WALAILAK JOURNAL
http://wjst.wu.ac.th Applied Sciences

New Constructions of Balanced Boolean Functions with Maximum Algebraic Immunity, High Nonlinearity and Optimal Algebraic Degree

Dheeraj Kumar SHARMA[*] and Rajoo PANDEY

Department of Electronics & Communication Engineering, National Institute of Technology Kurukshetra, 136119, India

([*]Corresponding author's e-mail: sharma987dheeraj@gmail.com)

Received: 27 August 2018, Revised: 1 April 2019, Accepted: 30 May 2019

Abstract

This paper consists of proposal of two new constructions of balanced Boolean function achieving a new lower bound of nonlinearity along with high algebraic degree and optimal or highest algebraic immunity. This construction has been made by using representation of Boolean function with primitive elements. Galois Field, F_{2^n} used in this representation has been constructed by using powers of primitive element such that greatest common divisor of power and $2^n - 1$ is 1. The constructed balanced $n-$ variable Boolean functions achieve higher nonlinearity, algebraic degree of $n-1$, and algebraic immunity of $\frac{n+1}{2}$ for odd n, $\frac{n}{2}$ for even n. The nonlinearity of Boolean function obtained in the proposed constructions is better as compared to existing Boolean functions available in the literature without adversely affecting other properties such as balancedness, algebraic degree and algebraic immunity.

Keywords: Boolean function, Nonlinearity, Cyclotomic coset, Algebraic degree, Algebraic immunity

Introduction

Boolean functions have been widely used for generation of LFSR based stream ciphers, cryptographic transformations of S-boxes, pseudorandom generators, etc. [1,2]. Various constructions of Boolean function with cryptographic properties, related preliminaries and their applications have been given in [1-37]. Boolean functions should be designed such that these are resistant to well-known cryptographic attacks, such as fast correlation attack, linear approximation attack, algebraic attack, Berlekamp Massey attack, Ronjom Hellseth attack, etc [2-4]. Nonlinearity is one of important cryptographic criteria for construction of Boolean function for higher values of n. It ensures good resistance against linear approximation attack and fast correlation attack. Generally, the Boolean function with lower nonlinearity has lower values of algebraic immunity and algebraic degree. High value of algebraic immunity is required to resist algebraic attack whereas high value of algebraic degree is required to provide good linear complexity [1]. Therefore, higher value of nonlinearity becomes very important cryptographic criterion for Boolean function to provide resistance against algebraic attack, linear approximation attack and fast correlation attack. It is also important to have high linear complexity. The Boolean functions with highest value of nonlinearity are called as bent functions. Yet, bent functions are not balanced. The Boolean functions are required to be balanced for keeping the pseudorandomness of generated sequence. From the above discussion, it is clear that constructing Boolean functions with higher nonlinearity, balancedness, higher algebraic degree and optimal or high algebraic immunity is highly desirable. However, there is trade-off among these cryptographic properties of Boolean function [1]. Therefore, it is a difficult task to construct a Boolean function with good values of these properties. In this paper, we have proposed two constructions of balanced Boolean function with a new lower bound of nonlinearity, high value of algebraic degree and optimal or highest achievable algebraic immunity. The

constructed balanced Boolean functions have achieved greater value of nonlinearity with high algebraic degree of $n-1$ and optimal or highest algebraic immunity of $\left\lceil \frac{n}{2} \right\rceil$. The proposed work demonstrates that it is possible to construct Boolean functions with good trade-off of cryptographic properties and these Boolean functions achieve the greater value of nonlinearity as compared to previous papers without compromising on other properties. To the best of our knowledge, it has not been shown previously in the literature.

In [5], the standard algebraic attack on stream ciphers has been proposed. Then, the concept of algebraic immunity was introduced in [6]. The algebraic immunity of a Boolean function should be high to resist the standard algebraic attack. Similarly, fast algebraic attack was also investigated in [11,14,15,23,24]. The Boolean functions proposed in various constructions in [15,25-32] have optimal algebraic immunity. Nevertheless, the nonlinearities of these Boolean functions are not much higher in order to resist the related attacks. A family of balanced Boolean functions with high nonlinearity, optimal algebraic immunity, optimal algebraic degree, and good resistance to fast algebraic attack has been proposed in [8], where support set defined using primitive element, α of F_{2^n} and support set $= \{x \in F_2^n | f(x) = 1\}$. A family of balanced Boolean functions for even n has been proposed in [33]. These Boolean functions possess high nonlinearity and optimal algebraic immunity. A class of $2k$-variable balanced Boolean functions with optimal algebraic immunity by using Dobbertin's iterative construction has been suggested in [34]. These Boolean functions have high nonlinearity and optimal algebraic degree. However, the functions in [33,34] are not resistant to fast algebraic attacks [35,36]. Three classes of balanced Boolean functions with optimal algebraic immunity has been proposed in [22]. The Boolean functions also possess high nonlinearity and optimal algebraic degree. In [18], three constructions of balanced Boolean functions with relevant cryptographic properties have been proposed. Boolean functions in [18] contain the functions in [8] as a subclass. Authors in [16] also presented a family of balanced Boolean functions. These functions are with optimal algebraic immunity in an even n. They also possess good resistance to fast algebraic attacks and have higher nonlinearity that is comparable with that of the functions in [8].

In [13], a framework for assessing the immunity against algebraic attacks using univariate representation of Boolean functions has been provided. It has been carried out by defining a matrix representation of annihilators. In [13], two families of Boolean functions with optimal algebraic immunity have also been proposed. In [18], authors have used the matrix representation defined in [13] and proposed three constructions of balanced Boolean functions with optimal algebraic immunity using two disjoint subsets $\{(W^0 \backslash Y^0) \cup I^0\}$ and $\{(W_0 \backslash Y_0) \cup I_0\}$. Support set of family of Boolean functions in [18] is also defined by using primitive element, α of F_{2^n}.

In this paper, it has been verified on SAGE that finite field F_{2^n} can also be formed by using powers of primitive elements. By using powers of primitive elements, we have proposed two constructions of balanced Boolean functions. The power of primitive element is taken to be co-prime with respect to $2^n - 1$. It has been given in [20] that all the elements of F_{2^n} can be obtained by considering the powers of first primitive element α^a such that greatest common divisor of a and $2^n - 1$ is 1, i.e $gcd(a, 2^n - 1) = 1$. Therefore, α^a can be considered as generator of non-zero elements of F_{2^n}. These constructions are also defined by using two disjoint subsets. The lower bound of nonlinearity of proposed Boolean functions for $n = 17, 19$ are better as compared to that of [8,16,18,22,37]. The nonlinearity of Boolean functions for $n = 8, 10, 11, 13, 14, 15, 16, 17, 19$ in Construction 1 and Construction 2 is greater than that of Boolean functions of previous papers [8,16,18,37]. These families of balanced Boolean functions have higher nonlinearity, optimal algebraic immunity, and algebraic degree of $n - 1$.

In Section 2 of this paper, preliminaries related to Boolean function are defined. In Section 3, two constructions of a family of Boolean functions are presented. The nonlinearity of Boolean function is calculated in Section 4. In Section 5, algebraic degree and algebraic immunity of Boolean function are obtained. Section 6 consists of conclusion and future work.

Preliminaries

The list of various symbols used in this paper has been provided in **Table 1**.

Table 1 List of symbols.

