Journal of Computer Science 8 (6): 809-814, 2012
ISSN 1549-3636

Generalization of Boolean Functions Properties to Functions Defined over GF(p)

[1]Saad Elmansori and [2]B.E. Esam
[1]Department of Engineering and Computer Science, Concordia University, Montreal, Canada
[2]Department of Computer Science-Technical College, Janzor, Libya

Abstract: Problem statement: Traditionally, cryptographic applications designed on hardware have always tried to take advantage of the simplicity of implementation functions over GF(p), p = 2, to reduce costs and improve performance. On the contrast, functions defined over GF(p); p > 2, possess far better cryptographic properties than GF(2) functions. **Approach:** We generalize some of the previous results on cryptographic Boolean functions to functions defined over GF(p); p > 2. **Results:** We generalize Siegenthaler's construction to functions defined over finite field. We characterize the linear structures of functions over GF(p) in terms of their Walsh transform values. We then investigate the relation between the autocorrelation coefficients of functions over GF(p) and their Walsh spectrum. We also derive an upper bound for the dimension of the linear space of the functions defined over GF(p). Finally, we present a method to construct a bent function from semi-bent functions. **Conclusion:** Functions defined over GF(p) can achieve better cryptographic bounds than GF(2) functions. In this paper we gave a generalization of several of the GF(2) cryptographic properties to functions defined over GF(p), where p is an odd prime.

Key words: Finite field, coding theory, cryptography, walsh transform, bent function

INTRODUCTION

The existence of a tradeoff between the cryptographic properties in GF(2) functions has an immense consequences on the security of the cryptosystem using these functions. For instance, the algebraic degree and the correlation immunity order in Boolean functions are two important security measures. It is well known that a cryptographic function that has a high resistance to correlation attacks may have a low linear complexity to counter the linear synthesis by the Berlekamp-Massey algorithm (Massey, 1969).

In the special case where p = 2, the Siegenthaler inequality (Siegenthaler, 1984) states that if a function f(x) with n variables is a correlation-immune of order m then its algebraic degree d≤ n-m. Moreover, if f(x) is an m-resilient, m≤ n - 2, then d≤ n-m-1. It is clear from the Siegenthaler inequality that we cannot construct a function over GF(2) with the maximum order of correlation immunity (n-1) and algebraic degree higher than 1. On the other hand, when the function is defined over GF(p), it is possible to construct an (n-1)-correlation immune function with algebraic degree greater than 1. For example, $\text{let } f(x): F_5^2 \longrightarrow F_5$ such that $f(x_1, x_2) = x_1 + x_2^3$. Then, f(x) is a resilient function of degree 1 and its algebraic degree equals 3 (Liu *et al*., 1998).

This example illustrate the fact that functions over GF(p) can possess high correlation immunity and high algebraic degree. Thus motivated by the better bounds these functions can achieve, various cryptographic properties have already been extended from GF(2) to other finite fields. For example, (Liu *et al*., 1998) presented a series of constructions of correlation-immune function over finite fields. Later, (Hu and Xiao, 2003) investigated the existence, construction, and enumeration of resilient functions. Li and Cusick (2005) extended the concept of the Strict Avalanche Criterion (SAC) to GF(p) functions. Due to its importance in cryptography and coding theory, bent function and its properties were generalized in (Kumar *et al*., 1985).

The concept of hyper-bent function was extended to functions over GF(p) in (Youssef, 2007). A new characterization of semi-bent and bent quadratic functions on finite fields was given in (Khoo *et al*., 2006). The author in (Li, 2008) generalized the counting results of rotation symmetric Boolean functions to the rotation symmetric polynomials over finite fields GF(p). Cusick *et al*. (2008) gave a lower bound on the number of n-variable balanced symmetric polynomials over finite fields GF(p). Recently, functions defined over GF(p) have been used to propose a new a group re-keying protocol based on modular

Corresponding Author: Saad Elmansori, Department of Engineering and Computer Science, Concordia University, Montreal, Canada

polynomial arithmetic (Sudha *et al*., 2009). In this paper, we generalize some of the previous results on cryptographic binary functions to functions defined over GF(p), where p is an odd prime.

Preliminaries: We present some definitions and algebraic preliminaries required to prove our result.

