Chapter 3

Cryptographic Boolean Functions

3.1 Introduction

Boolean functions are functions from the vector space of all binary vectors of length n to the finite field $\mathbb{F}_2$. They play an important role in coding theory and cryptology. In both applications, Boolean functions with a small number of variables n are used in practice due to efficiency. Though n is currently small, studying and determining the Boolean functions with specific and desired properties is a hard problem which cannot be solved by an exhaustive search due to the size of the space of n-variable Boolean functions which is 2^{2^n}.

3.2 Representation of Boolean Functions

A Boolean function f in n variable is a mapping $f(x) : \mathbb{F}_2^n \to \mathbb{F}_2$ such that $x = (x_1, x_2, ..., x_n)$ where $\mathbb{F}_2^n$ is the vector space of dimension-n over the binary field $\mathbb{F}_2$. Let $\mathscr{B}_n$ represent the set of all 2^{2^n} Boolean functions of n variables. Boolean functions can be represented in different forms, each with their own usefulness in regard to cryptographic analysis.

3.2.1 Truth Table and Polarity Truth Table

The Truth Table (TT) representation is the default representation of a Boolean function as it directly translates the definition of a Boolean function. The TT of a Boolean function f on $\mathbb{F}_2^n$ is a binary vector of length 2^n, each element of this binary vector is an image corresponding to a unique element in $\mathbb{F}_2^n$ ordered lexicographically.

Another representation that is closely related to TT is the Polarity Truth Table (PTT) or sequence of the function f, and is widely used in telecommunications. It is defined as $\hat{f}(x) = (-1)^{f(x)} = 1 - 2f(x)$ so that function values belong to the set $\{-1, 1\}$.

Example 3.1. *Table 3.1 shows the TT and PTT of a 3-variable Boolean function f.*

Table 3.1: Truth Table

x_0	x_1	x_2	$f(x)$	$\hat{f}(x)$
0	0	0	0	1
0	0	1	0	1
0	1	0	1	-1
0	1	1	0	1
1	0	0	0	1
1	0	1	1	-1
1	1	0	1	-1
1	1	1	1	-1

The truth table representation of Boolean function is the basis for the definition of several important properties, including Hamming weight and Hamming distance.

Definition 3.1. (Hamming weight)
Hamming weight of a Boolean function f, denoted by $wt(f)$ is defined as the number of 1's in the binary truth table (or the number of -1's in PTT) of the Boolean function.

$$wt(f) = \sum_x f(x) = \frac{1}{2}\left(2^n - \sum_x (\hat{f})(x)\right)$$

Definition 3.2. (Hamming distance)
Hamming distance between two functions $f \in \mathscr{B}_n$ and $g \in \mathscr{B}_n$ is defined as the number of truth table positions at which the functions differ. It can be expressed as the Hamming weight of the XOR sum of two functions.

$$distance(f, g) = wt(f \oplus g)$$

3.2.2 Algebraic Normal Form

Another way of uniquely representing a Boolean function f on $\mathbb{F}_2^n$ is by means of a polynomial in the ring $\mathbb{F}_2[x_0, x_1, ..., x_{n-1}]/ < x_0^2 - x_0, x_1^2 - x_1, ..., x_{n-1}^2 - x_{n-1} >$ and is defined as the algebraic normal form (ANF). The corresponding transformation is called the algebraic normal transform:

$$f(x_0, x_1, ..., x_{n-1}) = \sum_{j=(j_0,j_1,...,j_{n-1}) \in GF(2)^n} a_j x_0^{j_0} x_1^{j_1} ... x_{n-1}^{j_{n-1}} (\text{mod } 2), \text{ where } a_j \in GF(2).$$

From a truth table of an n-variable Boolean function f, the ANF can be computed as

$$f(x_0, x_1, ..., x_{n-1}) = \sum_{j=(j_0,j_1,...,j_{n-1})/f(j)=1} (x_0 \oplus j_0 \oplus 1)(x_1 \oplus j_1 \oplus 1)...(x_{n-1} \oplus j_{n-1} \oplus 1).$$