Symbol	Description
$\mathbf{F_2}$	Galois Field of Order 2
$\boldsymbol{\alpha}$	primitive element of finite field F_{2^n}
$\mathbf{F_2^n}$	n-dimensional vector space over Galois Field of order 2
$\mathbf{F_{2^n}}$	Finite field of Order 2^n
$\mathbf{F_{2^n}^*}$	Multiplicative group of non-zero elements of F_{2^n}
$\boldsymbol{f(x)}$ or $\boldsymbol{f}$	Boolean function
$\boldsymbol{B_n}$	Set of all n-variable Boolean function
$\boldsymbol{wt(f)}$	Hamming weight of Boolean function f
$\boldsymbol{W_f(\gamma)}$	Walsh-transform of Boolean function f
$\boldsymbol{nl(f)}$	nonlinearity of f
$\boldsymbol{AN(f)}$	Annihilator of f
$\boldsymbol{supp(f)}$	$x \in F_2^n$ such that $f(x) = 1$
$\boldsymbol{d_H(f,g)}$	Hamming distance between Boolean functions f and g
$\boldsymbol{zeros(f)}$	$x \in F_2^n \mid f(x) = 0$
$\boldsymbol{deg\ (f)}$	Algebraic degree of f
$\boldsymbol{Tr(x)}$	Absolute trace of x in finite field
$\boldsymbol{\psi(p^\kappa)}$	Multiplicative character of $F_{2^n}^*$
$\boldsymbol{G(\psi,\mu)}$	Gaussian sum in finite field
$\mathbf{C_S}$	Cyclotomic coset
$\boldsymbol{\mu(x)}$	Canonical additive character of F_{2^n}
$\boldsymbol{\tau(n)}$	Set of all coset leaders $mod 2^n - 1$

The $n-$variable Boolean function is denoted as $f(x_1,x_2,\dots,x_n)$. Boolean function can be represented by its truth table. The last column of its truth table consists of a binary string of its output values. Length of its binary string is equal to $2^n$and all of its output values are the following [18]:

$$f = [f(0,0,\dots,0), f(1,0,\dots,0),\dots, f(1,1,\dots,1)] \quad (1)$$

If output values of Boolean function have equal number of zeros and ones, then the Boolean function is called as balanced. Let B_n be the set of all $n-$variable Boolean function from F_2^n to F_2. Let support set, $supp(f)$ define $x \in F_2^n$ such that $f(x) = 1$, where F_2^n represents $n-$dimensional vector space over Galois Field of order $2, F_2$. It is also hamming weight of $f(x_1,x_2,\dots,x_n)$. Similarly, $zeros(f) = \{x \in F_2^n \mid f(x) = 0\}$ defines zeros of f. In other words, Boolean function can also be termed as balanced if hamming weight of $f(x_1,x_2,\dots,x_n)$ is 2^{n-1} [18]. Let $wt(f)$ denotes the hamming

weight of Boolean function f. Let hamming distance of two functions f and g is represented by $d_H(f,g)$. A univariate polynomial representation of a Boolean function f from F_2^n to F_2 is given by;

$$f(x) = \sum_{i=0}^{2^n-1} f_i x^i \quad (2)$$

where $f_0, f_{2^n-1}$are elements of F_2 and $f_i \in F_{2^n}$ & $f_{2i} = (f_i)^2$, for $1 \le i \le 2^n - 2$. Let $wt_2(i)$ be the hamming weight of binary representation of i, then largest integer $k = \{wt_2(i) | f_i \neq 0\}$ is algebraic degree, $deg\ (f)$of f. If algebraic degree is at most 1, then it is an affine function. The set of possible affine functions is represented by A_n. Let F_{2^n} be a finite field of order $2^n$and α be its primitive element, then $f(x) = \left[f(0),\ f(1),\ f(\alpha), \ldots\ldots,\ f(\alpha^{2^n-2})\right]$ defines Boolean function f.

The nonlinearity of f is defined as minimum hamming distance of f from $g \in A_n$. The nonlinearity of f can be defined in terms of Walsh transform [13]. The Walsh-transform of Boolean function $f(x)$ is given as:

$$W_f(\gamma) = \sum_{x \in F_2^n} (-1)^{f(x)+\gamma.x} \quad (3)$$

where $x = (x_1, \ldots\ldots, x_n)$ and $\gamma = (\gamma_1, \ldots, \gamma_n)$ both be affiliated to vector space F_2^n. The product $\gamma.x$ is an inner product, which is represented in [13] as:

$$\gamma.x = \gamma_1 x_1 + \cdots + \gamma_n x_n \quad (4)$$

If $W_f(0) = 0$, then f is said to be balanced. In terms of Walsh transform, the nonlinearity of Boolean function f is given as:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\gamma \in F_2^n} \left|W_f(\gamma)\right| \quad (5)$$

Consider $\alpha \in F = F_{q^n}$ and $K = F_q$, trace $Tr_{F/K}(\alpha)$ of α over K is defined as $Tr_{F/K}(\alpha) = \alpha + \alpha^q + \ldots\ldots\ldots + \alpha^{q^{n}-1}$. If K is the prime subfield of F, then $Tr_{F/K}(\alpha)$ is called the absolute trace of α and is denoted as $Tr_F(\alpha)$.

Annihilator of f is a Boolean function $g \in B_n$ such that $f * g = 0$ and it is denoted by $AN(f)$. The minimum algebraic degree of all annihilators of f or $f + 1$ is called as Algebraic immunity. For a fast algebraic attack on f, if there are $g \in B_n$ & $0 \neq \{h \in B_n\}$ with $deg(g) \le d_1 < deg(h) \le d_2 < n$, such that $fg = h$, then there is a (d_1, d_2) pair for f.

A cyclotomic coset C_S is described as $C_S = \{s, 2 \cdot s, 2^2 \cdot s, \ldots\ldots,\ 2^{e-1} \cdot s\}$ where $1 \le s \le 2^n - 2$ and e is smallest non-negative integer such that $s \equiv 2^e \cdot s (mod 2^n - 1)$ [13,18]. Coset leader is the smallest integer in C_S and $\tau(n)$ denotes set of all coset leaders $mod 2^n - 1$.

Some definitions have been taken from [13] and [18] in the following discussion. The product of minimal polynomials denoted as $R_b(x)$ is given by:

$$R_b(x) = \prod_{s \in \tau(n), wt(s)=b} m_{2^n-1-s}(x) \quad (6)$$

where $m_{2^n-1-s}(x)$ represents the minimal polynomial of $2^n - 1 - s$ element of F_{2^n}. As given in [20], (6) can be converted as;

$$R_b(x) = \prod_{wt(j)=n-b} (x + \alpha^j) \quad (7)$$

for $1 \le b \le n-1$ and $R_n(x) = R_0(x) = x+1$. Let $R_{d_1,d_2}(x) = \prod_{d=d_1}^{d_2} R_d(x)$ for $0 \le d_1 \le d_2 \le n$. Also, let $\boldsymbol{R}_{b_1+1,b_2}$ be a $B_1 \times B_2$ matrix and $B_1 = \sum_{s=0}^{b_1}\binom{n}{s}$, $B_2 = \sum_{s=0}^{b_2}\binom{n}{s}$ and rth row of matrix consist of the coefficient of polynomial $R_{b_1+1,b_2}(x)$ as given by;

$$R_{b_1+1,b_2}(x) = 1 + r_1 x + r_2 x^2 + \ldots + r_{E-1}x^{E-1} + x^E \tag{8}$$

where $E = \sum_{s=b_1+1}^{b_2}\binom{n}{s}$ and matrix $\boldsymbol{R}_{b_1+1,b_2}$ is defined by:

$$\begin{pmatrix} r_0 & r_1 & \cdots & r_E & 0 & \ldots & 0 \\ 0 & r_0 & & r_{E-1} & r_E & \ldots\ldots & 0 \\ \vdots & \vdots & \ldots & & \vdots & \ldots & \\ 0 & 0 & \cdots & \vdots\ \vdots & \ldots & & 0 \\ 0 & 0 & & 0\ \vdots & \ldots & & r_E \end{pmatrix} \tag{9}$$

The matrix $\boldsymbol{R}_{b_1+1,b_2}$ for $1 \le b_1 < b_2 \le n-1$ is defined as:

$$\boldsymbol{R}_{b_1+1,b_2} = [\boldsymbol{\varphi}_0, \boldsymbol{\varphi}_1, \ldots, \boldsymbol{\varphi}_{B_2-1}] \tag{10}$$

where vector $\boldsymbol{\varphi}_s$ represents sth column of $\boldsymbol{R}_{b_1+1,b_2}$ for $0 \le s \le B_2 - 1$ and jth component of $\boldsymbol{\varphi}_s$ represented by $\boldsymbol{\varphi}_s^j$ for $0 \le s \le B_1$.

