Construction of 1-Resilient Boolean Functions with Optimal Algebraic Immunity and Good Nonlinearity

Senshan Pan [*], Xiaotong Fu and Weiguo Zhang
ISN Lab, Xidian University, Xi'an 710071, P.R.China.

April 29, 2010

Abstract

This paper presents a construction for a class of 1-resilient Boolean functions with optimal algebraic immunity on an even number of variables by dividing them into two correlation classes, i.e. equivalence classes. From which, a nontrivial pair of functions has been found by applying the generating matrix. Apart from their good nonlinearity, the functions reach Siegenthaler's [16] upper bound of algebraic degree. Furthermore, a class of 1-resilient functions on any number $n > 2$ of variables with at least sub-optimal algebraic immunity is provided.

Keywords: Stream ciphers, Boolean functions, 1-Resilient, Algebraic immunity, Algebraic degree.

1 Introduction

Boolean functions are used as nonlinear combiners or nonlinear filters in certain models of stream cipher systems. Nowadays, a mounting number of attacks (Berlekamp-Massey attack, correlation attack, fast algebraic attack, i.e. FAA, etc.) has come out. This reality makes people have to revise old methods or design new ones to resist as many attacks as possible at the same time. Balance, a high nonlinearity, a high algebraic immunity, and in the case of the combiner model, a high correlation immunity (in the case of the filter model, a correlation immunity of order 1 is commonly considered as sufficient) are the cryptographic characteristic of good stream ciphers. The interaction of them is so complex that some properties are contrary to others to some extend. For instance, Maiorana-McFarland construction together with its variations is a popular and favorable approach for a number of well-behaved functions so far. Being constructed by affine subfunctions, M-M construction, however, has an evident drawback against FAA [4]. Finding the functions expected for by a trial and error method is unfeasible or at least harder and harder. It seems that in [4], a class of 1-resilient and optimal algebraic immunity functions was first obtained through a doubly indexed recursive relation. But its low nonlinearity impedes the utilization in cryptographic models. The construction employing symmetric functions present a risk if attacks using this peculiarity can be found in the future. Recently, [18] has provided 1-resilient functions with maximum degree and optimal algebraic immunity by a primary construction, when the number of variables n only equals

[*]Corresponding address: ISN Lab, Xidian University, Xi'an 710071, P.R.China. Email: pansenshan@gmail.com

to 6,8,10,12. Bars and Viola in [1] are trying to find a complete combinatorial characterization and thence to good random generation algorithms for well-behaved functions. Being a first step towards their extremely tough direction, the work of [1] is interesting and admiring.

In this paper we propose a construction method to design 1-resilient Boolean functions on even number variables ($n \geq 3$), where it retain the maximum degree and optimal algebraic immunity as [20]. The constructions provided here reveal a good adaptability: a function with higher nonlinearity can be obtained merely by finding the base function with improved nonlinearity without of the change of generating methods. Besides, we have improved the lower bound of nonlinearity by using the best example in [20].

The organization of this paper is as follows. In Section 2, the basic concepts and notions are presented. In Section 3, we present a secondary construction (i.e. Siegenthaler's construction) by concatenating two balanced Boolean functions f, g with odd variables n, where $deg(f) = n-1$, $AI(f) = (n+1)/2$, $g \in \hat{H}_f$ (cf. section 2). Our concrete realization is given in Section 4 by introducing the functions in [20]. In Section 5, a larger class of functions with sub-optimal algebraic immunity on any number (≥ 2) of variables. Finally, section 6 concludes the paper.