The algebraic degree of f, denoted by $\deg(f)$, is the number of variables in the longest term(s) of the ANF of f. If $deg(f) \leq 1$, then f is called an affine function. An affine function without the constant term (ie: $a_0 = 0$) is often called a linear function. An affine function with $deg(f) = 0$, which is either $f(x) = 0$ or $f(x) = 1$,

is called a constant function. There are 2^{n+1} affine functions in n- variable and let the set of these functions be denoted by $\mathscr{A}_n$. Note that any nonconstant affine function is balanced and for any affine function f, either $f(x \oplus y) = f(x) \oplus f(y)$ holds for all $x, y \in \mathbb{F}_2^n$ or it never holds for all $x, y \in \mathbb{F}_2^n$. As the structure of affine functions(i.e. their truth tables) leads to statistical weakness these type of functions are considered as weak by cryptographers.

Example 3.2. *ANF of Boolean function presented in Table 3.1 is* $x_1 + x_0x_2 + x_1x_2$ *and the degree of the Boolean function is 2.*

As the algebraic normal transform is a linear transformation, we can also use a matrix representation. Denote the column matrix containing the coefficients of the terms in the ANF of f for $0 \leq a \leq 2^n - 1$ ordered lexicographically by $[A_f]$, then
$[A_f] = A_n[f] \pmod 2$, where A_n is recursively determined by

$$A_0 = 1, A_n = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes A_{n-1} = \begin{bmatrix} A_{n-1} & 0 \\ A_{n-1} & A_{n-1} \end{bmatrix}$$

Note that this transform is an involution as $A_n^2 = I_{2^n} \pmod 2$ where I_{2^n} is the $2^n \times 2^n$ identity matrix, and hence $[f] = A_n[A_f] \pmod 2$.

3.2.3 Trace Representation

The trace representation plays an important role in sequence theory, and is also used for defining and studying Boolean functions. In the theory of finite fields, the trace function on the finite field $\mathbb{F}_{p^n}$ is the function $Tr : \mathbb{F}_{p^n} \to \mathbb{F}_p$ defined by

$$Tr(x) = x + x^p + x^{p^2} + x^{p^3} + ... + x^{p^{n-1}}.$$

Here we are considering the case when $p = 2$, that is, when our finite field is the binary field $\mathbb{F}_{2^n}$. From the isomorphic relation between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$, a Boolean

function f on $\mathbb{F}_2^n$ can be represented by $Tr(p(x))$ where $x \in \mathbb{F}_{2^n}$ and $p(x)$ a polynomial on one variable of degree atmost $2^n - 1$.

Example 3.3. *Trace representation of Boolean function presented in Table 3.1 is* $Tr(x^{3t+2})$ *with the primitive polynomial* $x^3 + x + 1$.

3.3 Tools for Analyzing Boolean Functions

3.3.1 Walsh-Hadamard Transform

The Walsh-Hadamard transform (WHT) is an orthogonal transform like the discrete Fourier transform. S. Golomb was the first to consider the Walsh-Hadamard transform of Boolean functions [25]. It is regarded as one of the leading transforms in Boolean function theory. Walsh transform (or Hadamard transform) of a Boolean function f yields the knowledge of correlations between f and linear functions.

Definition 3.3. The Walsh transform of an n-variable Boolean function f is an integer valued function $W_f : \mathbb{F}_2^n \to [-2^n, 2^n]$ defined by

$$W_f(\bar{a}) = \sum_{\bar{x} \in GF(2)^n} (-1)^{f(\bar{x}) \oplus \bar{a}.\bar{x}} = 2^n - 2wt(f \oplus \bar{a}.\bar{x})$$

The term $W_f(\bar{a})$ is called the Walsh coefficient of f at the point $\bar{a}$. The set of all the Walsh coefficients is referred as the Walsh spectrum of f.

