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

Saad Elmansori and B.E. Esam

1Department of Engineering and Computer Science, Concordia University, Montreal, Canada
2Department 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, let f(x): F_p^n → F_p such that f(x_1, x_2) = x_1 + x_2^2. 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...
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 $\mathbb{F}_p^n \rightarrow \mathbb{F}_p$ then $f$ can be uniquely expressed in the following form:

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1, i_2, \ldots, i_n=0}^{p-1} a_{i_1i_2\ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

where, $a_{i_1i_2\ldots i_n} \in \mathbb{F}_p$. This representation of $f$ is called the algebraic normal form of $f$. The largest $i_1 + i_2 + \ldots + i_n$ with $a_{i_1i_2\ldots i_n} \neq 0$ 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 $u = e^{i2\pi/n}$ be the $q$-th root unity in $\mathbb{C}$, where $i = \sqrt{-1}$. The Walsh transform of a function $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ is defined as follows Eq. 1:

$$F(w) = \sum_{x \in \mathbb{F}_p^n} u^{<w, x>}$$

The autocorrelation function is defined as Eq. 2:

$$AC(\alpha) = \sum_{x \in \mathbb{F}_p^n} u^{<x+\alpha, x>}$$

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

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

Definition 3: A function $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ is semi-bent if and only if the absolute values of its Walsh transform are $|p^{n/2} + 1|$ 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 $e \in \mathbb{F}_p^n$ 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 $X \in \mathbb{F}_p^n$. 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 $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ where $f = [f_1, f_2, \ldots, f_p]$. 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 $\overline{X} = (x_1, x_2, \ldots, x_{n-1})$ and $x = (x_1, x_2, \ldots, x_{n-1}, x_n)$, then:

$$f(x|x_n = 0) = f_1(\overline{X})$$

$$f(x|x_n = 1) = f_2(\overline{X})$$

$$\vdots$$

$$f(x|x_n = p-1) = f_p(\overline{X})$$

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

$$f(x) = (p-1)f_1(\overline{X}) \prod_{j=1}^{p-1} (x_n - j) + (p-1)f_2(\overline{X}) \prod_{j=0}^{p-2} (x_n - j)$$

$$\vdots$$

$$\sum_{i=1}^{p-1} (p-1)f_i(\overline{X}) \prod_{j=0}^{p-1-i} (x_n - j)$$

Walsh Transform: Let $\overline{w} = (w_1, w_2, \ldots, w_{n-1})$ and $w = (w_1, w_2, \ldots, w_{n-1}, w_n)$:
The Walsh transform of the concatenated function is given by:

\[
F(W) = \sum_{u \in F_p^n} u^{f(x)+w.x} - \sum_{u \in F_p^n} u^{g(x)+w.x} + \sum_{u \in F_p^n} u^{h(x)+w.x}.
\]

By noting that, \(<w.x> = <w.x> + w.x_n >

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

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 \(<w.x> \neq c\) and \(|F(w)| = p^{(n+1)/2}\) for all \(w\) such that \(<w.x> = e\).

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 \(<w.x> = c\) is \(p^{n-1}(p-1)\), which 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 \(<w.x> \neq c\), i.e., \(F(w) = 0\) if and only if \(<w.x> \neq c\) and also \(|F(w)| = p^{(n+1)/2}\) if and only if \(<w.x> = e\).

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 \(AC(\alpha)\) 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:

\[
AC(\alpha) = \frac{1}{p^r} \sum_{u \in F_p^n} |F(w)| u^{<\alpha,x>}.
\]

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

\[
u^{f(x)} = \frac{1}{p^r} \sum_{u \in F_p^n} F(w) u^{<\alpha,x>}.
\]

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

\[ AC(\alpha) = \frac{1}{p^n} \sum_{w \in \mathbb{F}_p} u^{-(f(x))w} \sum_{w \in \mathbb{F}_p} F(w) u^{cw.a} \]

\[ = \frac{1}{p^n} \sum_{w \in \mathbb{F}_p} F(w) u^{cw.a} \sum_{w \in \mathbb{F}_p} u^{-(f(x))w} \]

\[ = \frac{1}{p^n} \sum_{w \in \mathbb{F}_p} F(w) u^{cw.a} u^{-cw.a} \]

\[ = \frac{1}{p^n} \sum_{w \in \mathbb{F}_p} F(w) u^{cw.a} F(w)^* \]

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

\[ AC(\alpha) = \frac{1}{p^n} \sum_{w \in \mathbb{F}_p} |F(w)|^2 u^{cw.a} \]

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:

\[ |F(w)|^2 = \sum_{w \in \mathbb{F}_p} AC(\alpha) u^{cw.a} \] (3)

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

\[ \sum_{w \in \mathbb{F}_p} |F(w)|^2 = p^n \sum_{\alpha \in \mathbb{F}_p^*} AC^2(\alpha) \] (4)

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

\[ |F(w)|^2 = \sum_{\alpha \in \mathbb{F}_p^*} AC(\alpha) u^{-cw.a} \sum_{\beta \in \mathbb{F}_p^*} AC(\beta) u^{-cw.b} \]