2 Preliminary

A Boolean function $f(x)$ is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $x = (x_1, \cdots, x) \in \mathbb{F}_2^n$ and $\mathbb{F}_2^n$ is the vector space of tuples of elements from $\mathbb{F}_2$. To avoid confusion with the additions of integers in $\mathbb{R}$, denoted by $+$ and Σ_i, we deliberately denote the additions over $\mathbb{F}_2$ by $\oplus$ and $\bigoplus_i$ for the purpose of arousing readers' attention. $f(x)$ is generally represented by its algebraic normal form (ANF):

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u (\prod_{i=1}^{n} x_i^{u_i}) \tag{1}$$

where $\lambda_u \in \mathbb{F}_2,\ u = (u_1, \cdots, u_n)$. The algebraic degree of $f(x)$, denoted by $deg(f)$, is the maximal value of $wt(u)$ such that $\lambda_u \neq 0$, where $wt(u)$ denotes the Hamming weight of u. We denote $LT(f) = ct$ as the leading term of f, $LM(f) = t$ the leading monomial and $LC(f) = c$ the leading coefficient, where $c \in \mathbb{F}_2$ and t is a monomial of $\mathbb{F}_2[x_1, \cdots, x_n]/(x_1^2 + x_1, \cdots, x_n^2 + x_n)$. Apparently, $LC(f) = 1$ and $LT(f) = LM(f) = t$ as $f \in \mathbb{F}_2^n$. f is called an affine function when $deg(f) = 1$. An affine function with constant term equal to zero is called a linear function. Any linear function on $\mathbb{F}_2^n$ is denoted by:

$$\omega \cdot x = \omega_1 x_1 \oplus \cdots \oplus \omega_n x_n,$$

where $\omega = (\omega_1, \cdots, \omega_n),\ x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$. The Walsh spectrum of $f \in \mathcal{B}_n$ in point ω is denoted by $W_f(\omega)$ and calculated by

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \omega \cdot x}. \tag{2}$$

$f \in \mathcal{B}_n$ is said to be balanced if its output column in the truth table contains equal number of 0's and 1's (i.e. $W_f(0) = 0$).

In [19], a spectral characterization of resilient functions has been presented.

Lemma 1: A n-variable Boolean function is m-resilient if and only if its Walsh transform satisfies

$$W_f(\omega) = 0, \text{ for } 0 \le wt(\omega) \le m, \omega \in \mathbb{F}_2^n. \tag{3}$$

The Hamming distance between two n-variable Boolean functions f and ρ is denoted by

$$d(f,\rho) = \{x \in \mathbb{F}_2^n : f(x) \ne \rho(x)\}.$$

The set of all affine functions on $\mathbb{F}_2^n$ is denoted by $A(n)$. The nonlinearity of a Boolean function $f \in \mathcal{B}_n$ is its distance to the set of all affine functions and is defined as

$$N_f = \min_{\rho \in A(n)} (d(f,\rho)).$$

In term of Walsh spectra, the nonlinearity of f is given by [10]

$$N_f = 2^{n-1} - \frac{1}{2} \cdot \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|. \tag{4}$$

Parseval's equation [9] states that

$$\sum_{\omega \in \mathbb{F}_2^n} (W_f(\omega))^2 = 2^{2n}. \tag{5}$$

So any Boolean function f with n variables satisfies

$$\max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| \ge 2^{n/2};$$

the functions for which equality holds are called bent functions. Obviously, the nonlinearity of bent functions is $2^{n-1} - 2^{n/2-1}$, where n is even.

Let $Supp(f) = \{b_i = (b_{i1}, \cdots, b_{in}) | f(b_i) = 1, 1 \le i \le wt(f)\}$. Then f can be represented as follows:

$$f(x_1, \cdots, x_n) = \sum_{i=1}^{wt(f)} \prod_{j=1}^{n} (x_j + 1 + b_{ij}).$$

Clearly, $deg(f) < n$ if and only if $wt(f)$ is even. Moveover, $deg(f) = n-1$ if and only if wt(f) is even and

$$\bigoplus_{i=1}^{wt(f)} (b_{i1}, \cdots, b_{in}) \ne 0. \tag{6}$$

Definition 1: Let n be the number of variables, a Boolean function with n variables f belongs to the correlation class M_f defined by

$$< wt(f), deg(f), AI(f); \delta_n, \delta_{n-1}, \cdots, \delta_1 >,$$

where $wt(f)$ is its Hamming weight, $deg(f)$ is the algebraic degree of f, $AI(f)$ algebraic immunity and $\delta_i = wt(f|_{x_i=0}) - wt(f|_{x_i=1})$, for any $1 \le i \le n$.

