Chapter 2

Cryptographically Secure Boolean Functions

2.1 Introduction

Boolean functions are used in modern cryptosystems for providing confusion and diffusion. Several criteria for Boolean functions have been established over years by cryptographic community to achieve required security against various attacks such as algebraic attacks, correlation attacks, linear and differential attacks. These criteria include nonlinearity, avalanche criterion and correlation immunity and the like. The chapter is an attempt to present state of the art on properties of such Boolean functions and to suggest several directions for further research. Linear (non-linear) Feedback Shift Registers and Boolean functions are important building blocks for stream cipher systems. A standard model of stream cipher [12] [13] combines the outputs of several independent LFSR sequences using a non-linear Boolean function to produce the keystream. For the design of secure stream ciphers, one has to analyze different cryptographic properties of Boolean functions. In section 2.2 we give an insight into Boolean functions and its different forms of representations. Different complexity measures of Boolean functions are given in section 2.3 and the bounds and relations on these are detailed in section 2.4.


2.2 Representation of Boolean Functions

Boolean functions play a major role in the security of stream and block ciphers. Let \( n \) be a positive integer and \( B_n \) be the set of all \( n \)-variable Boolean functions defined over the vector space \( \mathbb{F}_2^n \) to \( \mathbb{F}_2 \). We denote \( \oplus \) for the addition in \( \mathbb{F}_2 \).

**Definition 2.2.1.** (Boolean Function). A Boolean function is a function \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) represented as a polynomial over \( \mathbb{F}_2 \) as

\[
f(x_1, x_2, \ldots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u, \quad a_u \in \mathbb{F}_2, \quad x, u \in \mathbb{F}_2^n.
\]

This representation is known as algebraic normal form (ANF) and its degree is called the algebraic degree. The Boolean functions whose algebraic degree do not exceed 1 are called the affine functions. The truth table (TT) of an \( n \)-variable Boolean function is the \( 2^n \) binary (0-1) sequence \((f(V_0), f(V_1), \ldots, f(V_{2^n-1}))\), where \( V_0 = (0, 0, \ldots, 0) \), \( V_1 = (0, 0, \ldots, 1) \), \( V_{2^n-1} = (1, 1, \ldots, 1) \), ordered in lexicographical order. There are algorithms for getting one form of representation of Boolean functions from its other form of representation. The trace function \( \text{Tr} : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) is defined as

\[
\text{Tr}(x) = x + x^2 + x^2 + \ldots + x^{2^{n-1}}.
\]

This representation plays a vital role in studying these functions. Every Boolean function \( f \) can be written in the form \( f(x) = \text{Tr}(F(x)) \), where \( F \) is a mapping from \( \mathbb{F}_2^n \) into \( \mathbb{F}_2^n \). There is another important representation, Numerical Normal Form but is not discussed in this chapter. The sign function of a Boolean function \( f \) is defined as \((-1)^f\).

**Definition 2.2.2.** (Balancedness). An \( n \)-variable Boolean function \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) is said to be balanced if the TT of \( f \) contains equal number of 1s and 0s.

**Definition 2.2.3.** (Walsh Transform). The Walsh transform of an \( n \)-variable Boolean function \( f \) is an integer valued function \( W_f : \mathbb{F}_2^n \rightarrow [-2^n, 2^n] \) defined by

\[
W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)}(-1)^{a \cdot x} = 2^n - 2wt(f \oplus a \cdot x), \quad a \in \mathbb{F}_2^n, \quad a \cdot x = a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n.
\]

The term \( W_f(a) \) is called Walsh coefficient of \( f \) at the point \( a \). The set of all the Walsh coefficients is referred as the Walsh spectrum of \( f \). This satisfies the Parseval’s equation \( \sum_{a \in \mathbb{F}_2^n} (W_f(a))^2 = 2^{2n} \).
The derivative of a Boolean function \( f \) with respect to \( a \in \mathbb{F}_2^n \) is \( D_f(a) = f(x) \oplus f(x \oplus a) \).