By taking the summation for both sides for all \( w \in \mathbb{F}_p \) we get:

\[ \sum_{w \in \mathbb{F}_p} |F(w)|^2 \]

\[ = \sum_{w \in \mathbb{F}_p} \sum_{\alpha \in \mathbb{F}_p^*} AC(\alpha) AC(\beta) u^{-\alpha-w} \sum_{b \in \mathbb{F}_p^*} AC(\beta) u^{-\beta-w} \]

\[ = \sum_{\alpha \in \mathbb{F}_p^*} AC(\alpha) AC(\beta) \sum_{w \in \mathbb{F}_p} u^{-(\alpha+\beta)w} \]

By noting that:

\[ \sum_{w \in \mathbb{F}_p} u^{-(\alpha+\beta)w} = \begin{cases} 0 & \alpha \neq -\beta \\ p^n & \alpha = -\beta \end{cases} \]

Then we have:

\[ \sum_{w \in \mathbb{F}_p} |F(w)|^2 = p^n \sum_{\alpha \in \mathbb{F}_p^*} AC^2(\alpha) \]

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:

\[ p^n F_{\text{max}}^2 (w) = \sum_{\alpha \in \mathbb{F}_p^*} AC^2(\alpha) \] (5)

**Proof:** Since \( f(x) \) is a semi-bent function, the Walsh transform contains the values \( F_{\text{max}}^2 (w) = p^{(n+1)/2} \) 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 \( F_{\text{max}}^2 (w) \). Thus:

\[ \sum_{w \in \mathbb{F}_p} |F(w)|^2 = p^n F_{\text{max}}^2 (w) = p^{3n+1} \]

Substituting in Lemma 3, we get:

\[ p^n \sum_{\alpha \in \mathbb{F}_p^*} AC^2(\alpha) = p^{3n+1} \]

\[ \sum_{\alpha \in \mathbb{F}_p^*} AC^2(\alpha) = p^{3n+1} \]

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 \( k \leq 1 \).

**Proof:**

\[ \sum_{\alpha \in \mathbb{F}_p^*} AC^2(\alpha) = \sum_{\alpha \in \mathbb{F}_p^*} AC^2(\alpha) + \sum_{\alpha \in \mathbb{F}_p^*} AC^2(\alpha) \]

If \( f(x) \) has a linear space of dimension \( k \), then:
Lemma 7: If \( g(x) = f(x) < x . e > \) then \( G(w) = F(w + e) \).

**Proof:**

\[
G(w) = \sum_{x \in \mathbb{F}_p} u^{f(x) - <x . e > - <x . w >} \\
= \sum_{x \in \mathbb{F}_p} u^{f(x) - <x . e > + <x . w >} \\
= \sum_{x \in \mathbb{F}_p} u^{f(x) - <x + w >} \\
= F(w + e)
\]

Lemma 8: If \( f(x) \) has linear structures \( a \) and \( b \) with corresponding constants \( c_1 \) and \( c_2 \), respectively. Then \( e = (e_1, e_2, ..., e_n) = a \oplus b \) is a linear structure for \( f(x) \) with a corresponding constant \( c_1 - c_2 \), where \( e_i = a_i \oplus b_i \mod p \), \( 1 \leq i \leq n \).

**Proof:**

Let \( f(x+e_1)-f(x) = c_1 \) and \( f(x+e_2)-f(x) = c_2 \). Then \( f(x+e_1)-f(x+e_2) = c_1 - c_2 \) and \( f(x + (e_1 \oplus e_2)) - f(x) = c_1 - c_2 \), which implies \( e_1 \oplus e_2 \) 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 \( a, b, 2 \mathbb{F}_p \) is also a linear structure for \( f(x) \), where \( a \) 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 \( \mathbb{F}_p \) with non trivial linear structures \( e_1, e_2, ..., e_{p-1} \). Then:

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

Is \( n + 1 \) bent function if \( < e_i . e_i > \neq 0 \), for all \( i = 1, ..., p-1 \).

**Proof:**

Since \( f(x) \) has linear structures \( e_1, e_2, ..., e_{p-1} \) with corresponding constants \( c_1, c_2, ..., c_{p-1} \), respectively, then from Lemmas 6 and 7, the function \( f(x) < x . e_i > \) is linear structure \( e_i \), and Walsh transform \( F(w + e_i) \).

From Corollary 1, we have:

\[
F(w) = 0 \iff < w . e_i > = c_i < w . e_i > c_i, \\
..., < w . e_{p-1} > = c_{p-1}
\]

\[
F(w) = p^{(p-1)/2} \iff < w . e_i > = c_i < w . e_i > = c_i, \\
..., < w . e_{p-1} > = c_{p-1}
\]

By noting that \( < (w+e_i) . e_i > = < w . e_i > + < e_i . e_i > \) where \( 1 \leq i \leq p - 1 \), then:
Thus, if \( w \cdot e_1 = c_1 \) then \( |F(w)| = p^{(n+1)/2} \). Consequently, if one of the \( |F(w)|, |F(w+e_1)|, |F(w+e_2)|, \ldots, |F(w+e_{p-1})| \) 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 Comput. 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.