Let $N^0(\boldsymbol{\varphi}_s) = l_1$ for $\boldsymbol{\varphi}_s^j = 0$ and $\boldsymbol{\varphi}_s^{l_1} = 1$, whenever a positive integer l_1 occurs for $0 \le j < l_1$ (if l_1 exists). Similarly we can also define $N_0(\boldsymbol{\varphi}_s) = l_2$ for $\boldsymbol{\varphi}_s^{B_1-1-j} = 0$ and $\boldsymbol{\varphi}_s^{B_1-1-l_2} = 1$, whenever a positive integer l_2 occurs for $0 \le j < l_2$. Let us consider a specific case $N^0(\boldsymbol{\varphi}_s) = 0$ if $\boldsymbol{\varphi}_s^0 = 1$ and $N_0(\boldsymbol{\varphi}_s) = 0$ if $\boldsymbol{\varphi}_s^{B_1-1} = 1$ [7]. Now, for $0 \le j \le B_1 - 1$, two set H^j and H_j are expressed as:

$$H^j = \{s | N^0(\boldsymbol{\varphi}_s) = \mathrm{j}, 0 \le \mathrm{s} \le 2^{\mathrm{n}-1} - 2\} \tag{11}$$

$$H_j = \{s | N_0(\boldsymbol{\varphi}_s) = \mathrm{j}, 2^{\mathrm{n}-1} - 1 \le \mathrm{s} \le 2^{\mathrm{n}} - 2\} \tag{12}$$

For $0 \le j \le B_1 - 1$, let I^0 and I_0 be two subsets such as;

$$I^0 = \{j | H^j \ne \emptyset, 0 \le j < B_1\} \tag{13}$$

$$I_0 = \{j | H_j \ne \emptyset, 0 \le j < B_1\} \tag{14}$$

and J^1 be a subset of I^0. For each $j \in J^1$, consider one integer i^j from the set H^j and define the set;

$$K^0 = \{i^j | j \in J^1\} \tag{15}$$

Construction of Boolean functions

In this section, two constructions of $n-$variable Boolean function f has been proposed by using powers of primitive elements of $\mathrm{F}_{2^{\mathrm{n}}}$. The power of primitive element is taken to be co-prime with respect to $2^n - 1$. It has been given in [20] that all the elements of $\mathrm{F}_{2^{\mathrm{n}}}$ can be obtained by considering the powers of first primitive element α^a such that greatest common divisor of a and $2^n - 1$ is 1, i.e $gcd(a, 2^n - 1) = 1$. Therefore, α^a can be considered as generator of non-zero elements of $\mathrm{F}_{2^{\mathrm{n}}}$. For the constructions, following sets P^0, Q^0 has been used:

$$P^0 = \{s | 0 \leq s \leq B_1 - 1\} \quad (16)$$

$$Q^0 = \{B_1 - 1 - j | j \in J^1\} \quad (17)$$

Using these sets, we propose two constructions of balanced Boolean functions and these two constructions are defined as:

Construction 1 Consider $f \in B_n$ for odd n such that;

$$supp(f) = \{\alpha^{sn} | s \in (P^0 \setminus Q^0) \cup K^0\} \quad (18)$$

Construction 2: Consider $f \in B_n$ for even n such that;

$$supp(f) = \{\alpha^{sn} | s \in (P^0 \setminus Q^0) \cup K^0\} \quad (19)$$

where P^0, Q^0 and K^0 are given by Eqs. (16), (17) and (15), respectively. These Boolean functions in Construction 1 and Construction 2 are balanced because $supp(f)$ has 2^{n-1} elements.

Note: Construction 1 and Construction 2 are the special case of Construction 1 and Construction 3 of [18] for which primitive element is taken to be α^n of F_{2^n}.

For Construction 1, $supp(f) = \{\alpha^{sn} | s \in (P^0 \setminus Q^0) \cup K^0\}$, then the Boolean function f will have different truth table as compared to Boolean function f of Construction 1 of [18]. Similarly, for Boolean function f of Construction 2, the truth table will be different of Boolean function f of Construction 3 of [18].

It has been checked by using SAGE program that the set $F = \{0, 1, \alpha^n, \alpha^{2n}, \ldots, \alpha^{(2^n-2)n}\}$ for $n = 5, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 19$ is a Galois field of 2^n elements, F_{2^n} for the following primitive polynomials $p_n(x)$ as given in **Table 2**.

Table 2 Primitive polynomials used for $n = 5, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 19$.

n	$p_n(x)$
5	$x^5 + x^2 + 1$
7	$x^7 + x + 1$
8	$x^8 + x^6 + x^5 + x + 1$
9	$x^9 + x^4 + 1$
10	$x^{10} + x^3 + 1$
11	$x^{11} + x^2 + 1$
13	$x^{13} + x^4 + x^3 + x + 1$
14	$x^{14} + x^{12} + x^{11} + x + 1$
15	$x^{15} + x + 1$
16	$x^{16} + x^5 + x^3 + x^2 + 1$
17	$x^{17} + x^3 + 1$
19	$x^{19} + x^6 + x^5 + x + 1$

Consider the following example for $n = 4$. It will explain the set F.

Example 1 Consider a Galois Field F_{2^4} generated by $p_4(x) = x^4 + x + 1$. The powers of $\sigma = \alpha^4$ are $\sigma^0 = 1,\ \sigma^1 = \alpha^4,\ \sigma^2 = p^8,\ \sigma^3 = \alpha^{12},\ \sigma^4 = \alpha^{16} = \alpha, \sigma^5 = \alpha = \alpha^5, \sigma^6 = \alpha^{24} = \alpha^9, \sigma^7 = \alpha^{28} = \alpha^{13},$ $\sigma^8 = \alpha^{32} = \alpha^2, \sigma^9 = \alpha^{36} = \alpha^6, \sigma^{10} = \alpha^{40} = \alpha^{10}, \sigma^{11} = \alpha^{44} = \alpha^{14}, \sigma^{12} = \alpha^{48} = \alpha^3, \sigma^{13} = \alpha^{52} = \alpha^7, \sigma^{14} = \alpha^{56} = \alpha^{11}, \quad \sigma^{15} = \alpha^{60} = 1.$
Since powers of $\sigma = \alpha^4$ generate all the nonzero elements of F_{2^n}, $\sigma = \alpha^4$ becomes a primitive element of F_{2^4}.

We use the following lemma to provide relationship between r_1 and r_{E-1} coefficients of (8).

Lemma 1 [18] $r_1 + r_{E-1} = 1$.
Proof. The proof is available in [18].

