A Class of 1−Resilient Function with High Nonlinearity and Algebraic Immunity

Ziran Tu* Yingpu Deng†

Abstract

In this paper, we propose a class of 1-resilient Boolean function with optimal algebraic degree and high nonlinearity, moreover, based on the conjecture proposed in [4], it can be proved that the algebraic immunity of our function is at least suboptimal.

Keywords: Boolean function, correlation immunity, algebraic immunity, bent function, resilient function, balanced, nonlinearity, algebraic degree

1 Introduction

Symmetric crypto-systems are commonly used in encrypting and decrypting communications. Stream ciphers is a popular and traditional symmetric system, in which there are two usual models, the filter model and the combiner model, both models have a critical part—-boolean functions. To resist known attacks, there have been many criteria for designing boolean functions, such as balanced-ness, a high algebraic degree, a high nonlinearity and a high correlation immunity. The concept of correlation immunity was proposed by Siegenthaler, then Xiao and Massey gave a simple spectra characterization[11]. For this reason, many papers discussed functions with high nonlinearity and high-order correlation immunity, and there have been many constructions [14, 15, 16, 17], but many are Maiorana-McFarland like functions. When n is small, some resilient functions with maximal nonlinearity have been obtained[18, 19, 20]. Moreover, the recent algebraic attacks proposed by Courtois and Meier[1, 2, 3, 6] have received the world's attention, then the algebraic immunity of boolean functions has been introduced, and the study of annihilators of boolean functions become important. Well, designing a boolean function to meet all criteria is really a challenge. An infinite class of boolean functions with optimum algebraic immunity, optimal algebraic degrees and very high nonlinearity, were proposed by Carlet and K.Feng in[10]. Very recently, Tu and Deng proposed in [4] a class of algebraic immunity optimal functions of even number variables under an assumption of a combinatoric conjecture, the nonlinearity of these functions were even better than functions proposed in [10]. Although Carlet proved in [21] that the tu-deng function was weak against fast algebraic attacks, he could repair this weakness through small modifications. However,

*Henan University of Science and Technology, Luoyang 471003, PR China. Email:naturetu@gmail.com

†Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, CAS, Beijing 100080, PR China. Email:dengyp@amss.ac.cn

among all the main designing criteria of boolean functions, the correlation immunity was ignored by tu-deng function.

In this paper, we propose an infinite class of boolean functions when the number of variables n is even, which seems to satisfy all the main cryptographic criteria: 1-resilient, algebraic degree optimal, high nonlinearity, and based on the conjecture in [4], the algebraic immunity is at least suboptimal.

2 Preliminaries

Let n be a positive integer. A Boolean function on n variables is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, which is the finite field with two elements. We denote B_n the set of all nonzero n-variable boolean functions.

Every Boolean function f in B_n has a unique representation as a multivariate polynomials over $\mathbb{F}_2$

$$f(x_1, x_2, ..., x_n) = \sum_{I \subseteq \{1,...,n\}} a_I \prod_{i \in I} x_i$$

where the a_I's are in $\mathbb{F}_2$, such kind of representation is called the algebraic normal form (ANF). The algebraic degree $deg(f)$ of f is defined to be the maximum degree of those monomials with nonzero coefficients in its algebraic normal form. A Boolean function f is called affine if $deg(f) \leqslant 1$, we denote A_n the set of all affine functions in B_n. The support of f is defined as $supp(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$, and the $wt(f)$ is the number of vectors which lie in $supp(f)$. For two functions f and g in B_n, the Hamming distance $d(f, g)$ between f and g is defined as $wt(f + g)$. The nonlinearity $nl(f)$ of a Boolean function f is defined as the minimum Hamming distance between f and all affine functions, i.e. $\mathrm{nl}(f) = \mathrm{Min}_{g \in A_n} d(f, g)$.

For any $a \in \mathbb{F}_2^n$, the value

$$\mathrm{W}_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+<x,a>}$$

is called the Walsh spectrum of f at a, where $< x, a >$ denotes the inner product between x and a i.e.$< x, a >= x_1a_1 + \ldots + x_na_n$. If $W_f(a) = 0$ for $1 \leqslant wt(a) \leqslant m$, then f is called m-th order correlation immune, this is the famous Xiao-Massey characterization of correlation immune functions. Moreover, if f is also balanced, we call f is m-th order resilient. The nonlinearity of a Boolean function f can be expressed via its Walsh spectra by the next formula

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\mathrm{Max}_{a \in \mathbb{F}_2^n} |\mathrm{W}_f(a)|.$$

It is well-known the nonlinearity satisfies the following inequality

$$\mathrm{nl}(f) \leqslant 2^{n-1} - 2^{\frac{n}{2}-1}$$

when n is even, the above upper bound can be attained, and such Boolean functions are called bent [7]. Bent function has several equivalent definitions, for instance, a function f is *bent* is equivalent to say that $supp(f)$ is a $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$-difference set in the additive group of $\mathbb{F}_2^n$.

Definition 2.1. [6] *The algebraic immunity $AI_n(f)$ of a n-variable Boolean function $f \in B_n$ is defined to be the lowest degree of nonzero functions g such that $fg = 0$ or $(f+1)g = 0$.*

3 Main Results

In this section, we give our construction which originates from Dillon's *partial spread* function in [8] and discuss its main cryptographic properties.