The periodic autocorrelation function of \( f \) is a real-valued function defined on all \( a \in \mathbb{F}_2^n \).

\[
\Delta_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus a)}
\]  

(2.1)

2.3 Complexity Criteria for Boolean Functions

2.3.1 Nonlinearity

Boolean functions are used to build cryptosystems like block ciphers and stream ciphers. The existence of affine approximations of the Boolean functions used in cryptosystems allows to build attacks on this system. That is it consist of simplifying the enciphering algorithm by a linear approximation. The main criteria for evaluating the complexity of cryptographic Boolean functions on \( \mathbb{F}_2^n \) is the nonlinearity. There are two accepted measures of nonlinearity, namely algebraic and functional measure. The algebraic measure of nonlinearity of a function is simply the degree of its ANF and the functional measure is the minimal distance from the function to the set of all affine functions.

Nonlinearity is closely related to the principle of confusion introduced by Claude Elwood Shannon in 1949 [5]. Since then it is used as a measure of complexity of Boolean functions and for measuring linear attacks involved in stream ciphers and block ciphers. The Hamming weight \( w_H(f) \) of a Boolean function \( f \) is the the cardinality of the set \( \{ x \in \mathbb{F}_2^n : f(x) = 1 \} \). The Hamming distance \( d(f, g) \) between two functions \( f \) and \( g \) is the Hamming weight \( w_H(f \oplus g) \) of the function \( f \oplus g \). Let \( A_n \subset B_n \) be the set of all affine functions.

**Definition 2.3.1.** (Nonlinearity). The nonlinearity \( N_f \) of a Boolean function \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) is its minimum Hamming distance to the set of all affine functions with \( n \)-variables.

\[
N_f = \min_{h \in A_n} d(f, h)
\]
where $d$ is the Hamming distance.

The Hamming distance is a natural measure to evaluate the difference between Boolean functions. This notion given by Rothaus [14] has been considered as the main criterion for quantifying the resistance of ciphers using those functions to several kinds of attacks like linear and correlation attacks. The nonlinearity of a Boolean function can be measured using Walsh spectrum of $f$ as

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_f(a)|.$$ (2.2)

**Bent functions**

A Boolean function can achieve maximum nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1}$ only when $n$ is even and the functions which achieve this are called Bent functions. These functions are introduced by Rothaus in 1976. They can be characterized in terms of their autocorrelation function. A Boolean function $f$ is Bent if and only if all of its derivatives $f(x) \oplus f(x \oplus a), a \in \mathbb{F}_2^n$ are balanced which implies $\Delta_f(a) = 0$ for all nonzero $a \in \mathbb{F}_2^n$. Rothaus inequality [14] states that any bent function has algebraic degree at most $\frac{n}{2}$, for $n \geq 4$. Bent functions have a lot of useful applications in the fields like coding theory, spread spectrum communications, cryptography etc. They have maximum nonlinearity and satisfy the Strict Avalanche Criterion (SAC), however they are not balanced and hence can not be directly used in many cryptosystems where the balanced property is needed. Still we can use these functions to construct balanced Boolean functions with high nonlinearity [15].

**Definition 2.3.2.** (Bent function). A Boolean function $f \in \mathcal{B}_n$ is called a bent function if its Walsh transform is two valued, i.e., $W_f(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_2^n$, where $n$ is necessarily even.

Some of the constructions of bent functions are due to Rothaus, Maiorana, McFarland, Dillon, Dobbertin, Adams, Tavares and Carlet [15] [16] [17] [18] [19]. Monomial bent functions are Boolean functions of the form $f : \mathbb{F}_2^n \to \mathbb{F}_2$ defined as $f(x) = Tr(\alpha x^d)$. If there exits an $\alpha \in \mathbb{F}_2^n$ such that the $Tr(\alpha x^d)$ is bent then the exponent $d$ is called a bent exponent. Most of
the known cases of constructions of bent functions can be discovered from monomial functions. Also if \( f \) is bent and \( l \) is affine, then \( f \oplus l \) is bent. A class of bent functions is called a complete class of functions if it is globally invariant under the action of the general affine group and the addition of affine functions.