This lemma shows that $(r_1, r_{E-1}) = (0,1)\ or\ (1,0)$, thereby existing one integer L_1 such that $r_s = 0$ for all $1 \le s \le L_1$ and $r_{L_1+1} = 1$, if $r_1 = 0$. Otherwise, one integer L_2 exist such that $r_{E-s} = 0$ for all $1 \le s \le L_2$ and $r_{E-L_2-1} = 1$. The set J is defined in [18] as:

$J = \{1, 2, \dots, L_1\},$ if $r_1 = 0$;
$J = \{1, 2, \dots, L_2\},$ if $r_{E-1} = 0$. (20)

Therefore, from Lemma 1, we can say that set J is nonempty. Let K be a subset of J and now define set W, Y and Z for $r_{E-1} = 0$ as;

$W = \{0, 1, 2, \dots., 2^{n-1} - 1\},\ Y = \{2^n - 2 - s \mid s \in \mathrm{K}\},\ Z = \{2^{n-1} - 1 - s \mid s \in \mathrm{K}\}.$ (21)

With the help of above analysis, we can represent a family of constructed Boolean function with support set as;

$$supp(f) = \{\alpha^{sn} | s \in (W \setminus Z) \cup Y\} \quad (22)$$

For $r_{E-1} = 0$, we take $W = P^0$, $Z = Q^0$ and $Y = K^0$; thus, this family of Boolean functions belongs to Construction 1 and Construction 2 for odd and even n. Therefore, we can say that this family of Boolean functions are balanced. In the similar way, we can define sets for $r_1 = 0$, and get a new family of Boolean functions. The proposed approach for constructions of Boolean function is described as a flowchart in **Figure 1**.

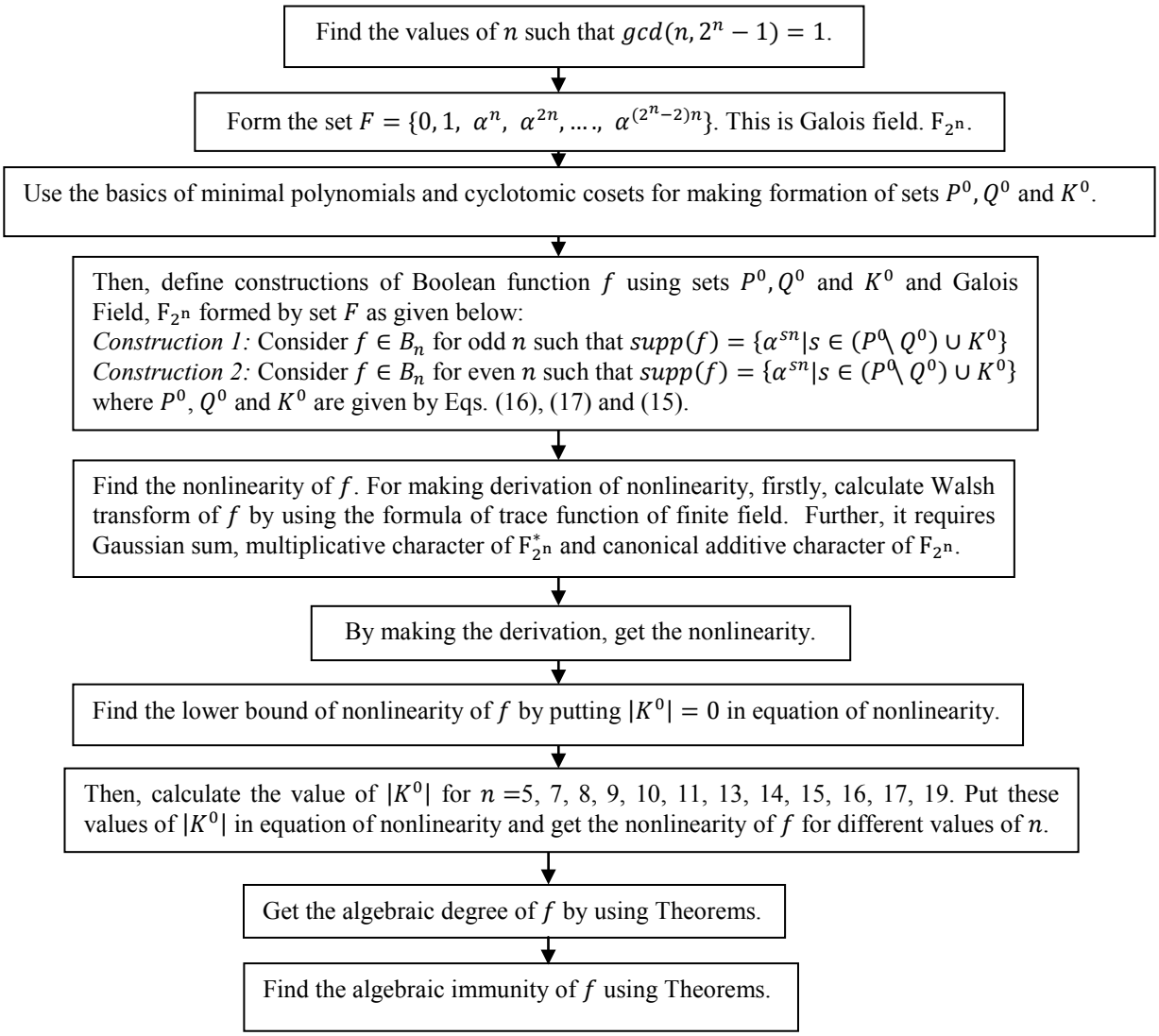

Figure 1 Flowchart showing various steps in the construction of Boolean function.

Nonlinearity of Boolean function *f*

This section consists of derivation of lower bound of nonlinearity of Boolean functions in Construction 1 and Construction 2. We have used the method developed in the paper [18]. In this method, we have used trace function for finding Walsh transform. Then, we have derived the lower bound of nonlinearity of Boolean function by using (5). To calculate the Walsh transform, following lemma of [16] from calculus theory has been used.

Lemma 2 [13] For $0 < z < \frac{\pi}{2}$, $\frac{1}{\sin(z)} < \frac{1}{z} + \frac{z}{4}$.

Theorem 1 The nonlinearity of Boolean functions in Construction 1 and Construction 2 is given by;

$$nl(f) > 2^{n-1} - \frac{2^{\frac{n}{2}+1}}{2^n-1}\left[\frac{(2^n-1)}{2\pi} ln2 + \frac{n\pi 2^{2n-4}}{4(2^n-1)} + \frac{(2^{n-1}-1)}{n}\left(\frac{1}{3\sqrt{3}} + \frac{(3n-2)}{6\sqrt{2}}\right) - \frac{(n+2)}{2\sqrt{2}n}\right] - 2|K^0| - 1$$

Proof. According to (5), for finding the nonlinearity of a Boolean function, we have to find the Walsh transform of Boolean function. Since, $W_f(0) = 0$ for balanced Boolean function, therefore, it is enough to find Walsh transform for $\gamma \in \mathrm{F}_{2^n}^*$ where $\mathrm{F}_{2^n}^*$ is the multiplicative group of non zero elements of F_{2^n}. For $r_{E-1} = 0$, Walsh-transform of Boolean functions f satisfies;

$$W_f(\gamma) = -2\sum_{s\in(W\setminus Y)\cup Z}(-1)^{Tr(\gamma\alpha^{sn})} \tag{23}$$

And then for Boolean function f;

$$\left|W_f(\gamma)\right| \le 2\left|\sum_{s=0}^{2^{n-1}-1}(-1)^{Tr(\gamma\alpha^{sn})}\right| + 4|K^0| \tag{24}$$