Definition 2: Let f,g are two Boolean functions with n variables. The equivalence relation $\mathcal{R}$ is defined by

$$f\mathcal{R}g \Longleftrightarrow M_f = M_g.$$

Generally,$< wt(f), deg(f); \delta_n, \cdots, \delta_1 >$ ($< wt(f); \delta_n, \cdots, \delta_1 >$) is the correlation class without of the consideration on algebraic immunity (algebraic immunity and degree).Notice that, for $1 \leq j \leq n$, we can get $\delta_j = \sum_{i=1}^{wt(f)}(-1)^{b_{ij}} = wt(f) - 2b_{*j}$, where $b_{*j} = \sum_{i=1}^{wt(f)} b_{ij}$. Thus a simple conclusion can be reached as follows:

Proposition 1: For two Boolean functions f and g, $deg(f) \geq n-1$. If $g \in M_f$, then $LT(g) = LT(f)$, i.e. the leading term are the same between f and g.

Definition 3: Let $p, q \in 0, \cdots, 2^n$, $\zeta^0 =< p; \delta_n^0, \cdots, \delta_1^0 >$,$\zeta^1 =< q; \delta_n^1, \cdots, \delta_1^1 >$. The operator class $*$ is defined by

$$\zeta^0 * \zeta^1 = \zeta,$$

where $\zeta =< p+q; \delta_{n+1} = p-q, \delta_n = \delta_n^0 + \delta_n^1, \cdots, \delta_1 = \delta_1^0 + \delta_1^1 >$. Let ζ^0 and ζ^1 denotes the set

$$\{h \in \{0,1\}^{2^{n+1}} | h = f||g = (1+x_{n+1})f + x_{n+1}g, f \in \zeta^0, g \in \zeta^1\}.$$

The following Lemma in [1] enable to decompose correlation classes recursively.

Lemma 2 (Decomposition):

$$\zeta = \bigcup_{\zeta^0 * \zeta^1 = \zeta} \zeta^0 \times \zeta^1.$$

Definition 4: Let $\zeta =< m, d, ai; \delta_n, \delta_{n-1}, \cdots, \delta_1 >$. The mirror class of ζ is the class

$$\hat{\zeta} =< m, d, ai; -\delta_n, -\delta_{n-1}, \cdots, -\delta_1 > . \tag{7}$$

An r^{th} order Reed-Muller code $R(r,n)$ is the set of all binary strings(vectors) of length 2^n associated with the Boolean polynomials $f(x_1, x_2, \cdots, x_n)$ of degree at most r. The collection of the Boolean functions with the leading term $LT(f)$ consists of the coset $f + R(deg(f)-1, n)$.

Notation 1:

$$\begin{aligned} H_f &= M_f \bigcap (f + R(deg(f)-1, n)), \\ \hat{H}_f &= \hat{M}_f \bigcap (f + R(deg(f)-1, n)), \end{aligned}$$

where n is the number of variables of f.

So, Proposition 1 can be written as $g \in H_f$, if $deg(f) \geq n-1$ and $g \in M_f$.

Definition 5: Let f be a Boolean function with n variables and Hamming weight $2m$. Then, f is first-order correlation-immune when $wt(f|_{x_i=0}) = wt(f|_{x_i=1}) = m$, for any $1 \leq i \leq n$.

It is easily seen that $\zeta = \hat{\zeta}$ if and only if $\forall f \in \zeta$ is a first-order correlation-immune. Besides, $f \in \zeta \Leftrightarrow \hat{f} \in \hat{\zeta}$, where $\hat{f} = f(x \bigoplus 1)$ denotes the reverse of the string f. As a consequence, we have $|\zeta| = |\hat{\zeta}|$.