**Higher Order Nonlinearity**

Let \( N_r(f) \) denote the distance between \( f \) and the set of all functions of degrees at most \( r \) (which is the Reed-Muller code), we call \( N_r(f) \) the \( r \)-th order nonlinearity of \( f \), where \( r \) is a positive integer. We have \( N_r(f) = 0 \) if and only if \( f \) has degree atmost \( r \). The knowledge of all the nonlinearities of orders \( r \geq 1 \) of a Boolean function includes the knowledge of its algebraic degree.

The best known asymptotic upper bound for \( r \geq 2 \) \[20\]

\[
N_r(f) \leq 2^{n-1} - \frac{\sqrt{15}}{2}(1 + \sqrt{2})^{r-2} 2^\frac{r}{2} + O(n^{r-2}) \quad (2.3)
\]

The upper bound for higher order nonlinearity of a balanced function \( f \) is given in \[21\] as

\[
N_r(f) \leq 2^{n-1} - 2^{n-r} \quad (2.4)
\]

**Linear Structures**

Differential cryptanalysis is the process to discover statistical patterns in the output distribution by having \( x \) and \( x \oplus a \) as an input pair and trying to analyze the difference in their output \( f(x) \oplus f(x \oplus a) \). A Boolean function \( f \) has resistance to differential cryptanalysis if for most nonzero \( a \), \( |\Delta_f(a)| \) is either zero or very close to zero, which implies the Boolean function \( f(x) \oplus f(x \oplus a) \) will be balanced or close to be balanced. If the Boolean function \( D_f(a) = f(x) \oplus f(x \oplus a) \) is a constant function, then the vector \( a \) is called a linear structure of \( f \) \[22\]. In other words, \( a \in F_2^n \) is a linear structure of \( f \) if \( |\Delta_f(a)| = 2^n \). It is trivial to say that all zero vector is a linear structure. The set of all linear structures of a function \( f \) form a linear subspace of \( F_2^n \), the dimension of which is called the linearity of \( f \). A nonzero linear structure is cryptographically undesirable.
Affine Invariance

Two functions \( f \) and \( g \) on \( \mathbb{F}_2^n \) are called affine equivalent if there exists a linear isomorphism \( L \) from \( \mathbb{F}_2^n \) to \( \mathbb{F}_2^n \) and a vector \( a, \lambda \in \mathbb{F}_2^n, \epsilon \in \mathbb{F}_2 \) such that \( f(x) = g(L(x) + a) + \lambda \cdot x + \epsilon \) for every input \( x \in \mathbb{F}_2^n \), where \( \lambda \cdot x \) is the inner product. The algebraic degree and the number of monomials in ANF of a Boolean function are some complexity criteria which requires a study. The general complexity criteria which are mostly interesting in cryptographic framework are affine invariant, because the attacks on cryptosystems which uses Boolean functions as one of the building blocks often work with the same complexity when the functions are replaced by affinely equivalent ones. Nonlinearity and algebraic degree are affine invariant. The notion of bent function is invariant under affine equivalence, the existence/non-existence of nonzero linear structures is clearly affine invariant. But the number of monomials in the ANF is not affine invariant. It is desirable that a complexity criterion to remain invariant under a large group of transformations.

Non-Normality

Dobbertin in [15] introduced the concept of normal Boolean functions in relation to the construction of bent functions. A Boolean function \( f \) on \( \mathbb{F}_2^n \) is called \( k \)-normal (resp. weakly-\( k \)-normal) if there exists a \( k \)-dimensional flat on which \( f \) is constant (affine). Here \( k \)-normality implies weak-\( k \)-normality and weak-\( k \)-normality implies \( (k-1) \) normality. Non-normality is a natural complexity criterion to consider in cryptography. Moreover, there is a relation between non-normality and nonlinearity which shows that for a function to have high nonlinearity, it must be non-(weakly)-normal at a reasonable level. Given a flat \( U \) of dimension \( k \) in \( \mathbb{F}_2^n, n = 2k \), there are exactly \( b_k = 2^{2k-2^k+1} \) Boolean functions that are constant on \( U \). Let \( f \) be a weakly-\( k \)-normal Boolean function on \( \mathbb{F}_2^n \) [23]. Then

\[
N_f \leq 2^{n-1} - 2^{k-1}
\]