Sometimes, the discrete Fourier transformation F_f is used instead of the Walsh transform: $F_f(\bar{a}) = \sum_{\bar{x} \in F_2^n} f(\bar{x})(-1)^{\bar{x} \cdot \bar{a}}$ which is related with the Walsh transform as follows[26]:

$$W_f(\bar{a}) = -2F_f(\bar{a}) + 2^n \delta(\bar{a})$$

where $\delta(\bar{a})$ denotes the Kronecker delta function ($\delta(\bar{0}) = 1, \delta(\bar{a}) = 0 \; \forall \bar{a} \neq \bar{0}$). The function $(-1)^f$ (resp. f) can be recovered by the inverse Walsh (resp. Fourier)

transform:

$$\hat{f}(\bar{a}) = \frac{1}{2^n}\sum_{\bar{a}} W_f(\bar{a})(-1)^{\bar{x}\cdot\bar{a}} \quad (\ resp.\ f(\bar{x}) = \frac{1}{2^n}\sum_{\bar{a}} F_f(\bar{a})(-1)^{\bar{x}\cdot\bar{a}}\ ).$$

A $(1,-1)$ matrix H of order n is called Hadamard matrix if $HH^T = nI_n$. Sylvester-Hadamard matrix (or Walsh-Hadamard matrix) is a special kind of Hadamard matrix of order 2^n denoted by H_n. It is generated by the recursive relation

$$H_0 = 1,\ H_n = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes H_{n-1} = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$$

Note that the columns of H_n are the column vectors $(-1)^{\bar{a}_i\cdot\bar{x}}$ where $0 \leq i \leq 2^n - 1$ and $\bar{a}_i$ corresponds to the binary representation of the integer i.

We see that $W_f(\bar{a})$ is actually a multiplication of the row vector $(-1)^{f(\bar{x})}$ and the column vector $(-1)^{\bar{a}\cdot\bar{x}}$. So multiplying the row vector $(-1)^{f(\bar{x})}$ by a matrix, H_n, gives us the whole Walsh spectrum of the Boolean function f.

Example 3.4. *Table 3.2 shows the Walsh transform of the Boolean function given in Table3.1*

Table 3.2: Walsh Hadamard Transform of f

a_0	a_1	a_2	$W_f(\bar{a})$
0	0	0	0
0	0	1	0
0	1	0	4
0	1	1	4
1	0	0	4
1	0	1	-4
1	1	0	0
1	1	1	0

We can compute Walsh transform of any Boolean function f from its truth table with $\mathcal{O}(2^{2n})$ operations. The same number of operations is required to compute inverse Walsh transform. However, using the butterfly algorithm [27] we can reduce the number of operations to $\mathcal{O}(n2^n)$ by factoring H_n.

3.3.2 Autocorrelation Spectrum

Given a Boolean function f, the derivative of f with respect to a vector $\bar{u}$, denoted by $D_{\bar{a}}(f)$, is defined by $D_{\bar{u}}(f) = f(\bar{x}) \oplus f(\bar{x} \oplus \bar{u})$. The autocorrelation function of the Boolean function f on F_2^n is a real-valued function defined for all $\bar{a} \in F_2^n$ as $\Delta_f(\bar{a}) = \sum_{\bar{x} \in F_2^n} (-1)^{f(\bar{x}) \oplus f(\bar{x} \oplus \bar{a})}$. In matrix notation, it is easily checked that this transformation can be written as $\Delta_f(\bar{a}) = [(-1)^f]^T D_a^n [(-1)^f]$ with the following recursive definition of $D_{\bar{a}}$

$$D_0^0 = 1;\ D_{\bar{a}}^n = \begin{bmatrix} D_{\bar{a}}^{n-1} & 0_{2^{n-1}} \\ 0_{2^{n-1}} & D_{\bar{a}}^{n-1} \end{bmatrix} \text{ if } \bar{a} < 2^{n-1}$$

$$D_{\bar{a}}^n = \begin{bmatrix} 0_{2^{n-1}} & D_{\bar{a}-2^{n-1}}^{n-1} \\ D_{\bar{a}-2^{n-1}}^{n-1} & 0_{2^{n-1}} \end{bmatrix} \text{ if } \bar{a} \geq 2^{n-1}$$

The following theorem shows the relation between autocorrelation function and Walsh transform

Theorem 3.4. *Wiener-Khintchine:*
If f is a Boolean function on n-variable then $\Delta_f(\bar{a}) = \sum_{\bar{u} \in \mathbb{F}_2^n} W_f(\bar{u})^2 (-1)^{\bar{a}.\bar{u}}$ for all $\bar{a} \in \mathbb{F}_2^n$.