If $F_p^n \longrightarrow F_p$ then f can be uniquely expressed in the following form:

$$f(x_1, x_2, ..., x_n) = \sum_{i_1=0}^{p-1}\sum_{i_2-0}^{p-1}....\sum_{in=0}^{p-1} a_{i1i2.....in} x_1^{i1} x_2^{i2} .....x_n^{in}$$

where, $a_{i1i2...in} \in F_p$. This representation of f is called the *algebraic normal form* of *f*. The largest $i_1 + i_2 + \ldots i_n$ with $a_{i1i2}\ldots i_n \neq 0$ is called the *algebraic degree* of f. The function f is called *balanced* if its output is uniformly distributed.

Definition 1: Let p be a prime and $u = e^{i(2\pi/p)}$ be the q-th root unity in C, where $i = \sqrt{-1}$. The Walsh transform of a function f : $F_p^n \longrightarrow F_p$ is defined as follows Eq. 1:

$$F(w) = \sum_{X \in F_p^n} u^{f(x)-<W.X>} \quad (1)$$

The autocorrelation function is defined as Eq. 2:

$$AC(\alpha) = \sum_{X \in F_p^n} u^{f(X+a)-f(X)} \quad (2)$$

where, $W, a \in F_p^n$ and <w.x> denotes the dot product between w and x, i.e., <w.x>=Pn I $\sum_{j=1}^{n} w_i x_i$ mod p. We will denote by |X| the magnitude of the complex number *X*. Most of the properties of the cryptographic functions can be measured using theWalsh transform or the autocorrelation function.

Definition 2: A function $f : F_p^n \longrightarrow F_p$ is bent if and only if $|F(W) = p^{n/2}|$for all $w \in F_p^n$ (Kumar *et al*., 1985).

Definition 3: A function $f : F_p^n \longrightarrow F_p$ is semi-bent if and only if the absolute values of its Walsh transform are $|p^{(n+1)/2}|$ and 0 that occur with frequency p^{n-1} and $p^{n-}p^{n-1}$, respectively.

Definition 4: The derivative of a function f(x) with respect to a vector $e \in F_p^n$ is defined as $d_e f(X) = f(x+e)-f(x)$. The vector e is called a linear structure of f(x) if $d_e f(x) = c$ (constant) for any $X \in F_p^n$. The set of all linear structures of f(x) form a subspace called linear subspace V_n.

Generalization of siegenthaler's construction: A simple and useful method to construct Boolean functions is through direct constructions. Direct constructions can produce functions that are optimal with respect to the designed property. Lots of research efforts have been put into these construction techniques in GF(2). Thus, it is significant to extend these constructions from GF(2) to GF(p). Siegenthaler, (1984) proposed a method to construct a Boolean function *f* of order n by combining two functions f_1, f_2 of order n-1, such that $f : F_2^n \times F_2^n \longrightarrow F_2 : (\bar{X}, x_n) \mapsto (x_n \otimes 1) f_1(\bar{X}) \otimes x_n f_2(\bar{x})$, wher e $\bar{X} = (x_1, ..., x_n - 1)$.

In the following, we generalize the Siegenthaler's construction method to functions over GF(p). We also derive some cryptographic properties of the constructed functions.

Let $f_1, f_2 |, ..., f_p : F_p^{n-1} \longrightarrow F_p$. Consider a function $f : F_p^n \longrightarrow F_p$ where $f = [f_1 \| f_2 \| ...f_p]$. In other words, f denotes the function whose truth table is the concatenation of the truth tables of $f_1, f_2, \ldots f_p$ in the given order.

Algebraic Normal Form (ANF): Let $\bar{X} = (x_1, x_2, ..., x_{n-1})$ and x = (x_1, x_2,…, x_{n-1}, x_n), then:

$$\begin{aligned} f(x|x_n = 0) &= f_1(\bar{X}) \\ f(x|x_n = 1) &= f_2(\bar{X}) \\ &\vdots \\ f(x|x_n = p-1) &= f_p(\bar{X}) \end{aligned}$$