Non-normal Boolean functions exist on \( \mathbb{F}_2^n, n = 2k \). An upper bound for the number of normal Boolean functions exists and Canteaut et al. proved
the existence of non-normal bent functions for \( n \geq 10 \) and weakly non-normal for \( n \geq 14 \) on \( \mathbb{F}_2^n \) [24]. Consequences of normality on bent functions are that if a bent function \( f \in \mathbb{F}_2^n \) is constant on an \( \frac{n}{2} \) - dimensional affine subspace, then \( f \) is balanced on each proper coset of the subspace. Also most of the known constructions of bent functions lead to normal bent functions [25].

### 2.3.2 Correlation Immunity

The concept of correlation immune functions was introduced by Siegenthaler [13]. A Boolean function \( f \) is called \( k \)-th order correlation immune iff \( W_f(a) = 0 \) for all vectors \( a \in \mathbb{F}_2^n \) with Hamming weight less than or equal to \( k \). Correlation immune functions are used in the design of pseudorandom number generators in stream ciphers to resist a correlation attack [12]. A balanced \( m \)-th order correlation immune Boolean function \( f \) is called \( m \)-resilient. Siegenthaler’s bound [13] states that an \( n \)-variable, \( m \)-th order correlation immune Boolean function \( f \) has degree at most \( n - m \). Moreover, if \( f \) is balanced and \( m < n - 1 \), then the degree \( d \) of \( f \) satisfies

\[
d \leq n - m - 1
\]

According to Siegenthaler, the functions achieving the equality in equation 2.6 are called optimized functions and P. Sarkar in his paper [26] constructed optimized functions.

### 2.3.3 Avalanche Criterion

A Boolean function \( f \) satisfies the avalanche criterion with respect to \( a \) if \( f(x) \oplus f(x \oplus a) \) is a balanced function for all vectors \( a \in \mathbb{F}_2^n \). Furthermore, \( f \) is said to satisfy the avalanche criterion of order \( l \) (propagation criterion of order \( l \) [27]) if it satisfies the avalanche criterion with respect to every nonzero vector whose Hamming weight is not greater than \( l \). It is to be noted that the strict avalanche criterion (SAC) is the same as the avalanche criterion of order one. In other words a small change in the input to the function leads to a large change in the output and so the word avalanche effect. A large change of uniform kind in the output corresponding to small
changes in the input implies SAC.

**Definition 2.3.3.** (SAC). A Boolean function \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) satisfies SAC if and only if the function \( f(x) \oplus f(x \oplus a) \) is balanced for every \( a \in \mathbb{F}_2^n \) with Hamming weight 1.

**Definition 2.3.4.** (SAC of order \( k \) or SAC\((k)\)). A Boolean function \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) satisfies the SAC of order \( k \) if fixing any \( k \) of the \( n \) bits in the input \( x \) results in a Boolean function in the remaining \( n - k \) variables which satisfies SAC. \[28\]

The SAC was first defined by Webster and Tavares [4]. The Avalanche Criterion and its generalizations are based on the properties of the derivatives of Boolean functions. They are related to the property of diffusion, which a cryptosystem must satisfy.