Example 3.5. *Table 3.3 shows the autocorrelation of the Boolean function given in Table 3.1 as*

Table 3.3: Autocorrelation Spectrum of f

a_0	a_1	a_2	$\Delta_f(a)$
0	0	0	8
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	-8
1	1	1	0

3.4 Cryptographic Properties of Boolean functions

3.4.1 Balancedness

A function is said to be balanced when half of the function values are equal to one ie; $wt(f) = 2^{n-1}$. Balancedness of a Boolean function is a significant cryptographic property as the output of the function should not leak any statistical information about structure. The number of balanced Boolean functions in n-variable is $\binom{2^n}{2^{n-1}}$.

3.4.2 Nonlinearity

The main criteria for evaluating the cryptographic complexity of Boolean functions is the nonlinearity. For cryptographic systems the method of confusion and diffusion as introduced by Shannon is used as a fundamental technique to achieve security. Confusion is reflected in nonlinearity of the Boolean functions describing the cryptographic transformation. Since then nonlinearity is used as a measure of complexity of Boolean functions and for measuring linear attacks involved in

stream ciphers and block ciphers. In this context it is important to have criteria which are measures for nonlinearity.

Nonlinearity criteria for Boolean functions are classified in view of their suitability for cryptographic design. The classification is set up in terms of the largest transformation group leaving a criterion invariant. This concept is fundamental in algebra. In cryptography it is motivated by the following point of view: A function is considered weak if it can be turned into a cryptographically weak function by means of simple (e.g. linear or affine) transformations. Consider the Boolean function $f(x_1, x_2, \ldots, x_n)$ whose algebraic normal form is obtained by summing up all possible product terms in $x_1, x_2, ..., x_n$. At the first glance this seems to be a good nonlinear function, since it contains all nonlinear terms. However f can be written as the product $f(x_1, x_2, \ldots, x_n) = (1 + x_1)(1 + x_2)\ldots.(1 + x_n)$ which transforms into the monomial function $g(x_1, x_2, \ldots, x_n) = x_1x_2...x_n$ by simply complementing all arguments. This turns f into a poor function with respect to the number of nonlinear terms. Thus a large number of nonlinear terms taken as a criterion is not suitable since it is not invariant under simple transformations.

It is common to describe the Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ in terms of their algebraic normal form. A function f is nonlinear (or non-affine) if its algebraic normal form contains terms of degree higher than one.

Definition 3.5. (Nonlinear order) The nonlinear order for a Boolean function f is the degree of the highest order terms in the algebraic normal form.

Definition 3.6. (Distance to affine functions) The nonlinearity $nl(f)$ of a Boolean function f is its minimum Hamming distance to affine functions.

Complex functions are supposed to be very different from the simplest (i.e. affine) Boolean functions, and the Hamming distance is a natural measure to evaluate this difference. Several years after the introduction of this notion by Rothaus [10], it has been confirmed as the main criterion quantifying the resistance of ciphers using the function to several kinds of attacks like linear and correlation attacks.

The nonlinearity is affine invariant and can be expressed by means of the Walsh transform of f as

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

Definition 3.7. (Distance to linear structures) A linear structure of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a vector $\bar{a}$ in $\mathbb{F}_2^n$ such that the expression $f(\bar{x} \oplus \bar{a}) \oplus f(\bar{x})$ takes the same value (0 or 1) for all $\bar{x} \in \mathbb{F}_2^n$.