Then we can write the ANF of f(x) as follows:

$$f(X) = (p-1) f_1(\bar{X}) \prod_{j=1}^{p-1} (x_n - j) + (p-1) f_2(\bar{X})$$

$$\prod_{\substack{j=0 \\ j\neq 0}}^{p-1} (x_n - j) + ... + (p-1) f_p(\bar{X}) \prod_{j=0}^{p-2} (x_n - j)$$

$$= \sum_{i=1}^{p} (p-1) f_i(\bar{X}) \prod_{\substack{j=1 \\ j\neq (i-1)}}^{p-1} (x_n - j)$$

Walsh Transform: Let $\bar{w} = (w_1, w_2, ..., w_{n-1})$ and w = (w_1,w_2,…,wn-$_1$,w_n):

$$\begin{aligned} f_1(\bar{X}) &= f(x\,|\,x_n = 0) \\ f_2(\bar{X}) &= f(x\,|\,x_n = 1) \\ &\vdots \\ f_p(\bar{X}) &= f(x\,|\,x_n = p-1) \end{aligned}$$

The Walsh transform of the concatenated function is given by:

$$\begin{aligned} F(W) &= \sum_{x\in F_p^n} u^{f(x)-\langle w.x\rangle} \\ &= \sum_{x|xn=0} \left| u^{f1(x)-\langle w.x\rangle} + \sum_{x|x_n=1} u^{f2(x)-\langle w.x\rangle} \right. \\ &+ .....+ \sum_{x|x_n=p-1} u f_p{}^{(x)-<w.x>}. \end{aligned}$$

By noting that, $< w.x >=< \bar{w}.\bar{x} > + w_n x_n$, then:

$$\begin{aligned} F(w) &= \sum_x u^{f_1(x)-<w.x>} + u^{-wn} \sum_x u^{f_2(x)-<\bar{w}.\bar{x}>} \\ &+ .....+ u-(p-1)w_n \sum_{\bar{x}} u^{f_p(\bar{x})-<\bar{w}.\bar{x}>} \\ &= F_1(\bar{w}) + u^{-wn} F_2(\bar{w}) + ... + u^{-(p-1)w_n} F_p(\bar{w}) \\ &= \sum_{j=1}^{p} u^{(1-i)w_n} F_i(\bar{w}). \end{aligned}$$

Characterization of linear structures of functions over GF(p): Direct use of Boolean functions possessing linear structure should be avoided in cryptographic applications. It has been shown in (Evertse, 1988; Hellman *et al*., 1976; Chaum and Evertse, 1986; Josef *et al*., 2002) that block ciphers with linear structure are vulnerable to attacks much faster than the exhaustive search. Several studies were conducted on the existence of the linear structures in several classes of Boolean functions, as in (Dubuc, 1998) for vectorial functions and for symmetric functions (Dawson and Wu, 1997). In the following, we study this criterion for functions defined over GF(p). In particular, we characterize linear structures of functions over GF(p) in terms of their Walsh transform values.

Theorem 1: (Generalization of Theorem 1 in (Dubuc, 1998)) f(x) has a linear structure $e \in F_p^n$ with a corresponding constant c if and only if F(w) = 0 for all w such that $< w.e > 6 \neq c$.

Proof: Since e is a linear structure of f(x), then f(x) = c, $c \in$ Fp. Let g(x) = f(x + e)-c, then G(w) = F(w):

$$\begin{aligned} G(W) &= \sum_{x\in F_p^n} u^{f(x+e)-c-c<x.w>} \\ &= \sum_{x\in F_p^n} u^{f(x)-c-<x-e>.w>} \\ &= \sum_{x\in F_p^n} u^{f(x)-<x.w>+<w.e>} \\ &= u^{<w.e>} F(w), \end{aligned}$$

Thus, e is a linear structure of f(x) if and only if f(x) = g(x). which implies that $< w . e > -c = 0$.

We use Theorem 1 to characterize the linear structures of semi-bent functions defined over GF(p).

Corollary 1: For a semi-bent function f(x), e is a linear structure with a corresponding constant c if and only if F(w) = 0 for all w such that $< w . e > 6 \neq c$ and $|F(w)| = p^{(n+1)/2}$ for all w such that $< w . e >= c$.