Proposition 2: The algebraic degree, algebraic immunity and nonlinearity of a Boolean function f are invariant under an affine transformation towards its input (i.e. $g(x) = f(Ax \bigoplus b)$, where $A \in GL_n(\mathbb{F}_2)$ and $b \in \mathbb{F}_2^n$).

3 Degree Optimized 1-Resilient Functions with Optimal Algebraic Immunity

Proposition 3 [4]: Let f, g be two Boolean functions on the variables $x_1, x_2, \cdots, x_n$ with $AI(f) = d_1$ and $AI(g) = d_2$. Let $h = (1 + x_{n+1})f + x_{n+1}g \in \mathbb{F}_2^{n+1}$. Then

1) If $d_1 \neq d_2$, then $AI_{n+1}(h) = mind_1, d_2 + 1$.

2) If $d_1 = d_2 = d$, then $d \leq AI_{n+1}(h) \leq d + 1$, and $AI_{n+1}(h) = d$ if and only if there exists $f_1, g_1 \in \mathbb{F}_2^n$ of algebraic degree d such that $f * f_1 = 0, g * g_1 = 0$ or $(1 + f) * f_1 = 0, (1 + g) * g_1 = 0$ and $deg(f_1 + g_1) \leq d - 1$.

Construction 1: Let n be any odd integer such that $n \geq 3$ and f is a balanced Boolean function with maximum degree $n-1$ and optimal algebraic immunity $(n+1)/2$, i.e. $f \in < 2^{n-1}, n-1, (n+1)/2; \delta_n, \cdots, \delta_1 >$. Let

$$h = (1 + x_{n-1})f + x_{n+1}g \in \mathbb{F}_2^{n+1},$$

where $g \in \hat{H}_f$.

Notice $\hat{H}_f$ is not empty for any Boolean function f aforementioned because of $\bar{f} = f + 1 \in \hat{H}_f$. Besides, there is another trivial element $\hat{f}$in $\hat{H}_f$.

Theorem 1: $h \in \mathbb{F}_2^{n+1}$ in Construction 1 is 1-resilient Boolean function with maximum degree and optimal algebraic immunity, if $g \in \hat{M}_f$.

Proof: If $g \in \hat{M}_f$, due to Proposition 1, f and g have the same leading term of degree $n-1$ (i.e. $g \in \hat{H}_f$) and h is the concatenation of f and g, $deg(h) \leq n - 1$. Besides, h contains the monomial $LT(f)$, so we have $h \in < 2^n, n - 1, AI(h); 0, 0, \cdots, 0 >$, which is 1-resilient function of optimized degree. Using Proposition 3, $(n + 1)/2 \leq AI(h) \leq (n + 3)/2$ for $AI(f) = AI(g) = (n + 1)/2$. However, $AI(h)$ is upper bounded by $(n + 1)/2$, so h has maximum algebraic immunity $(n + 1)/2$. Thus $h \in < 2^n, n - 1, (n + 1)/2; 0, 0, \cdots, 0 >$.

Theorem 2: The nonlinearity of h in Construction 1 is $N_h \geq N_f + N_g$.

Proof: Let $x = (x', x_{n+1}), \omega = (\omega', \omega_{n+1}) \in \mathbb{F}_2^{n+1}$.

$$\begin{aligned} W_h(\omega) &= \sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{\omega \cdot x \oplus h(x)} \\ &= \sum_{x \in \mathbb{F}_2^{n+1}} (-1)^{\omega' \cdot x' \oplus \omega_{n+1} x_{n+1} \oplus (1 + x_{n+1}) f(x') \oplus x_{n+1} g(x')} \\ &= \sum_{x' \in \mathbb{F}_2^n} (-1)^{f(x') \oplus \omega' \cdot x'} + (-1)^{\omega_{n+1}} \sum_{x' \in \mathbb{F}_2^n} (-1)^{g(x') \oplus \omega' \cdot x'} \\ &= W_f(\omega') + (-1)^{\omega_{n+1} W_g(\omega')} \end{aligned} \tag{8}$$

By(4), we have

$$N_h \geq N_f + N_g.$$

In particular,for $g = \bar{f}$, $N_h = 2N_f$.