For solving above equation, we will use Gaussian sums, which are one of the important types of exponential sums of finite fields [20]. Let $\varepsilon = e^{\frac{2\pi\sqrt{-1}}{2^n-1}}$ and $\gamma = \alpha^t$. Let multiplicative character of $\mathrm{F}_{2^n}^*$ be given by $\psi(\alpha^\kappa) = \varepsilon^\kappa$ with $0 \le \kappa \le 2^n - 2$, canonical additive character of F_{2^n} is given by $\mu(x) = (-1)^{Tr(x)}$. The Gaussian sum $G(\psi, \mu)$ is defined as;

$$G(\psi, \mu) = \sum_{s=0}^{2^n-2}\psi(\alpha^{sn})\mu(\alpha^{sn}) \tag{25}$$

and;

$$\mu(\alpha^{sn}) = (-1)^{Tr(\alpha^{sn})} = \frac{1}{2^n-1}\sum_{\kappa=0}^{2^n-2} G(\bar{\psi}^\kappa, \mu)\,\psi^k(\alpha^{sn}) \tag{26}$$

for $0 \le s \le 2^n - 2$ and bar in above equation denotes complex conjugation.
By (24) and (25), Walsh transform is represented by the following expression;

$$\left|W_f(\gamma)\right| \le \frac{2}{2^n-1}\left|\sum_{\kappa=0}^{2^n-2} G(\bar{\psi}^\kappa, \mu)\sum_{s=0}^{2^{n-1}-1}\psi^\kappa(\alpha^{t+sn})\right| + 4|K^0| \tag{27}$$

and;

$$\sum_{s=0}^{2^{n-1}-1}\psi^\kappa(\alpha^{t+sn}) = \varepsilon^{t\kappa}\left(\frac{1-\varepsilon^{\kappa n 2^{n-1}}}{1-\varepsilon^{\kappa n}}\right). \tag{28}$$

Putting this expression in (10);

$$\left|W_f(\gamma)\right| \le \frac{2}{2^n-1}\left|\sum_{\kappa=1}^{2^n-2} G(\bar{\psi}^\kappa, \mu)\varepsilon^{\kappa t}\left(\frac{1-\varepsilon^{\kappa n 2^{n-1}}}{1-\varepsilon^{\kappa n}}\right)\right| + 4|K^0| + \frac{2^n}{2^n-1} \tag{29}$$

As given in [18], $G(\bar{\psi}^0, \mu) = -1$, $\left|G(\bar{\psi}^k, \mu)\right| = 2^{\frac{n}{2}}$ for all $1 \le k \le 2^n - 2$ and;

$$\left|\frac{1-\varepsilon^{\kappa n 2^{n-1}}}{1-\varepsilon^{\kappa n}}\right| = \left|\frac{\varepsilon^{-\kappa n 2^{n-2}} - \varepsilon^{\kappa n 2^{n-2}}}{\varepsilon^{-\kappa n/2} - \varepsilon^{\kappa n/2}}\right| = \left|\frac{\sin\frac{\kappa n\pi 2^{n-1}}{2^n-1}}{\sin\frac{\kappa n\pi}{2^n-1}}\right| \tag{30}$$

By putting above values in (29), Walsh-transform is given by;

$$|W_f(\gamma)| \le \frac{2^{\frac{n}{2}+1}}{2^n-1}\left(\sum_{\kappa=1}^{2^{n-2}}\left|\frac{\sin\frac{\kappa n\pi 2^{n-1}}{2^n-1}}{\sin\frac{\kappa n\pi}{2^n-1}}\right|\right) + 4|K^0| + \frac{2^n}{2^n-1}$$
$$\le \frac{2^{\frac{n}{2}+2}}{2^n-1}\sum_{\kappa=1}^{2^{n-1}-1}\left|\frac{\sin\frac{\kappa n\pi 2^{n-1}}{2^n-1}}{\sin\frac{\kappa n\pi}{2^n-1}}\right| + 4|K^0| + \frac{2^n}{2^n-1}$$
$$|W_f(\gamma)| \le \frac{2^{\frac{n}{2}+2}}{2^n-1}\left(\sum_{\kappa=1}^{2^{n-2}}\frac{1}{\sin\frac{(2\kappa-1)n\pi}{2^n-1}} + \sum_{\kappa=1}^{2^{n-2}-1}\frac{1}{2\cos\frac{\kappa n\pi}{2^n-1}}\right) + 4|K^0| + \frac{2^n}{2^n-1}. \quad (31)$$

By using Lemma 2, we have;

$$\sum_{\kappa=1}^{2^{n-2}}\frac{1}{\sin\frac{(2\kappa-1)n\pi}{2^n-1}} \le \sum_{\kappa=1}^{2^{n-2}}\frac{2^n-1}{(2k-1)n\pi} + \frac{1}{4}\sum_{\kappa=1}^{2^{n-2}}\frac{(2k-1)n\pi}{2^n-1}$$
$$< \frac{(2^n-1)}{n\pi}\sum_{\kappa=1}^{2^{n-2}}\frac{1}{(2k-1)} + \frac{n\pi}{4(2^n-1)}\sum_{\kappa=1}^{2^{n-2}}(2k-1)$$
$$< \frac{(2^n-1)}{n\pi}\left[\sum_{\kappa=1}^{2^{n-2}}\left(\frac{1}{(2k-1)}+\frac{1}{2k}-\frac{1}{2k}\right)\right] + \frac{n\pi}{2(2^n-1)}\sum_{\kappa=1}^{2^{n-2}}k - \frac{n\pi 2^{n-2}}{4(2^n-1)}$$
$$< \frac{(2^n-1)}{n\pi}\left[\sum_{\kappa=1}^{2^{n-2}}\left(\frac{1}{(2k-1)}+\frac{1}{2k}\right) - \frac{1}{2}\sum_{\kappa=1}^{2^{n-2}}\frac{1}{k}\right] + \frac{n\pi}{2(2^n-1)}\frac{2^{n-2}(2^{n-2}+1)}{2} - \frac{n\pi 2^{n-2}}{4(2^n-1)}$$

$$< \frac{(2^n-1)}{n\pi}\left[\sum_{\kappa=1}^{2^{n-1}}\frac{1}{k} - \frac{1}{2}\int_{k=1}^{2^{n-2}}\frac{dk}{k}\right] + \frac{n\pi}{4(2^n-1)}[2^{2n-4}+2^{n-2}-2^{n-2}]$$
$$< \frac{(2^n-1)}{n\pi}\left[\int_{k=1}^{2^{n-1}}\frac{dk}{k} - \frac{n-2}{2}ln2\right] + \frac{n\pi}{4(2^n-1)}[2^{2n-4}]$$
$$< \frac{(2^n-1)}{n\pi}\left[(n-1)ln2 - \frac{n-2}{2}ln2\right] + \frac{n\pi 2^{2n-4}}{4(2^n-1)}$$
$$< \frac{(2^n-1)}{n\pi}\left[\frac{n}{2}ln2\right] + \frac{n\pi 2^{2n-4}}{4(2^n-1)}$$
$$\sum_{\kappa=1}^{2^{n-2}}\frac{1}{\sin\frac{(2\kappa-1)n\pi}{2^n-1}} < \frac{(2^n-1)}{2\pi}ln2 + \frac{n\pi 2^{2n-4}}{4(2^n-1)} \quad (32)$$

And the expression of other summation in (31) is given as;

$$\sum_{\kappa=1}^{2^{n-2}-1}\frac{1}{2\cos\frac{\kappa n\pi}{2^n-1}} < \sum_{j=1}^{\frac{2^{n-1}-1}{3n}}\frac{1}{2\cos\frac{\pi}{6}} + \sum_{j=\frac{2^{n-1}+2}{3n}}^{2^{n-2}-1}\frac{1}{2\cos\frac{\pi}{4}}$$
$$< \left[\frac{2^{n-1}-1}{3\sqrt{3}n}\right] + \frac{1}{\sqrt{2}}\left[2^{n-2}-1-\frac{2^{n-1}+2}{3n}\right]$$
$$< \frac{1}{3\sqrt{3}n}[2^{n-1}-1] + \frac{1}{\sqrt{2}}\left[\frac{2^{n-1}}{2}-1-\frac{2^{n-1}-1}{3n}-\frac{1}{n}\right]$$
$$< \frac{1}{3\sqrt{3}n}[2^{n-1}-1] + \frac{1}{\sqrt{2}}\left[\frac{2^{n-1}-1}{2}-\frac{1}{2}-\frac{2^{n-1}-1}{3n}-\frac{1}{n}\right]$$
$$< \frac{1}{3\sqrt{3}n}[2^{n-1}-1] + \frac{1}{\sqrt{2}}\left[(2^{n-1}-1)\left[\frac{1}{2}-\frac{1}{3n}\right]-\frac{1}{2}-\frac{1}{n}\right]$$
$$\sum_{\kappa=1}^{2^{n-2}-1}\frac{1}{2\cos\frac{\kappa n\pi}{2^n-1}} < \frac{(2^{n-1}-1)}{n}\left[\frac{1}{3\sqrt{3}}+\frac{(3n-2)}{6\sqrt{2}}\right] - \frac{(n+2)}{2\sqrt{2}n} \quad (33)$$