Proof: The absolute value of the Walsh transform of the semi-bent function have only two values 0 and p(n+1) = 2. Since the number of w that satisfy the equation <w. e>6 = c is pn-1(p-1), which it is exactly the same number of zeros in the Walsh transform F(w) = 0. Hence, there is a one-to-one mapping between the Walsh transform and the relation $< w . e > \neq c$, i.e., F(w) = 0 if and only if $<w . e > \neq c$ and also $|F(w)| = p^{(n+1)/2}$ if and only if $< w . e >= c$.

Relation between the autocorrelation function and the walsh transform: The autocorrelation is another useful criterion in analyzing Boolean functions. It measures the probability distribution of the output difference of the function for a fixed input difference. The autocorrelation coefficient AC(α) measures the statistical bias of the output distribution of $d\alpha f(x)$ relative to the uniform distribution. In the next, we show how the autocorrelation coefficients of functions over GF(p) are related to their Walsh spectrum.

Lemma 2: Let f(x) be a function defined over GF(p). Then:

$$AC(\alpha) = \frac{1}{p^n} \sum_{w\in F_p^n} |F(w)|^2 u^{<w.\alpha>}$$

Proof: Using the inverse of the Walsh transform in equation 1, we get:

$$u^{f(x)} = \frac{1}{p^n} \sum_{w\in F_p^n} F(w) u^{<w.x>}$$

Thus:

$$u^{f(x+\alpha)} = \frac{1}{p^n}\sum_{w\in F_p^n} F(w)u^{<w.(x+\alpha)>}$$
$$= \frac{1}{p^n}\sum_{w\in F_p^n} F(w)u^{<w.x>}u^{<w.a>}$$

From the definition of the autocorrelation function in equation 2, we get:

$$AC(\alpha) = \frac{1}{p^n}\sum_{x\in F_p^n} u^{-f(x)}\sum_{w\in F_p^n} F(w)u^{<w.x>}u^{<w.\alpha>}$$
$$= \frac{1}{p^n}\sum_{w\in F_p^n} F(w)u^{<w.\alpha>}\sum_{x\in F_p^n} u^{-f(x)}u^{<w.x>}$$
$$= \frac{1}{p^n}\sum_{w\in F_p^n} F(w)u^{<w.\alpha>}\sum_{x\in F_p^n} u^{-f(x)}u^{<w.x>}$$
$$= \frac{1}{p^n}\sum_{w\in F_p^n} F(w)u^{<w.\alpha>}F*(w),$$

where *F*¤(w) is the complex conjugate of F(w). Then we have:

$$AC(\alpha) = \frac{1}{p^n}\sum_{w\in F_p^n} |F(w)|^2 u^{<w.\alpha>}$$

The following corollary follows directly from the definition of the inverse Walsh transform and Lemma 2.

Corollary 2: Let f(x) be a function defined over GF(p). Then Eq. 3:

$$|F(w)^2| = \sum_{a\in F_p^n} AC(\alpha)u^{-<w.\alpha>} \quad (3)$$

Lemma 3: Let *f*(x) be a function defined over GF(p). Then Eq. 4:

$$\sum_{w\in F_p^n} |F(w)|^4 = p^n\sum_{\alpha\in F_p^n} AC^2(\alpha) \quad (4)$$

Proof: Squaring both sides of the equation in Corollary 2 we get:

$$|F(w)|^4 = \sum_{a\in F_p^n} AC(\alpha)u^{-<\alpha.w>}\sum_{\beta\in F_p^n} AC(\beta)u^{-<\beta.w>}$$

By taking the summation for both sides for all w 2 Fn p we get:

$$\sum_{w\in F_p^n} |F(w)|^4$$
$$= \sum_{w\in F_p^n}\sum_{\alpha\in F_p^n}\sum_{\beta\in F_p^n} AC(\alpha)AC(\beta)u^{<(-\alpha-\beta).w>}$$
$$= \sum_{\alpha\in F_p^n}\sum_{\beta\in F_p^n} AC(\alpha)AC(\beta)\sum_{w\in F_p^n} u^{<(-\alpha-\beta).w>}$$

By noting that:

$$\sum_{w\in F_p^n} u^{<(-\alpha-\beta).w>} = \begin{cases} 0 & \alpha \neq -\beta \\ p^n & \alpha = -\beta \end{cases}$$

Then we have:

$$\sum_{w\in F_p^n} |F(w)|^4 = p^n\sum_{\alpha\in F_p^n} AC^2(\alpha)$$

We now derive the relation between the Walsh spectrum of the semi-bent functions and their autocorrelation coefficients.