Next, we want to figure out whether there is an nontrivial function in $\hat{H}_f$ (i.e. $g \neq \bar{f}, \hat{f}$). This can convert to proofing whether there is a third element in H_f besides f and $\hat{f} + 1$. The answer seems yes, but it has not been proofed yet. However, another property is enough:

Proposition 4: A pair of Boolean functions with n variables (f^*, g^*) deduced from a given $f \in \mathbb{F}_2^n$ can always be found, where $deg(f^*) = n-1$, $AI(f^*) = (n+1)/2$, $N_{f^*} = N_f$ and $g^* \in \hat{H}_{f^*}$, $g^* \neq \hat{f}, \bar{f}$.

Proof: Let us consider the affine transformations: $f(x) \mapsto f(Ax \bigoplus b)$, where $A \in GL_n(\mathbb{F}_2)$ and $b \in \mathbb{F}_2^n$.

Recall $Supp(f) = \{b_i = (b_{i1}, \cdots, b_{in}) | f(b_i) = 1, 1 \leq i \leq wt(f) = 2^{n-1}\}$, where $b_i < b_j$ means

$$b_{ik} < b_{jk}, b_{ik+1} = b_{jk+1}, b_{ik+2} = b_{jk+2}, \cdots, b_{in} = b_{jn}, \exists 1 \leq k \leq n.$$

Let $(n, 2^{n-1})$ matrix $S_f = (b_1, b_2, \cdots, b_{2^{n-1}})$. $rank(S_f) \leq n$, and any two columns of S_f are distinct. Therefore, its rank is n, or else there must be a k, s.t. $b_{1k} = b_{2k} = \cdots = b_{2^{n-1}k}$, which indicates $f_0 = 0, f_1 = 1$ or $f_0 = 1, f_1 = 0$ for $f = (1 + x_k)f_0 + x_k f_1$, where $f_0, f_1 \in F_2[x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n]$. But the latter case is contrary to $deg(f) = n-1$, where $n \geq 3$. S_f can be regarded as a generating matrix and all of its codewords consist of the space of dimension n. Therefore, there are 2^n distinct codewords. The weight distribution of them denotes $\{w_0, w_1, \cdots, w_{2^{n-1}}\}$, so at least 2^{n-1} pairs of codewords has the same weight.

It can be seen that

$$< \delta_n(f), \cdots, \delta_1(f) > \neq < 0, \cdots, 0 >$$

because of Siegenthaler's upper bound.

1) If there is a t, s.t. $1 \leq t \leq n$, $\delta_t = 0$, then $f(x \bigoplus 1_t) \in H_f$ and $f(x \bigoplus 1_t) \neq f(x)$, where $1_t \in \mathbb{F}_2^n$ denotes all of its coordinates are 0 except t^{th}. Because there $\exists k$, $1 \leq k \leq n$ and $k \neq t$, $\sum_{i=1}^{wt(f)} b_{ik}$ is odd from (6),

$$Supp(f(x \bigoplus 1_t)) \neq Supp(f).$$

Clearly, $f(x \bigoplus 1_t) \neq \hat{f} + 1$. Thus $(f^*, g^*) = (f(x), f(x \bigoplus 1_t) + 1)$.

2) If all $\delta \neq 0$. If there exists $\delta_s = \delta_t$, where $1 \leq s < t \leq n$. s^{th} row differs from t^{th} row. A permutation matrix A can be used to swap x_s and x_t. Although $S_{f(Ax)} \neq S_f$, a special case, $Supp(f(Ax)) = Supp(f)$ may be happen. In case of that situation, we can perform an invertible transformation to alter the rows of S_f except s^{th} and t^{th} rows. Thus an nontrivial pair of (f^*, g^*) can be obtained. If no two δs are the same, a invertible matrix A of dimension n may be employed to renew the generating matrix to $S_{f(Ax)}$, which has two different codewords of the same weight. Similarly, we can obtain a required (f^*, g^*).