From (31), (32) and (33), Walsh-transform for $\gamma \in \mathrm{F}_{2^n}^*$ is given by;

$$|W_f(\gamma)| \le \frac{2^{\frac{n}{2}+2}}{2^n-1}\left[\frac{(2^n-1)}{2\pi}ln2 + \frac{n\pi 2^{2(n-2)}}{4(2^n-1)} + \frac{(2^{n-1}-1)}{n}\left(\frac{1}{3\sqrt{3}}+\frac{(3n-2)}{6\sqrt{2}}\right) - \frac{(n+2)}{2\sqrt{2}n}\right] + 4|K^0| + \frac{2^n}{2^n-1} \quad (34)$$

Since, $W_f(0) = 0$ for balanced Boolean function. Therefore, by using (5), the nonlinearity of Boolean function f in Construction 1 and Construction 2 is provided as $nl(f) = 2^{n-1} - \frac{1}{2}\max_{\gamma\in\mathrm{F}_2^n}|W_f(\gamma)|$. Substituting (34) in above equation, we get;

$$nl(f) > 2^{n-1} - \frac{2^{\frac{n}{2}+1}}{2^n-1}\left[\frac{(2^n-1)}{2\pi} ln2 + \frac{n\pi 2^{2n-4}}{4(2^n-1)} + \frac{(2^{n-1}-1)}{n}\left(\frac{1}{3\sqrt{3}} + \frac{(3n-2)}{6\sqrt{2}}\right) - \frac{(n+2)}{2\sqrt{2}n}\right] - 2|K^0| - 1 \quad (35)$$

By making similar analysis for $r_1 = 0$ and $\gamma \in F_{2^n}^*$, same equation as above for $nl(f)$ will be obtained. However, in the case of $r_1 = 0$, sets S, Y and Z will be different from $r_{E-1} = 0$. This is left as an open problem to find the lower bound of nonlinearity.

Table 3 Comparison of lower bound of nonlinearity of f from previous papers.

n	The bound in [8]	The bound in [22]	The bound in [18]	The bound in [16]	The bound in [37]	The bound from Theorem 1 with $\|K^0\| = 0$
5	1.763363407	2.286675194	3.302582586		5.101344930	3.6568
7	26.36971911	31.34530696	34.37712174		37.73859719	35.079
8	68.09659747	78.12250526	82.82435241	86.91864318	87.54131214	84.1306
9	161.6849643	180.2345270	187.2981566		193.9992625	189.7118
10	364.8920089	397.4578707	407.8615650	416.716608	417.4653787	412.1732
11	796.3883648	851.5568804	866.6841395		880.5305827	874.1389
13	3561.877002	3709.289413	3740.543932		3769.622283	3761.1992
14	7380.562538	7615.534364	7660.149141	7700.901005	7702.398012	7693.5650
15	15156.98621	15526.93013	15590.43917		15651.86605	15643.7293
16	30920.18676	31496.77161	31587.00116	31673.83658	31676.33065	31670.9864
17	62763.45267	63654.56287	63782.58095		63912.47489	**63913.6403**
19	255960.8738	258046.5310	258303.5671		258577.9353	**258615.2095**

The lower bound of nonlinearity of f in Construction 1 and Construction 2 can be calculated by using $|K^0| = 0$ in (35). Some values of the lower bound of nonlinearity for different values of n and their comparison with previous papers have been listed in **Table 3**. A brief analysis of the results shown in **Table 3** is provided here. In [8], the lower bound of nonlinearity is found to be $2^{n-1} + \frac{2^{n/2+1}}{\pi} \ln\left(\frac{\pi}{4(2^n-1)}\right) - 1$ and its values have been shown in second column in **Table 3**. The lower bound is improved to $2^{n-1} - \left(\frac{\ln 2}{3}(n-1) + \frac{3}{2}\right)2^{\frac{n}{2}}$ in [22] and its corresponding values for different n are given in third column in **Table 3**. The lower bound is further improved to $2^{n-1} - \left(\frac{\ln 2}{3}(n-1) + \frac{5}{6} + \frac{1}{3\sqrt{3}} + \frac{1}{6\sqrt{2}}\right)2^{\frac{n}{2}} - 1$ in [18] and the corresponding values for different n are recorded in forth column of **Table 3**. The lower bound of nonlinearity is again improved in [16] by making construction of Boolean functions for 2k variables, ie. for even n. In [16], lower bound has been found to be $2^{n-1} - \left(\frac{n \ln 2}{\pi} + 0.74\right)2^{\frac{n}{2}} - 1$. The values of lower bound of nonlinearity of [16] for even n have been shown in fifth column of **Table 3**. These values are greater than those of [8],[22] and [18]. More improvement in the lower bound of nonlinearity is provided in [37] by making similar type of constructions as done in [18] and its bound is raised to $2^{n-1} - \left(\frac{n \ln 2}{\pi} + 0.7322106411\right)2^{\frac{n}{2}} - \frac{2^{n-1}}{2^n-1}$. This value is slightly greater than that of [16]. Corresponding values of lower bound have been shown in sixth column of **Table 3**. The lower bound of this paper has been provided in seventh column of **Table 3**. It can be observed that the lower bound of Boolean function in proposed construction is greater than that of lower bound of previous papers [8,16,18,22] for all given values of n. But it is greater than that of [37] for $n \geq 17$. Although the results in **Table 3** are shown upto $n = 19$, however, it is obvious that the lower bound of nonlinearity will

be greater than all other Boolean functions included in the table for n >19 also when $\gcd(n, 2^n - 1) = 1$. This work can be further extended to find the lower bound for higher values of n. It also shows that for higher values of n, we might achieve good value of nonlinearity without $|K^0|$.

By finding values of $|K^0|$, $nl(f)$ of f in Construction 1 and Construction 2 is calculated for $n = 5$, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 19 as shown in **Table 4**. The $nl(f)$ is also compared with nonlinearity of Boolean functions of previous papers [8,16,18,37]. From **Table 4**, it can be noted that nonlinearity of f is greater than that of Boolean functions for n =8, 10, 11, 13, 14, 15, 16, 17, 19 of previous papers [8,16,18,37] and it is greater or equal to that of [8,16,18,37] for $n = 5$, 7. Therefore, it can be concluded from **Table 4** that nonlinearity of f is either greater or equal to nonlinearity of previous papers [8],[18] and [16] after n >19 also when $\gcd(n, 2^n - 1) = 1$.

Table 4 Comparison of nonlinearity of f from previous papers.

n	Nonlinearity in [8]	Nonlinearity in [18]	Nonlinearity in [16]	Nonlinearity in [37]	Nonlinearity in this paper
5	10	10		12	12
7	54	54		54	54
8	112	114	112	114	**116**
9	232	230		234	**234**
10	478	480	476	478	**484**
11	980	980		980	**988**
13	3988	3988		3988	**4008**
14	8072	8072	8028	8072	**8106**
15	16212	16212		16212	**16266**
16	32530	32530	32508	32530	**32614**
17	65210	65210		65210	**65340**
19	261294	261294		261294	**261606**

Algebraic degree and Algebraic immunity of f

In this section, algebraic degree and algebraic immunity of Boolean function f in Construction 1 and Construction 2 has been found.