Theorem 4: Let *f*(x) be a semi-bent function defined over *GF*(*p*). Then Eq. 5:

$$p^n F^2{}_{max}(w) = \sum_{\alpha\in F_p^n} AC^2(\alpha) \quad (5)$$

Proof: Since f(x) is a semi-bent function, the Walsh transform contains the values F_{max} (w) = $p^{(n+1)/2}$ and occurs p^{n-1} times while 0 occurs (p^n- p^{n-1}) times. We refer throughout the rest of this paper to the value $p^{(n+1)/2}$ as F_{max}(w). Thus:

$$\sum_{w\in F_p^n} |F(w)|^4 = p^{n-1}F^4{}_{max}(w) = p^{3n+1}$$

Substituting in Lemma 3, we get:

$$p^n\sum_{\alpha\in F_p^n} AC^2(\alpha) = p^{3n+1}$$
$$\sum_{\alpha\in F_p^n} AC^2(\alpha) = p^{2n+1}$$
$$= p^nF^2{}_{max}(w)$$

Walsh spectrum of GF(p) functions with linear structure We derive the upper bound of the dimension of the linear space of the functions defined over GF(p).

Theorem 5: (Generalization of theorem 3 in (Canteaut *et al*., 2000)) Let f(x) be a function defined over GF(p) with n variables. Then, the dimension k of the linear space V_n is such that k ≤ 1.

Proof:

$$\sum_{\alpha\in F_p^n} AC^2(\alpha) = \sum_{\alpha\in v} AC^2(\alpha) + \sum_{\alpha\notin v} AC^2(\alpha)$$

If f(x) has a linear space of dimension k, then:

$$\sum_{\alpha\in F_p^n} AC^2(\alpha) = p^k p^{2n} + \sum_{\alpha\notin v} AC^2(\alpha) \geq p^{2n+k}$$

Substituting in Theorem 4 we get:

$$p^n F^2{}_{max}(w) \geq p^{2n+k}$$

Thus:

$$F_{max}(w) \geq p^{\frac{2n+k}{2}}$$

For a semi-bent function $F_{max}(w) = p^{\frac{n+1}{2}}$, then:

$$p^{\frac{n+1}{2}} \geq p^{\frac{n+k}{2}},$$

which implies that $k \leq 1$.

Construction of bent functions from semi-bent functions with linear structure: Bent functions achieve the best possible nonlinearity. Accordingly, they provide good confusion properties, and they are perfect in resisting differential cryptanalysis (Biham and Shamir, 1991) and by definition linear cryptanalysis (Matsui, 1994). Their major flaw is that they are not balanced. Another useful class of functions which achieve high nonlinearity is semi-bent functions. These functions also possess good cryptographic characteristics, and some of them are balanced. Bent and semi-bent functions over GF(p), p > 2, can exist in even and odd dimensions. It is possible to construct bent functions with (n+1) variables from semi-bent function with n variables, and similarly, construct semi-bent functions with n variables from bent functions with (n + 1) variables. Here, we focus on constructing bent functions with n+1 variables from semi-bent functions with n variables.

The following lemmas are needed to simplify the proof of Theorem 9.

Lemma 6: Let g(x) = f(x)-<x.e>. If e is a linear structure for f(x) with a corresponding constant c, then g(x) has e as a linear structure with the corresponding constant c- < e . e >.

Proof: If f(x + e) - f(x) = c and g(x) = f(x)- < x . e > then:

$$\begin{aligned} &g(x+e)-g(x)\\ &= f(x+e)-<(x+e).e>-f(x)+<x.e>\\ &= f(x+e)-<x.e>-<e.e>-f(x)+<x.e>\\ &= f(x+e)-f(x)-<e.e>\\ &= c-<e.e> \end{aligned}$$

Lemma 7: If g(x) = f(x)- < x . e > then G(w) = F(w + e).