In other words, $\bar{a} \in F_2^n$ is a linear structure of f if $|\Delta_f(\bar{a})| = 2^n$. 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 $\mathbb{F}_2^n$, the dimension of which is called the linearity of f. A nonzero linear structure is cryptographically undesirable. Also the existence/non-existence of nonzero linear structures is clearly affine invariant.

With regard to these nonlinear criteria an optimum class of functions is considered. These functions simultaneously have maximum distance to affine functions and maximum distance to linear structures, as well as minimum correlation to affine functions. The functions with these properties coincide with certain functions known in combinatorial theory, where they are called bent functions. They have practical applications for block ciphers as well as stream ciphers. In particular they give rise to a new solution of the correlation problem.

An n- variable 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 were introduced by Rothaus in 1976. A Boolean function f is bent if and only if all of its derivatives $f(\bar{x}) \oplus f(\bar{x} \oplus \bar{a})$, $\bar{a} \in \mathbb{F}_2^n$ are balanced which implies $\Delta_f(\bar{a}) = 0$ for all nonzero $\bar{a} \in \mathbb{F}_2^n$. Rothaus [10] has noted that the algebraic degree of any bent function on n-variable ($n \geq 4$) can not exceed $\frac{n}{2}$. Bent functions have a lot of useful applications in the fields like coding theory, spread spectrum communications, cryptography etc. They have maximum nonlinearity however, they are not balanced and hence can not be directly used in many cryptosystems where the balanced property is needed. We can use these functions to construct balanced Boolean functions with high nonlinearity [28]. Some of the constructions of bent functions are due to Rothaus, Maiorana, McFarland, Dillon, Dobbertin,

Adams, Tavares and Carlet [28, 29, 30, 31, 32]. 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 α 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.

There are no perfect nonlinear functions with an odd number of arguments. This relies on the fact that the absolute value of the Walsh transform of a perfect nonlinear function has to be constant. However for odd dimensions we can construct functions with the property that the absolute value of their Walsh transform is two-valued. Perfect nonlinearity may not be compatible with other cryptographic design criteria. For example perfect nonlinearity cannot be achieved in conjunction with balancedness or highest nonlinear order. However a reasonable strategy will be to find nearly perfect nonlinear functions which satisfy additional design criteria.

Definition 3.8. (Higher Order Nonlinearity) The r^{th} order nonlinearity $N_r(f)$ of a Boolean function f is defined as the distance between f and the set of all functions of degrees at most r.

Note that $N_r(f) = 0$ 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 has been given in [33] as

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

The upper bound for higher order nonlinearity of a balanced function f is given in [34] as

$$N_r(f) \leq 2^{n-1} - 2^{n-r}$$

3.4.3 Correlation Immunity and Resilience

Cryptographic Boolean functions whose output leaks no information about its input variables are of great importance, such functions are called correlation immune functions. Correlation immune Boolean functions were introduced by Siegenthaler [35] for their ability to resist certain kinds of divide and conquer attacks on a model of stream ciphers.

Definition 3.9. (Correlation immunity) A Boolean function $f(x_1, x_2, \ldots, x_n)$ is correlation immune of order m, $1 \leq m \leq n$, denoted by CI(m), if for any choice of m distinct variables $x_{i_1}, x_{i_2}, ..., x_{i_m}$ the output f is statistically independent of the variables $x_{i_1}, x_{i_2}, ..., x_{i_m}$, i.e., $I(x_{i_1}, x_{i_2}, ..., x_{i_m}; f) = 0$ where $I(x_{i_1}, x_{i_2}, ..., x_{i_m}; f)$ denotes the mutual information between $x_{i_1}, x_{i_2}, ..., x_{i_m}$ and f.

In other words a Boolean function f in n- variables is correlation immune of order m if the output of the function is statistically independent of the combination of any m of its inputs. Later Xiao and Massey [36] gave a characterization of correlation immunity based on the Walsh transform of a Boolean function as follows.

