their properties have got special attention during last few years and the researchers have developed several important techniques, using which it is now possible to construct Boolean functions that provide protection against the known attacks.

The Boolean functions used in various cryptosystems should satisfy various cryptographic criteria. However, it is impossible to optimize all the criteria simultaneously, so there are some tradeoffs among these criteria. According to the application, one has to decide that which criteria are more important. For example, for the pseudorandomness of keystream, the functions employed in the stream ciphers should be *balanced*. The Boolean functions used in stream ciphers as a combiner function should possess *high nonlinearity* to prevent the system from linear approximation attack [5, 16, 17]. Matsui [16] has proposed linear cryptanalysis scheme for block ciphers. The security of block ciphers depends on the strength of chosen S-boxes. To protect the block ciphers from linear cryptanalysis, the employed S-boxes should be highly nonlinear.

Biham and Shamir [2] have proposed differential attack which involves a comparison between the XOR of two inputs and XOR of corresponding outputs. Webster and Tavares [32] have introduced the notion of *strict avalanche criteria* (SAC), which is later generalized to *propagation criteria* (PC) by Preneel et al. [18]. The SAC and PC are two important cryptographic criteria for S-boxes to provide protection from differential attack. However, SAC and PC provide information only about local properties of cryptographic functions. For global analysis of these functions, Zhang and Zheng [33] have introduced a new criteria known as *global avalanche characteristics* (GAC) and proposed two indicators: the sum-of-squares indicator σ_f and the absolute indicator $\triangle_f$ of one Boolean function. Zhou et al. [34] have generalized this concept by introducing two indicators: the *sum-of-squares indicator* $\sigma_{f,g}$ and the *absolute indicator* $\triangle_{f,g}$ for two cryptographic functions. They have deduced some lower and upper bounds on these indicators and established their relationship with higher order nonlinearities.

Let $\mathbb{Z}_2$ be the finite field of characteristic 2. A function from $\mathbb{Z}_2^n \to \mathbb{Z}_2$ is called Boolean function

on n-variables. Let $\mathcal{B}_n$ be the set of all such Boolean functions. The Hamming weight $wt(u)$ of $u \in \mathbb{Z}_2^n$ is the number of ones in u. The most important tool for analysis of most of the cryptographic criteria is the Walsh Hadamard transform (WHT). The WHT, $W_f : \mathbb{Z}_2^n \to [-2^n, 2^n]$ of $f \in \mathcal{B}_n$ is defined as $W_f(a) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x)+a \cdot x}$. $f \in \mathcal{B}_n$ is balanced if and only if $W_f(0) = 0$. A function $f \in \mathcal{B}_n$ is called correlation immune of order r if $W_f(a) = 0$ for all a with $1 \leq wt(a) \leq r$ [26]. A balanced r-correlation immune function is called *r-resilient*. Resiliency is an important criterion which prevents the cryptographic system from information leakage and correlation attack [7, 13]. Gao et al. [11] have constructed nonlinear plateaued resilient functions with disjoint spectra.

The nonlinearity $nl(f)$ of $f \in \mathcal{B}_n$ is defined as the minimum Hamming distance of f from the set of all affine functions. In terms of WHT, $nl(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{Z}_2^n} |W_f(a)|$. The functions possessing maximum possible nonlinearity are called *bent* [20] and exist only for even n. A natural generalization of nonlinearity is the *rth order nonlinearity* (nl_r), which is defined as the minimum Hamming distance of f from the set of all functions of degree at most r. In [3], Carlet has extensively studied rth order nonlinearity of Boolean functions and provided lower bounds on $nl_r(f)$ in a recursive framework using $(r-1)$th order nonlinearity of the derivative of $f \in \mathcal{B}_n$. He has derived lower bounds on nl_r for several classes of Boolean functions such as inverse functions, Welch functions, Kasami functions and the functions in Maiorana-McFarland (MMF) bent class. Using Carlet's recursive approach, the lower bounds on second order nonlinearities of some highly nonlinear Boolean functions have been obtained in [10, 12, 30].