**Global Avalanche Characteristics**

A Boolean function satisfying avalanche criterion of order \( k \) does not have linear structures with Hamming weight less than or equal to \( k \) and which does not prevent the possibility of having linear structures with Hamming weight greater than \( k \). This suggests that avalanche of order \( k \) for a Boolean function is not a sufficient indicator to identify the possibility of differential cryptanalysis. This encouraged Zang and Zeng to propose GAC indicators [29]. The GAC indicators consists of the sum of squares indicator and absolute indicator defined respectively as \( \sigma_f = \sum_{a \in \mathbb{F}_2^n} (\Delta_f(a))^2 \) and \( \Delta_{\text{max}} = \max_{a \in \mathbb{F}_2^n, a \neq 0} |\Delta_f(a)| \). The smaller \( \sigma_f \) and \( \Delta_{\text{max}} \) the better \( f \) will be resisting differential cryptanalysis, that is in order to achieve good diffusion, cryptographic functions should have low sum-of-squares indicator and absolute indicator. The avalanche property for functions can be reflected by these two GAC indicators \( \sigma_f \) and \( \Delta_{\text{max}} \). Both the indicators are affine invariant.

**2.3.4 Algebraic Immunity**

Let \( f \) be an \( n \)-variable Boolean function. Its algebraic immunity \( AI(f) \) equals the minimum algebraic degree of all the nonzero annihilators of \( f \) and \( f \oplus 1 \). Since \( f \) is an annihilator of \( f \oplus 1 \) and \( f \oplus 1 \) is an annihilator of
the algebraic immunity is upper bounded by the algebraic degree of \( f \). But we have got a tight bound on algebraic immunity [30] given as

\[
AI(f) \leq \left\lceil \frac{n}{2} \right\rceil
\]

(2.7)

and for all \( a < 1 \), the lower bound for \( AI(f) \) is approximately [31]

\[
\frac{n}{2} - \sqrt{\frac{n}{2} \log_e \left( \frac{n}{a \log_e 2} \right)}
\]

(2.8)

Let \( A \) be the set containing all annihilators with degree at most \( k \) of a Boolean function \( f \). For a Boolean function \( f \) of degree \( r \), the dimension of \( A \) is at most

\[
\sum_{i=0}^{k} \binom{a}{i} - \sum_{i=0}^{k} \binom{n-r}{i}
\]

(2.9)

Algebraic immunity of a Boolean function is affine invariant.

### 2.4 Bounds and Relations on Complexity Measures

A variety of criteria for choosing Boolean functions with cryptographic applications have been identified. There is a general principle that a Boolean function cannot simultaneously have too many cryptographically desirable properties. The tradeoffs among these criteria have received a lot of attention in the literature for a long time. The more the criteria to be taken into account, the more difficult problem is to obtain a Boolean function satisfying these properties.

#### 2.4.1 Bounds on Nonlinearity

The universal bound (or covering radius) for nonlinearity of Boolean functions over \( \mathbb{F}_2^n \) is given by \( nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1} \). The equality holds if and only if \( f \) is a bent function. When \( n \) is odd this bound is not tight. For odd \( n \), one can find Boolean functions with nonlinearity satisfying

\[
2^{n-1} - 2^{\frac{n+1}{2}} \leq nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}
\]
The nonlinearity value $2^n - 2^{n-1}$ is achieved by any $n$ variable Boolean function resulting from the concatenation of two $n - 1$ variable bent functions, so this value is called bent concatenation bound. This bound is also called quadratic bound as it is achieved by quadratic functions [23]. For odd $n \leq 7$ it is known that the maximum nonlinearity is equal to the bent concatenation bound. Using combinatorial techniques and search methods Patterson and Wiedemann [32] demonstrated a construction in the idempotent class of 15-variable Boolean functions with nonlinearity 16276 which exceeds the bent concatenation bound by 20. The idempotents can be regarded as rotation symmetric Boolean functions with proper choice of basis. Until the year 2006, the maximum nonlinearity known for the case of $n = 9, 11$ and 13 was equal to bent concatenation bound. In 2006 Selçuk Kavut et al. [33] discovered 9-variable functions with nonlinearity exceeding the bent concatenation bound in the class of rotation symmetric Boolean functions.