4 Concrete Realization

This section presents a concrete realization using Boolean functions in [20] as f, which construction is as follows:

Construction 2 [20]: $f(x)$ denotes a Boolean function on $\mathbb{F}_2^n$ and $Supp(f) = \{A^i b_1 | 0 \leq i \leq 2^{n-1}\}$, where $0 \neq b_1 \in \mathbb{F}_2^n$, A is the companion matrix of a primitive polynomial $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + 1$ over the field $\mathbb{F}_2$, i.e.

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & c_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}.$$

Theorem 3[20]: f has maximum degree n-1 and optimal algebraic immunity $\lceil n/2 \rceil$. Besides,it reaches a high nonlinearity, which is better than [5].

Now, a class of 1-resilient Boolean functions which is still degree maximized and algebraic immunity optimized has been possessed by using f aforementioned.

Example 1: Let $f \in \mathbb{F}_2^9$ be a Boolean function from Construction 2, where its nonlinearity is 236 [20]. We can get 1-resilient function h, where the lower bound is 472.

5 1-Resilient Functions with Sub-Optimal Algebraic Immunity

Generally, we can get a extended version of Construction 1 for any $n \geq 2$. This class of Boolean functions can achieve sub-optimized algebraic immunity.

Construction 3: let n be any integer such that $n \geq 2$ and f is a balanced Boolean function with maximum degree $n-1$ and optimal algebraic immunity $\lfloor (n+1)/2 \rfloor$, i.e. $f \in < 2^{n-1}, n-1, (n+1)/2; \delta_n, \cdots, \delta_1 >$. Let

$$h = (1 + x_{n+1})f + x_{n+1}g \in \mathbb{F}_2^{n+1},$$

where $g \in \hat{H}_f$.

Theorem 4: $h \in \mathbb{F}_2^{n+1}$ in Construction 3 is 1-resilient Boolean function with maximum degree and algebraic immunity at least $\lfloor (n+1)/2 \rfloor$, if $g \in \hat{M}_f$.

Example 2: We use the function $f \in \mathbb{F}_2^{16}$, where $N_f = 32556$ [20], then h is 1-resilient function with sub-optimal algebraic immunity and $N_h \geq 65112$.

6 Conclusion

In this paper, we have described a technique for constructing 1-resilient functions with maximum degree and optimal algebraic immunity on even number variables. Unfortunately, this construction only results a part of the entire functions belong to $< 2^n, n-1, (n+1)/2; 0, 0, \cdots, 0 >$. Because it has two subsets

$$< 2^{n-1}, n-1, (n+1)/2; \delta_n, \cdots, \delta_1 > \times < 2^{n-1}, n-1, (n-1)/2; -\delta_n, \cdots, -\delta_1 >,$$
$$< 2^{n-1}, n-2, (n+1)/2; \delta_n, \cdots, \delta_1 > \times < 2^{n-1}, d, (n+1)/2; -\delta_n, \cdots, -\delta_1 >,$$

where $n \geq 3$ is odd, $d < n-2$. The characteristic of those classes are so far hard to predict. The best nonlinearity of Construction 1 is unknown. Maybe by lowering the algebraic degree of one correlation class, we can get the functions with a higher nonlinearity. In the end, we present a larger class of 1-resilient Boolean functions with sub-optimal Algebraic immunity.

References

[1] J.-M Le Bars and A. Viola, "Equivalence classes of Boolean functions for first-order correlation," IEEE Transactions on Information Theory, vol. 56, no. 3, pp. 1247-1261, Mar, 2010.

[2] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," in Advances in Cryptology - CRYPTO'91 (Lecture Notes in Computer Sceince). Berlin, Germany: Springer-Verlag, 1992, vol. 547, pp. 86-100.