Recently, many generalizations of Boolean function have been proposed [4, 8, 15, 23]. In [15], Kumar et al. generalized the classical Boolean functions to q-ary functions. A q-ary function is a function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, where $\mathbb{Z}_q$ is the ring of integers modulo q. Let $\mathcal{B}_{n,q}$ be the set of all such functions on n-variables. The WHT, $W_f : \mathbb{Z}_q^n \to \mathbb{C}$ of $f \in \mathcal{B}_{n,q}$ is defined as $W_f(a) = \sum_{x \in \mathbb{Z}_q^n} \xi^{f(x)+a \cdot x}$, where $\xi = e^{\frac{2\pi i}{q}}$ and $\mathbb{C}$ is the set of complex numbers. A function $f \in \mathcal{B}_{n,q}$ is called *q-ary bent* if $|W_f(a)| = 1$ for all $a \in \mathbb{Z}_q^n$. It may be noted that Boolean bent functions exists only for even n, whereas q-ary bent functions exist for every value of q and n except for n odd and $q \equiv 2(\mod 4)$. Kumar et al. [15] have observed that establishing analogous properties for q-ary bent function are far more difficult. They have discussed several important properties of q-ary bent functions in terms of their WHT and autocorrelation spectrum. They have shown that $f \in \mathcal{B}_{n,q}$ is q-ary bent if and only if its autocorrelation $\mathcal{C}_f(\mathbf{x})$ is identically zero for every nonzero $\mathbf{x}$ in $\mathbb{Z}_q^n$. Further, they have provided natural generalization of MMF type bent functions. The *cross-correlation* of $f, g \in \mathcal{B}_{n,q}$ at $\mathbf{u} \in \mathbb{Z}_q^n$ is defined as $\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})}$. For $f = g$, $\mathcal{C}_f = \mathcal{C}_{f,f}$ is called the *autocorrelation* of f [15, 22]. From *confusion* and *diffusion* aspect, it is good if the constituent functions of a secret key cryptosystem have low correlation [22, 25].

Agievich [1] has provided a technique to discuss *regular* q-ary bent functions in terms of bent rectangles. Jadda and Parraud [14] have characterized $\mathbb{Z}_4$-balancedness and $\mathbb{Z}_4$-nonlinearity on the basis of Hamming metric and Lee metric. Sol*é* and Tokareva [27] have provided a direct link among bent functions, q-ary bent (for $q = 4$) functions and bent functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ (due to Schmidt [23]). Çeşmelioğlu et al. [6] have analyzed a class of bent functions which contains regular bent, weakly regular bent and not weakly regular bent functions for both n even and n odd. Maiorana-McFarland type bent functions are contained in this class. They have analyzed the *normality* of q-ary bent functions in odd characteristic. For n even, they have observed that many q-ary (also quadratic) bent functions in odd characteristic are not normal.

On the other hand, Riera and Parker [19] have extended the notion of bentness to some generalized bent criteria by analyzing Boolean functions having flat spectrum with resect to one or more unitary transforms. The transforms they have chosen are n-fold tensor product of the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the WHT $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and the nega-Hadamard transform (NHT) $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, $i^2 = -1$. The NHT, $N_f : \mathbb{Z}_2^n \to \mathbb{C}$ of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is given as $N_f(\mathbf{u}) = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{x})+\mathbf{x}\cdot\mathbf{u}} i^{wt(\mathbf{x})}$. A function $f \in \mathcal{B}_n$ is *negabent* if $|N_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. The functions which are both bent and negabent are of recent interest. For constructions and various properties of such functions we refer to [19, 24, 28, 29].

In this thesis, we study various cryptographic and combinatorial properties of Boolean functions and q-ary functions as they have wide applications in cryptography, coding theory and computer science. We provide several constructions of Boolean functions and q-ary functions which satisfy several cryptographic criteria. We provide direct link among several cryptographic criteria on the basis of WHT and crosscorrelation of q-ary functions. The chapter wise summary of the thesis is as follows:

Chapter 1 provides the introduction and a brief summary of the thesis.

Chapter 2 contains necessary preliminaries required in the subsequent chapters.

In **Chapter** 3, we consider the problem of computing lower bounds on second order nonlinearities of cubic monomial functions of the form

1. $f(x) = tr_1^n(\lambda x^{2^{2r}+2^{r+1}+1})$, where $n = 3r,\ 5r$ and $\lambda \in \mathbb{Z}_{2^n} \setminus \{0\}$,
2. $f(x) = tr_1^n(\lambda x^{2^{2r}+2^r+1})$, where $n = 3r$ and $\lambda \in \mathbb{Z}_{2^r} \setminus \{0\}$.