Proof:

$$\begin{aligned} G(w) &= \sum_{x\in F_p^n} u^{f(x)-<x.e>-<x.w>}\\ &= \sum_{x\in F_p^n} u^{f(x)-[<x.e>+<x.w>]}\\ &= \sum_{x\in F_p^n} u f(x)^{-<x.(w+e)>}\\ &= F(w+e) \end{aligned}$$

Lemma 8: If f(x) has linear structures a and b with corresponding constants c1 and c2, respectively. Then e = (e_1, e_2,…, e_n) = a b is a linear structure for f(x) with a corresponding constants c_1-c_2, where e_i = ai-bi mod p, 1≤i≤n.

Proof: Let $f(x+e_1)-f(x) = c_1$ and $f(x+e_2)-f(x) = c_2$. Then $f(x+e_1)-f(x+e_1) = c_1-c_2$ and $f(x + (e_1+ e_2))-f(x) = c_1-c_2$, which implies ($e_1$- e_2) is a linear structure with a corresponding constant c_1-c_2.

From the above lemma, it follows that if e is a linear structure for f(x), then a e, a 2 Fp is also a linear structure for f(x), where a e denotes the vector whose coordinates are obtained by multiplying the individual coordinates of e by a mod p.

Theorem 9: Let f(x) be a semi-bent function defined over GF(p) with non trivial linear structures e_1,e_2,…, e_{p-1}. Then:

$$[f(x)\ \|f(x)-<x.e_1>\|\ f(x)-<x.e_2>\|... \\ ...\|f(x)-<x.e_{p-1}>]$$

Is n + 1 bent function if <ei . ei>6= 0, for all i = 1,….,p-1.

Proof: Since f(x) has linear structures e_1, e_2,…., e_{p-1} with corresponding constants $c_{1....,}c_{p-1}$; respectively, then from Lemmas 6 and 7, the function f(x)- < x-e_i >, 1 ≤ I ≤$_{p-1}$; will have a linear structure ei with a corresponding constant ci-<e_i.e_i> and Walsh transform F(w + e_i).

From Corollary 1, we have:

$$\begin{aligned} F(w) = 0 \Leftrightarrow &<w.e_1> \neq c_1, <w.e_2> \neq c_2,\\ &...,<w.e_{p-1}> \neq c_{p-1}\\ F(w) = p^{(n+1)/2} \Leftrightarrow &<w.e_1> = c_1, <w.e_2> = c_2,\\ &...,<w.e_{p-1}> = c_{p-1} \end{aligned}$$

By noting that <(w+e_i).e_i> = <w.e_i>+<e_i.e_i> where 1 ≤ I ≤ p - 1, then:

$$
\begin{aligned}
F(w+e_1)=0 &\Leftrightarrow < w \,.\, e_1 > + < e_1 \,.\, e_1 > \\
&\neq c_1 - < e_1 \,.\, e_1 > \\
\left|F(w+e_1)\right| = p^{(n+1)/2} &\Leftrightarrow < w.e_1 > + < e_1 .e_1 > \\
&= c_1 - < e_1 .e_1 > \\
F(w+e_2)=0 &\Leftrightarrow < w.e_2 > + < e_2 .e_2 > \\
&\neq c_2 - < e_2 .e_2 > \\
\left|F(w+e_2)\right| = p^{(n+1)/2} &\Leftrightarrow < w.e_2 > + < e_2 .e_2 > \\
&= c_2 - < e_2 .e_2 > \\
&\vdots \\
F(w+e_{p-1})=0 &\Leftrightarrow < w.e_{p-1} > + < e_{p-1}.e_{p-1} > \\
&\neq c_{p-1} - < e_{p-1}.e_{p-1} > \\
\left|F(w+e_{p-1})\right| = p^{(n+1)/2} &< w.e_{p-1} > + \\
&< e_{p-1}.e_{p-1} >= c_{p-1} - < e_{p-1}.e_{p-1} >
\end{aligned}
$$

Thus, if < w. e1 >= c_1 then then |F(w) | = $p^{(n+1)/2}$,F (F(w+e_2)) = 0, F(w+e_{p-1}). Consequently, if one of the |F(w)|F(w+e_1),|F(w+e_2)|,…,F(w+e_{p-1}) equals $p^{(n+1)/2}$ the others equal zero, which implies that *F*(w) corresponds to the Walsh transform of an n + 1 bent function.