[3] C.Carlet, “On bent and highly nonlinear balanced / resilient functions and their algebraic immunities,” Proceedings of AAECC 16, LNCS 3857, pp. 1-28, 2006.

[4] C. Carlet, D. K. Dalai, K. C. Gupta and S. Maitra, “Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction,” IEEE Transactions on Information Theory, vol. 52, no. 7, pp. 3105-3121, Jul, 2006.

[5] C.Carlet and K.Feng, “An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity,” in Proc. Advances in Cryptology-ASIACRYPT, Nerlin, Germany, 2008, vol. 5350, Lecture Notes in Computer Science, pp 425-440.

[6] S. Chee, S. Lee, D. Lee and S. H. Sung, “On the correlation immune functions and their nonlinearity,” in Advances in CryptologyAsiacrypt’96 (Lecture Notes in Computer Sceince). Berlin, Germany: Springer-Verlag, 1997, vol. 1163, pp. 232-243.

[7] D. K. Dalai, K. C. Gupta, S. Maitra, “Notion of algebraic immunity and its evaluation related to fast algebraic attacks,” In Second International Workshop on Boolean Function Cryptography and Applications, 2006.

[8] J. F. Dillon, Elementary Hadamard difference set, Ph.D. Thesis, University of Maryland, 1974.

[9] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.

[10] W. Meier and O. Staffelbach, “Nonlinearity criteria for cryptographic functions,” in Advances in Cryptology - EUROCRYPT’89 (Lecture Notes in Computer Sceince), Berlin, Germany: Springer-Verlag, 1990, vol. 434, pp. 549-562.

[11] O. S. Rothaus, On ’bent’ functions, Journal of Combinatorial Theory, Ser.A, vol. 20, pp. 300-305, 1976.

[12] P. Sarkar and S. Maitra, “Construction of nonlinear Boolean functions with important cryptographic properties,” in Advances in Cryptology - EUROCRYPT 2000 (Lecture Notes in Computer Sceince), Berlin, Germany: Springer-Verlag, 2000, vol. 1807, pp. 485-506.

[13] P. Sarkar and S. Maitra, “Nonlinearity bounds and constructions of resilient Boolean functions,” in Advances in Cryptology - CRYPTO 2000 (Lecture Notes in Computer Sceince), Berlin, Germany: Springer-Verlag, 2000, vol. 1880, pp. 515-532.

[14] P. Sarkar and S. Maitra, “Construction of nonlinear resilient Boolean functions using small affine functions,” IEEE Transactions on Information Theory, vol. 50, no. 9, pp. 2185-2193, Sept. 2004.

[15] J. Seberry, X.M. Zhang, and Y. Zheng, “On constructions and nonlinearity of correlation immune Boolean functions,” in Advances in Cryptology - EUROCRYPT’93 (Lecture Notes in Computer Sceince), Berlin, Germany: Springer-Verlag, 1984, vol. 765, pp. 181-199.

[16] T. Siegenthaler, “Correlation-immunity of nonlinear combining functions for cryptographic applications,” IEEE Transactions on Information Theory, vol. 30, no.5, pp. 776-780, September 1984.

[17] Y. V. Tarannikov, "On resilient Boolean functions with maximum possible nonlinearity," in Progress in Cryptology - INDOCRYPT 2000 (Lecture Notes in Computer Science). Berlin, Germany: Springer Verlag, 2000, vol. 1977, pp. 19-30.

[18] Ziran Tu and Yingpu Deng, "A class of 1-resilient function with high nonlinearity and algebraic immunity," Cryptography ePrint Archive, Report 2010/179, 2010. http://eprint.iacr.org/.

[19] G.-Z. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," IEEE Transactions on Information Theory, vol. 34, no. 3, pp. 569-571, 1988.

[20] Qichun Wang, Jie Peng, Haibin Kan and Xiangyang Xue. "Constructions of cryptographiclly significant Boolean functions using primitive polynomials," Will appear in IEEE Transactions on Information Theory, Vol. 56,No. 6, June, 2010.