Boolean functions in the above classes possess no affine derivative. The general lower bounds on second-order nonlinearities of the cubic Boolean functions which have no affine derivative have been deduced by Carlet [3]. It is observed that the bounds obtained by us for the above classes of functions are better than the general bounds obtained by Carlet [3] and the bounds of some other classes of Boolean functions which are recently studied [10, 12, 30]. The direct computation using the algorithm of Fourquet and Tavernier [9] shows that some functions in these classes have bounds very close the largest known second-order nonlinearity. Further, we obtain lower bounds on second-order nonlinearities for some classes of cubic Boolean functions based on secondary constructions. The results of this chapter are published in [S11,SB13b].

Gao et al. [11] have provided a method for the construction of plateaued resilient functions with disjoint spectra. In **Chapter 4** using this technique, we provide some new constructions of highly nonlinear resilient Boolean functions on large number of variables with disjoint spectra by concatenating disjoint spectra functions on small number of variables. We observe that in some cases the nonlinearity bounds of the constructed functions are better than the bounds obtained by Gao et al. [11]. The results of this chapter are published in [S12].

Chapter 5 onward are devoted to the study of various cryptographic properties and constructions of q-ary functions.

In **Chapter 5** we compute the crosscorrelation of a subclass of generalized Maiorana-McFarland (GMMF) type bent functions. We provide a characterization of quaternary (4-ary) bent functions on $(n+1)$-variables in terms of their subfunctions on n-variables. We slightly generalize a result of Tokerava [31] by proving that the direct sum of two q-ary bent functions f_1 and f_2 is q-ary bent if and only if f_1 and f_2 both are q-ary bent. We present several results on q-ary

functions in terms of their WHT and crosscorrelation. Analogous to the indicators $\sigma_{f,g}$ and $\triangle_{f,g}$ in Boolean case, we define two similar indicators: the *sum-of-squares-of-modulus indicator* (SSMI) $\sigma_{f,g}$ and the *modulus indicator* (MI) $\triangle_{f,g}$ to measure the global avalanche characteristic (GAC) of two q-ary functions. We study q-ary functions in terms of these two indicators and derive some lower and upper bounds on these indicators. Also, we provide some constructions of balanced quaternary functions with high nonlinearity under Lee metric. The contents of this chapter are published in [SBS13].

In **Chapter 6**, we study some further properties of q-ary functions and provide some constructions for ternary ($q = 3$) functions. We provide a method for the construction of ternary functions on $(n + 1)$-variables by using decomposition functions f_1, f_2, f_3 on n-variables, and investigate a link between the SSMI of a $(n + 1)$-variable ternary function f and the SSMI of their n-variable decomposition functions f_1, f_2, f_3. Also, we provide a construction of ternary functions with low value of SSMI by using perfectly uncorrelated ternary functions and modified ternary bent functions. We investigate a relationship among the indicators, $\sigma_{f,g}$, σ_f (the SSMI of f) and σ_g (the SSMI of g) of two q-ary functions f and g. Further, we deduce upper bounds to the indicators the SSMI and the MI of two q-ary functions for the case that one of them is s-plateaued q-ary function. The contents of this chapter are published in [SB13a].

In **Chapter 7** we present construction of two classes of q-ary *balanced* functions which have good GAC measured in terms of two indicators SSMI and MI, and *propagation criterion* (PC). We show that the cryptographic criteria the SSMI, MI, and PC of q-ary functions are invariant under affine transformations. Also, we give a construction of q-ary s-plateaued functions and obtain their SSMI. We provide a relationship between the autocorrelation spectrum of a cubic Boolean function and the dimension of the kernel of the bilinear form associated with the derivative of the function. Using this result, we identify several classes of cubic semi-bent Boolean functions which have good bounds on their SSMI and MI, and hence show good behavior with respect to the GAC. The contents of this chapter are published in [SBS14].

In **Chapter 8** we have extended the notion of binary negabent functions to the q-ary functions. We investigate Several properties of q-ary nega-Hadamard transform (NHT) and its behavior on various combinations of q-ary functions. We provide some results describing the properties of q-ary negabent functions. We generalize a result of Schmidt [24, Lemma 1] (obtained for binary case) to $\mathbb{Z}_q$. We have established a connection between the q-ary nega-autocorrelations of two q-ary functions and their NHT. Further, we provide a characterization of quaternary negabent functions on $n + 1$ variables in terms of their subfunctions on n-variables.