Lemma 3 [13] By using univariate polynomial representation, Boolean function f is given by;

$$f(x) = \sum_{s=0}^{2^n-1} f_s x^s \tag{36}$$

and coefficients f_s are specified as $f_s = f(0)$ for $s = 0$, $f_s = F(\alpha^{-s})$ for $1 \le s \le 2^{n-2}$ and $f_s = F(1) + f_0$ for $s = 2^{n-1}$ and $F(x) = \sum_{s=0}^{2^n-2} f(\alpha^{sn}) x^s$.
a) For $1 \le b < n - 1, deg(f) = b$, if following conditions are satisfied:

$$R_{b+1,n+1}(x) | F(x), R_n(x) | F(x) + f(0), \text{ and } R_b(x) \nmid F(x) \tag{37}$$

where symbol "|" represents "factor of" and symbol "∤" represents "not factor of".
b) For $b = n - 1, deg(f) = b$ if the following conditions are satisfied:

$$R_n(x) | F(x) + f(0), \text{ and } R_b(x) \nmid F(x). \tag{38}$$

Using these two conditions, we can find out the algebraic degree of Boolean function.

Theorem 2 [18] There is a Boolean function f with $deg(f) = n-1$, if proper subset of J given by (20) for $r_{E-1} = 0$ is non-empty.
Proof. Using Lemma 3(a), $F(x) + f(0) = \sum_{s=0}^{2^n-2} f(\alpha^{sn}) + f(0) = 0$, if and only if $|\text{supp}(f)| = 2^{n-1}$ is even. Then, always $R_n(x)|F(x) + f(0)$.
Using Lemma 3(b), $deg(f) = n-1$, if and only if $b = n-1$, i.e., $F(x) = \sum_{x\epsilon \text{supp}(f)} x \neq 0$. If $\sum_{x\epsilon \text{supp}(f)} x = 0$, then degree of Boolean function f is less than $n-1$.

Let $\beta \subseteq J$ and an element s is chosen in $J\backslash\beta$ and replace an element s' in β with s, then a Boolean function f' can be constructed from (18) and (19) with the help of subset $\beta' = (\{s\} \cup \beta)\backslash\{s'\}$ of J. For $r_{E-1} = 0$,

$$\sum_{x\in \text{supp}(f')} x = \sum_{x\in \text{supp}(f)} x + \alpha^{n2^{n-1}-n-sn} + \alpha^{n2^n-2n-sn} + \alpha^{n2^{n-1}-n-s'n} + \alpha^{n2^n-2n-s'n}$$
$$\sum_{x\in \text{supp}(f')} x = \left(1 + \alpha^{n2^{n-1}-n}\right)\left(\alpha^{n2^{n-1}-n-sn} + \alpha^{n2^{n-1}-n-s'n}\right) \neq 0 \quad (39)$$

Therefore, by Lemma 3(b), $deg(f') = n-1$, and hence, there is a Boolean function f in the Construction 1 and Construction 2 with $deg(f) = n-1$, if $|J| > 1$.

Lemma 4 (Theorem 4, [13]) An annihilator $g \in AN(f)$ with $deg(g) \leq b < n$ exists for an n-variable Boolean function f, if and only if $\delta_g(b) > 0$, where;

$$\delta_g(b) = \sum_{i=0}^{b} \binom{n}{i} - rank(\boldsymbol{R}^{1_f}_{b+1,n-1}) \quad (40)$$

and $\boldsymbol{R}^{1_f}_{b+1,n-1}$ is specified as submatrix of $\boldsymbol{R}_{b+1,n-1}$for every i^{th}column such that $\alpha^i \in supp(f)$ is contained in $\boldsymbol{R}^{1_f}_{b+1,n-1}$.

It can be proved that there is no annihilator $g \in AN(f)$ with $deg(g) \leq b < \left\lceil \frac{n}{2} \right\rceil$ using Lemma 4, if $\delta_g(b) = 0$ for $b = \left\lceil \frac{n}{2} \right\rceil - 1$.

Lemma 5 (Theorem 5, [13]) An annihilator $h \in AN(f+1)$ with $deg(h) \leq b < n$ exists for an n-variable Boolean function f, if and only if $\delta_h(b) > 0$, where;

$$\delta_h(b) = \sum_{i=0}^{b} \binom{n}{i} - rank([\gamma_{1_f}(b) \quad \boldsymbol{R}^{0_f}_{b+1,n-1}]) \quad (41)$$

$\boldsymbol{R}^{0_f}_{b+1,n-1}$ is a submatrix of $\boldsymbol{R}_{b+1,n-1}$for every i^{th}column such that $\alpha^i \in zeros(f)$ is contained in $\boldsymbol{R}^{0_f}_{b+1,n-1}$and $\gamma_{1_f}(b) = \boldsymbol{R}^{1_f}_{b+1,n-1}.1^T_{|\text{supp}(f)|}$ and $1^T_{|\text{supp}(f)|}$ represents the transpose of the all ones vector with length $|\text{supp}(f)|$.

It can be proved that there is no annihilator $h \in AN(f+1)$ with $deg(h) \leq b < \left\lceil \frac{n}{2} \right\rceil$ using Lemma 5, if $\delta_h(b) = 0$ for $b = \left\lceil \frac{n}{2} \right\rceil - 1$.

Theorem 3 In Construction 1 and Construction 2, the Boolean function f has algebraic immunity $\frac{n+1}{2}$ and $\frac{n}{2}$. The Boolean function f is balanced.
Proof: In Construction 1 and Construction 2, Boolean function defined by (18) and (19) are balanced because $supp(f)$ has 2^{n-1} elements. It will be proved that an n-variable Boolean function f in Construction 1 possess algebraic immunity of $\frac{n+1}{2}$. Let nonzero $g \in AN(f)$. For Construction 1;

$$\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1} = (\boldsymbol{\varphi}_s)_{s\in(P^0\setminus Q^0)\cup K^0} \tag{42}$$

By interchanging the $(B_1 - 1 - j)$th and i^jth columns of $\boldsymbol{R}_{\frac{n+1}{2},n-1}$ for all $j \in J_1$, an upper triangular matrix is obtained consisting of ith column with $0 \leq i < B_1$, since;

$$\mathrm{N}_0(\boldsymbol{\varphi}_{B_1-1-j}) = \mathrm{N}_0(\boldsymbol{\varphi}_{ij}) = j \tag{43}$$

where $j \in J_1$. These upper triangular matrix diagonal elements are 1. Therefore it's invertible. $(\boldsymbol{\varphi}_s)_{s\in(P^0\setminus Q^0)\cup K^0}$ can be used to obtain above upper triangular matrix by using elementary column transformations. Therefore, $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1} = (\boldsymbol{\varphi}_s)_{s\in(P^0\setminus Q^0)\cup K^0}$ achieves full rank i.e. 2^{n-1}. From (40), we get;

$$\delta_g\left(\tfrac{n-1}{2}\right) = \sum_{i=0}^{\frac{n-1}{2}}\binom{n}{i} - rank(\boldsymbol{R}^{1_f}_{b+1,n-1}) = 2^{n-1} - 2^{n-1} = 0.$$

Therefore, by Lemma 4, there does not exist any annihilator $g \in AN(f)$ with $deg(g) \leq \frac{n-1}{2} < n$. Similar analysis can be done for $\boldsymbol{R}^{0_f}_{\frac{n+1}{2},n-1}$ and from (41), we can prove that $\delta_h\left(\frac{n-1}{2}\right) = 0$. Hence, by using Lemma 5, there does not exist any annihilator $h \in AN(f+1)$ with $deg(h) \leq b < n$. Therefore, the algebraic immunity of Boolean function f in Construction 1 is $\frac{n+1}{2}$.
Similarly, it can be proved that the Boolean function f in Construction 2 has algebraic immunity $\frac{n}{2}$.