A Boolean function f is called m^{th} order correlation immune iff $W_f(a) = 0$ for all vectors $a \in \mathbb{F}_2^n$ with $0 < Wt(w) \leq m$.

A balanced m^{th} order correlation immune Boolean function f is called m-resilient. In 1984 Siegenthaler [35] noted 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 $d \leq n - m - 1$. Functions achieving the Siegenthaler's bound are called optimized functions.

3.4.4 Avalanche Characteristics

The design of conventional cryptographic systems relies on two fundamental principles introduced by Shannon : confusion and diffusion. Confusion aims at concealing any algebraic structure in the system. Diffusion consists in spreading out

the influence of a minor modification of the input data over all outputs. Confusion and diffusion can be quantified by some properties of the Boolean functions describing the system. Confusion corresponds to the nonlinearity of the involved functions, while diffusion is related to the propagation characteristics of the considered Boolean function f. These properties describe the behaviors of the derivatives $D_u(f)$ of the Boolean function. The relevant cryptographic quantities are the biases of the output probability distributions of the derivatives relatively to the uniform distribution; they are measured by the auto-correlation coefficients of the function.

Definition 3.10. (Strict Avalanche Criteria) A Boolean function in n variables is said to satisfy Strict Avalanche Criteria (SAC) if complementing any one of the n input bits results in changing the output bit with probability exactly one half.

This is exactly having $f(x)\oplus f(x\oplus a)$ being balanced for all a in $\mathbb{F}_2^n$ with $wt(a) = 1$. In terms of autocorrelation this is having $|\Delta_f(a)| = 0 \quad \forall a \in \mathbb{F}_2^n$ with $wt(a) = 1$. The SAC was introduced by Webster and Tavares[37]. Later Forré [26] extended this concept by defining the higher order SAC

Definition 3.11. (SAC(k)) A Boolean function of n variables satisfies the SAC of order k (SAC(k)), for $0 \leq k \leq n-2$, if whenever k input bits are fixed arbitrarily, the resulting function of $n-k$ variables satisfies SAC.

Lloyd [38] notices that if $f(x)$ is a Boolean function in $n > 2$ variables which satisfies the SAC of order k, $1 \leq k \leq n-2$ then $f(x)$ also satisfies the SAC of order j for any $j = 0, 1, ...k-1$. The properties of SAC functions have been well studied (see[39, 40, 41]). But the problem with SAC functions is that they can have a large number of vectors with Hamming weight greater than one as their linear structures. Therefore the SAC was generalized to Propagation Characteristic (PC) by Preneel [42]

Definition 3.12. (PC(l)) A Boolean function f of n variables satisfies the propagation characteristic of degree l, PC(l), complementing l or less bits results in the output of f being complemented with a probability of a half.

This is exactly having $f(x) \oplus f(x \oplus a)$ being balanced for all a in $\mathbb{F}_2^n$ with $wt(a) \leq l$. In terms of autocorrelation this is having $|\Delta_f(a)| = 0 \ \ \forall a \in \mathbb{F}_2^n$ with $1 \leq wt(a) \leq l$. A stronger property than PC(l) is PC(l) of order k, which is satisfied when at most k coordinates of the input x are fixed and f still satisfy PC(l).

A Boolean function satisfying PC(l) doesn't have linear structures with Hamming weight less than l. However, the PC(l) criterion does not prevent the possibility of having linear structures of Hamming weight more than l. This suggests that even the PC is not a sufficient indicator to identify the possibility of differential attacks. This encouraged Zhang and Zheng [43] to propose the Global Avalanche Characteristics (GAC) indicator. GAC indicators consists of a sum of squares indicators and absolute indicators defined respectively as $\sigma_f = \sum_{a \in \mathbb{F}_2^n} (\Delta_f(a))^2$ and $\Delta_{max} = \max_{a \in \mathbb{F}_2^n, a \neq 0} |\Delta_f(a)|$. The smaller σ_f and Δ_f the better f will be resisting differential cryptanalysis, that is in order to achieve good diffusion, cryptographic functions should have low sum-of-squares indicators and absolute indicators. Since Boolean functions does not guarantee satisfying the avalanche criterion and so the avalanche property for functions can be reflected by these two GAC indicators σ_f and Δ_f. Both the indicators are affine invariant.