List of Publications

• Journals

[SBS14] Singh D., Bhaintwal M., Singh B. K., Constructions of q-ary functions with good global avalanche characteristics, International Journal of Computer Mathematics (Publisher: Taylor & Francis), 2014, DOI:10.1080/00207160.2014.902940

[SBS13] Singh D., Bhaintwal M., Singh B. K., Some results on q-ary bent functions, International Journal of Computer Mathematics (Publisher: Taylor & Francis), Vol. 90 (9), pp. 1761-1773, 2013.

[S11] Singh D., Second order nonlinearities of some classes of cubic Boolean functions based on

secondary constructions, International Journal of Computer Science and Information Technologies, Vol. 2 (2), pp. 786-791, 2011.

- **Conferences**

[SB13a] Singh D., Bhaintwal M., On the sum-of-squares-modulus indicator of q-ary functions, In Proc. of the international conference "Advances in Computing, Communications and Informatics" ICACCI-2013, during August 22-25, 2013 at SJCE University, Mysore, India, Available at IEEE Xplore, pp. 599-603, 2013, DOI: 10.1109/ICACCI.2013.6637240

[SB13b] Singh D., Bhaintwal M., On second order nonlinearities of two classes of cubic Boolean functions, In Proc. of the International conference "Heterogeneous Networking for Quality, Reliability, Security and Robustness" QSHINE-2013, during January 11-12, 2013 at Department of Mathematics, GB University, Greater Noida, India, Lecture Notes of the Institute for Computer Sciences, LNICST, Vol. 115, Springer-Verlag Berlin Heidelberg, pp. 560-567, 2013.

[S12] Singh D., Construction of highly nonlinear plateaued resilient functions with disjoint spectra, In Proc. of the International conference "Mathematical Modelling and Scientific Computation" ICMMSC-2012, during March 16-18, 2012 at Department of Mathematics, GRI, Gandhigram, Tamilnadu, India, Communications in Computer and Information Science, CCIS, Vol. 283, Springer-Verlag Berlin Heidelberg, pp. 522-529, 2012.

References

[1] Agievich S.V., Bent rectangles, NATO Advanced Study Institute on Boolean Functions in Cryptology and Inform. Security, Zvenigorod, Russia, Proc: Netherlands, IOS Press, pp. 3-22, 2008. Available at http://arxiv.org/abs/0804.0209.

[2] Biham E., Shamir A., Differential cryptanalysis of DES-like cryptosystems, J. of Crypto., Vol. 4(1), pp. 372, 1991.

[3] Carlet C., Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, IEEE Trans. Inform. Theory, Vol. 54 (3), pp. 1262-1272, 2008.

[4] Carlet C., Boolean functions for cryptography and error correcting codes, Chapter of the monograph, Boolean Models and Methods in Mathematics, Computer Science and Engineering, Cambridge Uni. Press, Y. Crama, P. Hammer (eds.), pp. 257-397, 2010.

[5] Carlet C., Dalai D.K., Gupta K.C., Maitra S., Algebraic immunity for cryptographically significant Boolean functions: analysis and construction, IEEE Trans. Inform. Theory,, Vol. 52(7), pp. 3105-3121, 2006.

[6] Çeşmelioğlu A., Meidl W., Pott A., Generalized Maiorana-McFarland class and normality of p-ary bent functions, Finite Fields Appli., Vol. 24, pp. 105117, 2013.

[7] Courtois N., Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt, In: Proc. of the ICISC'02, LNCS, Springer-Verlag, Vol. 2587, pp. 182-199, 2002.

[8] Dobbertin H., Leander G., Bent functions embedded into the recursive framework of $\mathcal{Z}$-bent functions, Design Codes Crypto. Vol. 49, pp. 3-22, 2008.

[9] Fourquet R., Tavernier C., An improved list decoding algorithm for the second-order Reed Muller codes and its applications, Designs Codes Crypto., Vol. 49, pp. 323-340, 2008.

[10] Gangopadhyay S., Sarkar S., Telang R., On the lower bounds of the second-order nonlinearities of some Boolean functions, Inform. Sci., Vol. 180, pp. 266-273, 2010.

[11] Gao S., Ma W., Zhao Y., Zhuo Z., Walsh spectrum of cryptographically concatenating functions and its application in constructing resilient Boolean functions. J. Comput. Inform. Syst. Vol. 7(4), pp. 1074-1081, 2011.