Balanced functions with high nonlinearity are of great interest in cryptography. But balanced functions never achieve the universal bound of nonlinearity. The upper bound for nonlinearity of balanced functions ($n \geq 3$) given in [34] is as follows.

$$nl(f) \leq \begin{cases} 2^{n-1} - 2^{\frac{n}{2}-1} - 2, & \text{if } n \text{ is even} \\ \lfloor \lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \rfloor \rfloor, & \text{if } n \text{ is odd} \end{cases}$$

where $\lfloor x \rfloor$ denotes the largest even integer less than or equal to $x$. The maximum nonlinearities achieved by balanced Boolean functions for $n \leq 6$ equals the quadratic bound given above. But for balanced Boolean functions over $\mathbb{F}_2^n$ with $n = 7$ and $n = 8$, the maximum nonlinearity achieved is 56 and 116 respectively instead of 58 and 118 which are the upper bounds (quadratic bound). So finding balanced Boolean functions with maximum nonlinearity (ie. achieving the upper bound given above) using some deterministic process for $n \geq 8$ still remains an open problem.
2.4.2 Tradeoff Between Nonlinearity and Algebraic Immunity

Relationship between the \( r \)-th order nonlinearity and algebraic immunity strengthens the reasons for considering algebraic immunity as a further cryptographic complexity criterion. Dalai et al. in [35] gave a lower bound on the (first order) nonlinearity of Boolean functions with its algebraic immunity \( AI(f) \) as

\[
nl(f) \geq \sum_{i=0}^{AI(f)-2} \binom{n}{i}
\]

Lobanov [36] improved the lower bound as

\[
nl(f) \geq 2 \sum_{i=0}^{AI(f)-2} \binom{n-1}{i}
\]

For a Boolean function \( f \) in \( n \) variables and \( r \) a positive integer. The \( r \)-th order nonlinearity of \( f \) satisfies:

\[
N_r(f) \geq 2 \sum_{i=0}^{AI(f)-r} \binom{n-r}{i}
\]

2.4.3 Tradeoff Between Nonlinearity and Avalanche Criterion

A function \( f \) on \( \mathbb{F}_2^n \) is bent iff \( f \) satisfies the avalanche criterion of order \( n \). For an \( f \) satisfying avalanche criterion of order \( k \), the nonlinearity \( nl(f) \) of \( f \) satisfies

\[
nl(f) \leq 2^{n-1} - 2^{n-1-\frac{k}{2}}
\]

The equality holds if \( f \) is a bent function for \( n = k \) even.

General bounds for the sum of squares indicator and absolute indicator of a Boolean function \( f \) is given respectively as follows.

\[
2^{2n} \leq \sigma_f \leq 2^{3n}
\]

\[
0 \leq \Delta_{\text{max}} \leq 2^n
\]
Based on the autocorrelation of a function, the two upper bounds on the nonlinearity of a Boolean function $f$ are given by

$$nl(f) \leq 2^{n-1} - \frac{1}{2} (\sigma_f)^{\frac{1}{2}}$$

$$nl(f) \leq 2^{n-1} - \frac{1}{2} \sqrt{2^n + \Delta_{max}}$$

If a Boolean function $f$ satisfies avalanche criterion with respect to all vectors except for a subset $\mathcal{R}$ of vectors in $\mathbb{F}_2^n$, then

$$nl(f) \geq 2^{n-1} - 2^{n-1} \sqrt{|\mathcal{R}|}$$

A shortcoming of the above equation is that $\mathcal{R}$ is large and this problem is addressed through the following bound [37].

$$nl(f) \geq 2^{n-1} - 2^{n-1} \rho^{-1}$$

where $\rho$ is the dimension of the maximal linear subspace of the space $E = \{0\} \cup \mathcal{R}^c$, where $\mathcal{R}^c$ is the complement of $\mathcal{R}$ in $\mathbb{F}_2^n$. A more improved lower bound on nonlinearity is given in [37] as

$$nl(f) \geq 2^{n-1} - 2^{\frac{1}{2} (n-r)-1} \sqrt{2^n + (|\mathcal{R} \cap W| - 1) \Delta_{max}}$$

where $W$ is any $r$-dimensional linear subspace of $\mathbb{F}_2^n$, $r = 0, 1, ..., n$.