Conclusions and future work

Two constructions of balanced n-variable Boolean functions with high nonlinearity, maximum algebraic immunity and optimal algebraic degree which are required for cryptographic purpose have been proposed. The lower bound of nonlinearity of Boolean functions in Construction 1 and Construction 2 is greater than that of lower bound of previous papers [8,16,18,22] for all given values of n. But it is greater than that of [37] only for n = 17, 19. The nonlinearity of these Boolean functions is greater than that of [8,16,18,22,37] for n = 8, 9, 10, 11, 13, 14, 15, 16, 17, 19. These Boolean functions have also achieved algebraic degree of $n-1$ and algebraic immunity of $\frac{n+1}{2}$ for odd n, $\frac{n}{2}$ for even n. It is, therefore, concluded that Boolean function in proposed constructions are better suited to provide a higher resistance against linear approximation attack, fast correlation attack, algebraic attack, and to provide high linear complexity in comparison with Boolean functions of [8,16,18,22,37]. The present work can be further extended to find the primitive polynomials such that Boolean function f achieves higher nonlinearity in the proposed constructions. The mathematical analysis of the resistance to algebraic attacks and fast algebraic attacks for proposed Boolean functions can also be carried out.

References

[1] C Carlet. *Boolean Functions for Cryptography and Error Correcting Codes*. Cambridge University Press, Cambridge, 2010.
[2] C Ding, G Xiao and W Shan. *The Stability Theory of Stream Ciphers. In*: Lecture Notes in Computer Science, Springer, Heidelberg, 1991, p. 81-125.
[3] W Meier and O Staffelbach. *Fast Correlation Attacks on Stream Ciphers*. *In*: Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, 1988, p. 301-14.
[4] S Rønjom and T Helleseth. A new attack on the filter generator. *IEEE T. Inform. Theory* 2007; **53**, 1752-8.
[5] N Courtois and W Meier. Algebraic attacks on stream ciphers with linear feedback. *In*: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, 2003, p. 345-59.
[6] W Meier, E Pasalic and C Carlet. Algebraic attacks and decomposition of Boolean functions. *In*: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, 2004, p. 474-91.
[7] K Verma and D K Sharma. New constructions of Boolean functions using cyclotomic cosets. *In*: Proceedings of the 2016 International Conference on Emerging Trends in Communication Technologies (ETCT), IEEE, Dehradun, 2016, p. 1-4.
[8] C Carlet and K Feng. An infinite class of balanced functions with optimal algebraic immunity, Good immunity to fast algebraic attacks and good nonlinearity. *In*: Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, 2008, p. 425-40.
[9] LM Cheng, PD Yi and DY Song. Identification and construction of Boolean functions with maximum algebraic immunity. *Sci. China Inform. Sci.* 2010; **53**, 1379-96.
[10] DY Song and PD Yi. Construction of Boolean functions with maximum algebraic immunity and count of their annihilators at lowest degree. *Sci. China Inform. Sci.* 2010; **53**, 780-7.
[11] F Armknecht. Improving fast algebraic attacks. *In*: Proceedings of the International Workshop on Fast Software Encryption. Springer, Berlin, 2004, p. 65-82.
[12] NT Courtois. Fast algebraic attacks on stream cipher with linear feedback. *In*: Proceedings of the Annual International Cryptology Conference. Springer, Berlin, 2003, p. 176-94.
[13] P Rizomiliotis. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation. *IEEE T. Inform. Theory* 2010; **56**, 4014-24.
[14] P Hawkes and G Rose. Rewriting variables: The complexity of fast algebraic attacks on stream ciphers. *In*: Proceedings of the Annual International Cryptology Conference. Springer, Berlin, 2004, p. 390-406.
[15] C Carlet, DK Dalai, KC Gupta and S Maitra. Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction. *IEEE T. Inform. Theory* 2006; **52**, 3105-21.
[16] D Tang, C Carlet and X Tang. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. *IEEE T. Inform. Theory* 2013; **59**, 653-64.
[17] J Du, S Fu, L Qu, C Li and S Pang. New constructions of q-variable 1-resilient rotation symmetric functions over F_p. *Sci. China Inform. Sci.* 2016; **59**, 1-3.
[18] X Zeng, C Carlet, J Shan and L Hu. More Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks. *IEEE T. Inform. Theory*. 2011; **57**, 6310-20.
[19] G Gao, Y Guo and Y Zhao. Recent result on balanced symmetric Boolean function. *IEEE T. Inform. Theory* 2016; **62**, 5199-203.
[20] R Lidl and H Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, 1986.
[21] S Lin and DJ Costello. *Error Control Coding*. 2nd ed. Pearson Education, New Jersey, 1983.
[22] Q Wang, J Peng, H Kan and X Xue. Construction of cryptographically significant Boolean functions using primitive polynomials. *IEEE T. Inform. Theory* 2010; **56**, 3048-53.

[23] M Liu, Y Zhang and D Liu. Perfect algebraic immune functions. *In*: Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, 2012, p. 172-89.
[24] P Rizomiliotis. On the security of the Feng-Liao-Yang Boolean functions with optimal algebraic immunity against fast algebraic attacks. *Des. Code Cryptogr.* 2010; **57**, 283-92.
[25] A Braeken and B Preneel. On the algebraic immunity of symmetric Boolean functions. *In*: Proceedings of the International Conference on Cryptology in India. Springer, Berlin, 2005, p. 35-48.
[26] C Carlet. A method of construction of balanced functions with optimum algebraic immunity. *In*: Proceedings of the International Workshop on Coding and Cryptology. Wuyishan, China. 2008, p. 25-43.
[27] C Carlet, X Zeng, C Li and L Hu. Further properties of several classes of Boolean functions with optimum algebraic immunity. *Des. Code. Cryptogr.* 2009; **52**, 303-38.
[28] D K Dalai, K C Gupta and S Maitra. Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity. *In*: Proceedings of the International Workshop on Fast Software Encryption. Springer, Berlin, 2005. p. 98-111.
[29] D K Dalai, S Maitra and S Sarkar. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. *Des. Code Cryptogr.* 2006; **40**, 41-58.
[30] N Li and W Qi. Construction and analysis of Boolean functions of 2t+1 variables with maximum algebraic immunity. *In*: Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, 2006, p. 84-98.
[31] N Li, L Qu, W Qi, G Feng, C Li and D Xie. On the construction of Boolean functions with optimal algebraic immunity. *IEEE T. Inform. Theory* 2008; **54**, 1330-4.
[32] L Qu, K Feng, F Liu and L Wang. Constructing symmetric Boolean functions with maximum algebraic immunity. *IEEE T. Inform. Theory* 2009; **55**, 2406-12.
[33] Z Tu and Y Deng. A conjecture on binary string and its applications on constructing Boolean functions of optimal algebraic immunity. *Des. Code Cryptogr.* 2011; **60**, 1-14.
[34] X Tang, D Tang, X Zeng and L Hu. Balanced Boolean functions with (almost) optimal algebraic immunity and very high nonlinearity. Available at: https://eprint.iacr.org/2010/443.pdf, accessed December 2010.
[35] C Carlet. On a weakness of the Tu-Deng function and its repair. Available at: https://eprint.iacr.org/2009/606.pdf, accessed December 2009.
[36] Q Wang and T Johansson. A note on fast algebraic attacks and higher order nonlinearities. *In*: Proceedings of the International Conference on Information Security and Cryptology. Springer, Berlin, 2010. p. 84-98.
[37] J Li, C Carlet, X Zeng, C Li, L Hu and J Shan. Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks. *Des. Code Cryptogr.* 2015; **76**, 279-305.