[12] Gode R., Gangopadhyay S., On second order nonlinearities of cubic monomial Boolean functions, Available at http://eprint.iacr.org/2009/502.pdf

[13] Gong G., Khoo K., Additive autocorrelation of resilient Boolean functions, In Selected Areas in Cryptography-2003, LNCS, Springer, Heidelberg, pp. 275-290, 2004.

[14] Jadda Z., Parraud P., $\mathbb{Z}_4$-nonlinearity of a constructed quaternary cryptographic functions class, C. Carlet and A. Pott (Eds.), SETA-2010, LNCS, Springer, Heidelberg, Vol. 6338, pp. 270-283, 2010.

[15] Kumar P.V., Scholtz R.A., Welch L.R., Generalized bent functions and their properties. J. of Combinatorial Theory, Ser. A 1(40), pp. 90-107, 1985.

[16] Matsui M., Linear cryptanalysis method for DES cipher, In Advances in Cryptology-EUROCRYPT'93, LNCS, Springer, Heidelberg, pp. 386-397, 1994.

[17] Palit S., Roy B.K., Cryptanalysis of LFSR-encrypted codes with unknown combining function, K.Y. Lam, E. Okamoto and C. Xing (Eds.), ASIACRYPT'99, LNCS, Springer-Verlag, Berlin, Heidelberg, Vol. 1716, pp. 306-320, 1999.

[18] Preneel B., Leekwijck W.V., Linden L.V., Govaerts R., Vandewalle J., Propagation characteristics of Boolean functions, In Advances in Cryptology- EUROCRYPT'90, LNCS, Springer, Heidelberg, New York, Vol. 437, pp. 155-165, 1991.

[19] Riera C., Parker M.G., Generalized bent criteria for Boolean functions (I), IEEE Trans. Inform. Theory, Vol. 52(9), pp. 4142-4159, 2006.

[20] Rothaus O.S., On bent functions. J. of Combinatorial Th. Ser. A, Vol. 20, pp. 300-305, 1976.

[21] Rueppel R.A., Analysis and Design of Stream Ciphers, Springer Verlag, 1986.

[22] Sarkar P., Maitra S., Cross-correlation analysis of cryptographically useful Boolean functions. Theory of Computing Systems, Vol. 35, pp. 39-57, 2002.

[23] Schmidt K.U., Quaternary constant-amplitude codes for multicode CDMA, IEEE Trans. Inform. Theory, Vol. 55(4), pp. 1824-1832, 2009.

[24] Schmidt K.U., Parker M.G., Pott A., Negabent functions in the Maiorana-McFarland class, in Proc. Inter. Conf. Seq. Appl., SETA-2008, LNCS-5203 Springer, Heidelberg, pp. 390-402. 2008.

[25] Shannon C., Communication theory of secrecy systems, Bell System Technical Journal Vol. 28, pp. 656-715, 1949.

[26] Siegenthaler T., Correlation immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Inform. Theory, Vol. 30(5), pp. 776-780, 1984.

[27] Solé P., Tokareva N., Connections between quaternary and binary bent functions. Available at, http://www.eprint.iacr.org/2009/544.

[28] Stănică P., Gangopadhyay S., Chaturvedi A., Gangopadhyay A., Maitra S., Investigations on bent and negabent functions via the nega-Hadamard transform, IEEE Trans. Inform. Theory, Vol. 58(6), pp. 4064-4072, 2012.

[29] Su W., Pott A., Tang X., Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree. Available at: arXiv:1205.6568v1 [cs.IT] 2012.

[30] Sun G., Wu C., The lower bounds on the second-order nonlinearity of a class of Boolean functions with high nonlinearity, Appli. Alg. in Eng. Commu. Comp., Vol. 22, pp. 37-45, 2011.

[31] Tokareva N., Generalizations of bent functions: A survey. Journal of Applied and Industrial Mathematics Vol. 5(1), pp. 110-129, 2011.

[32] Webster A.F., Tavares S.E., On the design of S-boxes, In Advances in Cryptology-CRYPTO'85, LNCS, Springer, Heidelberg, New York, Vol. 219, pp. 523-534, 1986.

[33] Zhang X. M., Zheng Y., GAC- the criterion for global acalanche criteria of cryptographic functions, J. Univ. Comp. Sci., Vol. 1(5), pp. 316-333, 1995.

[34] Zhou Y., Xie M., Xiao G., On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, Inform. Sci., Vol. 180, pp. 256-265, 2010.