CONCLUSION

Functions defined over GF(p) can achieve better cryptographic bounds than GF(2) functions. Thus, In this paper we gave a generalization of several of the GF(2) cryptographic properties to functions defined over GF(p), where p is an odd prime.

REFERENCES

Biham, E. and A. Shamir, 1991. Differential cryptanalysis of des-like cryptosystems. Lecture Notes Comput. Sci., Crypto, 4: 3-72. DOI: 10.1007/BF00630563

Canteaut, A., C. Carlet, P. Charpin and C. Fontaine, 2000. Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions. Lecture Notes Comp. Sci., Eurocrypt, 1807: 507-522. DOI: 10.1007/3-540-45539-6_36

Chaum, D. and J.H. Evertse, 1986. Cryptanalysis of des with a reduced number of rounds sequences of linear factors in block ciphers. Lecture Notes Com. Sci., CRYPTO, 218: 192-211. DOI: 10.1007/3-540-39799-X_16

Cusick, T.W., Y. Li and P. Stanica, 2008. Balanced symmetric functions over GF(p). IEEE Trans. Inform. Theory, 54: 1304-1307. DOI: 10.1109/TIT.2007.915920

Dawson, E. and C.K. Wu, 1997. On the linear structure of symmetric boolean functions. Aust. J. Combinatorics, 16: 239-243.

Dubuc, S., 1998. Linear structures of Boolean functions. Proceeding of the IEEE International Symposium Information Theory, Aug 16-21, IEEE Xplore Press, Cambridge, pp: 440-440. DOI: 10.1109/ISIT.1998.709045

Evertse, J.H., 1988. Linear structures in block ciphers. Lecture Notes Comp. Sci., Eurocrypt, 304: 249-266.

Hellman, M., R. Merkle, R. Schroeppel, L.Washington and W. Diffie *et al*., 1976. Results of an initial attempt to cryptanalyze the NBS data encryption standard. Stanford University, Stanford Electronics Laboratories.

Hu, Y. and G. Xiao, 2003. Resilient functions over finite fields. IEEE Trans. Inform. Theory, 49: 2040-2046. DOI: 10.1109/TIT.2003.814489

Josef, P., S. Jennifer and H. Thomas, 2002. Fundamentals of Computer Security. 1st Edn., Springer, New York, ISBN-10: 3540431012, pp: 677.

Khoo, K., G. Gong and D. Stinson, 2006. A new characterization of semi-bent and bent functions on finite fields. Designs, Codes Cryptography, 38: 279-295. DOI: 10.1007/s10623-005-6345-x

Kumar, P.V., R.A. Scholtz and L.R. Welch, 1985. Generalized bent functions and their properties. J. Combinatorial Theory, Ser., 40: 90-107. DOI: 10.1016/0097-3165(85)90049-4

Li, Y. and T. Cusick, 2005. Strict avalanche criterion over finite fields. J. Math. Cryptology, 1: 65-78.

Li, Y., 2008. Results on rotation symmetric polynomials over GF(p). Inform. Sci., 178: 280-286. DOI: 10.1016/j.ins.2007.03.031

Liu, M., P. Lu and G.L. Mullen, 1998. Correlation-immune functions over finite fields. IEEE Trans. Inform. Theory, 44: 1273-1276. DOI: 10.1109/18.669323

Massey, J., 1969. Shift-register synthesis and bch decoding. IEEE Trans. Inform. Theory, 15: 122-127. DOI: 10.1109/TIT.1969.1054260

Matsui, M., 1994. Linear cryptanalysis method for des cipher. Lecture Notes Comp. Sci. Eurocrypt, 765: 386-397. DOI: 10.1007/3-540-48285-7_33

Siegenthaler, T., 1984. Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.). IEEE Trans. Inform. Theory, 30: 776-780. DOI: 10.1109/TIT.1984.1056949

Sudha, S., A. Samsudin and M.A. Alia, 2009. Group Re-keying protocol based on modular polynomial arithmetic over galois field GF(2n). Am. J. Applied Sci., 6: 1714-1717. DOI: 10.3844/ajassp.2009.1714.1717

Youssef, A.M., 2007. Generalized hyper-bent functions over GF(p). Discrete Applied Math., 155: 1066-1070. DOI: 10.1016/j.dam.2006.11.007