2.4.4 Tradeoff Between Nonlinearity and Correlation Immunity

The first paper which explicitly shows the tradeoff between correlation immunity and nonlinearity is by Chee et al. [38]. They proved that the nonlinearity of an $n$ variable Boolean function which is correlation immune of order $k$ cannot exceed $2^{n-1} - 2^{n-1} \mu(n, k)^{\frac{1}{2}}$ where $\mu(n, k) = 2^n - \sum_{i=1}^{k} \binom{n}{i}$.

Let $f$ be an $n$ variable $m$-th order correlation immune Boolean function. Sarkar and Maitra [39] noted that the nonlinearity of such functions are bounded by
for $n$ even: $nl(f) \leq \begin{cases} 2^{n-1} - 2^m, & \text{if } m > \frac{n}{2} - 1 \\ 2^{n-1} - 2^{\frac{n}{2}-1} - 2^m, & \text{if } m \leq \frac{n}{2} - 1 \end{cases}$

for $n$ odd: $nl(f) \leq \begin{cases} 2^{n-1} - 2^m, & \text{if } N_f > 2^{n-1} - 2^m \\ \max_{h \geq 0} \{h2^m\} \leq nl(f), & \text{if } N_f \leq 2^{n-1} - 2^m \end{cases}$

if the function $f$ is balanced then

for $n$ even: $nl(f) \leq \begin{cases} 2^{n-1} - 2^{m+1}, & \text{if } m + 1 > \frac{n}{2} - 1 \\ 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+1}, & \text{if } m + 1 \leq \frac{n}{2} - 1 \end{cases}$

for $n$ odd: $nl(f) \leq \begin{cases} 2^{n-1} - 2^{m+1}, & \text{if } nl(f) > 2^{n-1} - 2^{m+1} \\ \max_{h \geq 0} \{h2^{m+1}\} \leq nl(f), & \text{if } nl(f) \leq 2^{n-1} - 2^{m+1} \end{cases}$

Boolean functions whose Walsh spectrum takes only three values are called plateaued functions. Zheng and Zhang [40] proved that the $m$-th order correlation immune functions on $n$-variable has the nonlinearity $2^{n-1} - 2^{m+1}$ if and only if it is plateaued.

Claude Carlet [23] noted that the nonlinearity of $m$-th order correlation immune Boolean functions on $n$-variables is bounded by

$$2^{n-1} - 2^m \left[ 4f \frac{2^{n-m-1}}{\sqrt{2^n - \sum_{i=1}^{m} \binom{n}{i}}} \right].$$

If $f$ is balanced then the nonlinearity cannot exceed

$$2^{n-1} - 2^{m+1} \left[ \frac{2^{n-m-2}}{\sqrt{2^n - \sum_{i=1}^{m} \binom{n}{i}}} \right].$$

Claude Carlet also suggested [41] an upper bound for $m$-resilient Boolean functions $f$ with algebraic degree $d$ as follows

$$nl(f) \leq 2^{n-1} - 2^{m+1 + \left[ \frac{n-m-2}{d} \right]}, \text{ for } n < 2(m + 2 + \left[ \frac{n-m-2}{d} \right])$$
If \( n \geq 2(m + 2 + \lfloor \frac{n-m-2}{2} \rfloor) \) then

\[
\text{nl}(f) \leq \begin{cases} 
2^n - 2^{m+1} + \lfloor \frac{n-m-2}{2} \rfloor, & \text{if } n \text{ is even} \\
2^n - 2^{m+1} + \lfloor \frac{n-m-2}{2} \rfloor \lceil 2^{n-m-2} - \lfloor \frac{n-m-2}{2} \rfloor \rceil & \text{if } n \text{ is odd}
\end{cases}
\]

Suppose \( m \)-resilient Boolean function \( f \) attains the nonlinearity bound \( \text{nl}(f) = 2^{n-1} - 2^{m+1} \) for \( m > \frac{n}{2} - 2 \), then \( f \) attains the Siegenthaler's degree bound \( d = n - m - 1 \) [41].