3.4.5 Algebraic Immunity

Due to the great success of algebraic attacks [44] the notation of algebraic immunity of Boolean functions was introduced in [45]. It is used to measure the ability of functions to resist this kind of attacks.

Definition 3.13. (Algebraic Immunity) The algebraic immunity (AI) of a Boolean function is the smallest possible degree of non-zero Boolean functions that can annihilate it or its complement.

Since f is an annihilator of $f \oplus 1$ and $f \oplus 1$ is an annihilator of f, the algebraic immunity is upper bounded by the algebraic degree of f. But the tight upper bound on algebraic immunity [44] is $AI(f) \leq \lceil \frac{n}{2} \rceil$.

3.5 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 trade-offs 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 the problem is to obtain a Boolean function satisfying these properties.

3.5.1 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 $2^{n-1} - 2^{\frac{n-1}{2}}$ 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 [46]. 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 [11] 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. [12] 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 given in [47] 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 $\lfloor \lfloor x \rfloor \rfloor$ 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.

3.5.2 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 [48] 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 [49] improved the lower bound as

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

Let f be a Boolean function in n variables and let r be a positive integer. The r^{th} order nonlinearity of f satisfies:

$$N_r(f) \geq 2 \sum_{i=0}^{AI(f)-r-1} \binom{n-r}{i}$$

3.5.3 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.

$$2^{2n} \leq \sigma_f \leq 2^{3n}$$

$$0 \leq \Delta_{max} \leq 2^n$$

Based on the autocorrelation of a function, the two upper bounds on the nonlinearity of a Boolean function f are given by

$$nl(f) \leq 2^{n-1} - \frac{1}{2}(\sigma_f)^{\frac{1}{4}}$$

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

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

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

A shortcoming of the above equation is that $\Re$ is large and this problem is addressed through the following bound [50].

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

where ρ is the dimension of the maximal linear subspace of the space $E = \{0\} \cup \Re^c$, where $\Re^c$ is the complement of $\Re$ in $\mathbb{F}_2^n$. A more improved lower bound on nonlinearity is given in [50] as

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

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

3.5.4 Tradeoff Between Nonlinearity and Correlation Immunity

The first paper which explicitly shows the tradeoff between correlation immunity and nonlinearity is by Chee et al.[51]. 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 [52] noted that the nonlinearity of such functions are bounded by

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

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

if the function f is balanced then

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

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

Boolean functions whose Walsh spectrum takes only three values are called plateaued functions. Zheng and Zhang [53] 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 [46] noted that the nonlinearity of m^{th} order correlation immune Boolean functions on n- variables is bounded by $2^{n-1} - 2^m\lceil 4f\frac{2^{n-m-1}}{\sqrt{2^n - \sum_{i=1}^{m}\binom{n}{i}}}\rceil$.

If f is balanced then the nonlinearity cannot exceed $2^{n-1} - 2^{m+1}\lceil\frac{2^{n-m-2}}{\sqrt{2^n - \sum_{i=1}^{m}\binom{n}{i}}}\rceil$

Claude Carlet also suggested [54] an upper bound for m-resilient Boolean functions f with algebraic degree d as follows

$$nl(f) \leq 2^{n-1} - 2^{m+1+\lfloor\frac{n-m-2}{d}\rfloor}, \; for\; n < 2(m+2+\lfloor\frac{n-m-2}{d}\rfloor)$$

If $n \geq 2(m+2+\lfloor\frac{n-m-2}{d}\rfloor)$ then

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

Suppose m-resilient Boolean function f attains the nonlinearity bound $nl(f) = 2^{n-1} - 2^{m+1}$ for $m > \frac{n}{2} - 2$, then the f also attains the Siegenthaler's degree bound $d = n - m - 1$ [54].