Construction 3.1. *Let $n = 2k$ and $\mathbb{F}_{2^k}$ be a finite field, α is primitive in $\mathbb{F}_{2^k}$. Let $0 \leqslant s \leqslant 2^k - 2$ and $A = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^{k-1}-1}\}$, we define a n-variable function $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$, whose support $supp(f)$ is constituted by the following four parts:*

- $\{(x, y) : y = \alpha^i x, x \in \mathbb{F}_{2^k}^*, i = s+1, s+2, \cdots, s + 2^{k-1} - 1\}$
- $\{(x, y) : y = \alpha^s x, x \in A\}$
- $\{(x, 0) : x \in \mathbb{F}_{2^k} \setminus A\}$
- $\{(0, y) : y \in \mathbb{F}_{2^k} \setminus \alpha^s A\}$

Proposition 3.2. *Let function f be defined as in 3.1, then f is 1-resilient.*

Proof. The balanced-ness of f is trivial, we need to verify that $W_f(a) = 0$ for each a satisfying $wt(a) = 1$. When a, b are not all zeros, we have

$$\begin{aligned} W_f(a, b) &= \sum_{(x,y)\in\mathbb{F}_{2^k}} (-1)^{f(x,y)+tr(ax+by)} \\ &= -2 \sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)} \end{aligned}$$

we can see

$$\begin{aligned} \sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)} &= \sum_{i=t+1}^{t+2^{k-1}-1} \sum_{x\in\mathbb{F}_{2^k}^*} (-1)^{tr((a+b\alpha^i)x)} + \sum_{x\in A}(-1)^{tr((a+b\alpha^t)x)} \\ &+ \sum_{x\in\mathbb{F}_{2^k}\setminus A} (-1)^{tr(ax)} + \sum_{y\in\mathbb{F}_{2^k}\setminus\alpha^s A} (-1)^{tr(by)} \end{aligned}$$

We consider Walsh spectra of two kinds of points:

1. $a \neq 0$,$b = 0$, then

$$\begin{aligned} \sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)} &= 1 - 2^{k-1} + 2^k - |A| \\ &+ \sum_{x\in\mathbb{F}_{2^k}\setminus A} (-1)^{tr(ax)} + \sum_{x\in A}(-1)^{tr(ax)} \end{aligned}$$

2. $b \neq 0$,$a = 0$, then

$$\sum_{x,y \in supp(f)} (-1)^{tr(ax+by)} = 1 - 2^{k-1} + 2^k - |A| + \sum_{y \in \mathbb{F}_{2^k} \setminus \alpha^s A} (-1)^{tr(by)} + \sum_{y \in \alpha^s A} (-1)^{tr(by)}$$

Combining with the cardinality $|A| = 2^{k-1}+1$, then it is obvious to see that f is 1-resilient.

From Siegenthaler's inequality[22], we know that for a n-variable, m-th order resilient boolean function g, it should be satisfied that $m + deg(g) \leqslant n - 1$. Concerning to our construction, we will see that f in 3.1 is algebraic degree optimal.

Proposition 3.3. *Let function f be defined as in 3.1, then $deg(f) = n - 2$.*

Proof. Note that f is a ps^--like function. Let $g, h : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$, we define g by $supp(g) = \{(x, y) : y = \alpha^i x, x \in \mathbb{F}^*_{2^k}, i = s, s+1, \cdots, s + 2^{k-1} - 1\}$ and h by $supp(h) = \{(0, 0)\} \cup \{(x, y) : y = \alpha^s x, x \notin A\} \cup \{(x, 0) : x \notin A\} \cup \{(0, y) : y \notin \alpha^s A\}$, then $f = g + h$, and $g \in ps^-$, we know $deg(g) = k$ from [7], to prove $deg(f) = n-2$, we only need to prove $deg(h) = n - 2$. By Lagrange's interpolation formula, we have

$$\begin{aligned} h(x, y) &= (x^{2^k-1} + 1)(y^{2^k-1} + 1) + \sum_{a \notin A} ((x + a)^{2^k-1} + 1)((y + \alpha^s a)^{2^k-1} + 1) \\ &+ \sum_{a \notin A} ((x + a)^{2^k-1} + 1)(y^{2^k-1} + 1) + \sum_{b \notin \alpha^s A} (x^{2^k-1} + 1)((y + b)^{2^k-1} + 1) \end{aligned}$$

by collection of like terms, then

$$h(x, y) = x^{2^k-1}y^{2^k-1} + \sum_{a \notin A} (x+a)^{2^k-1}(y+\alpha^s a)^{2^k-1} + x^{2^k-1}(y+\alpha^s a)^{2^k-1} + (x+a)^{2^k-1}y^{2^k-1}$$

Since $|A| = 2^{k-1} + 1$, then the coefficient of $x^{2^k-1}y^{2^k-1}$ is zero, and then

$$\begin{aligned} h(x, y) &= \sum_{a \notin A} \sum_{j=1}^{2^k-1} \binom{2^k - 1}{j} x^{2^k-1-j}(y + \alpha^s a)^{2^k-1} + \sum_{a \notin A} \sum_{j=1}^{2^k-1} \binom{2^k - 1}{j} x^{2^k-1-j}y^{2^k-1} \\ &= \sum_{a \notin A} \sum_{j=1}^{2^k-1} \binom{2^k - 1}{j} x^{2^k-1-j} \sum_{l=0}^{2^k-1} \binom{2^k - 1}{l} y^{2^k-1-l}(\alpha^s a)^l \\ &+ \sum_{a \notin A} \sum_{j=1}^{2^k-1} \binom{2^k - 1}{j} x^{2^k-1-j}y^{2^k-1} \\ &= \sum_{a \notin A} \sum_{j=1}^{2^k-1} \sum_{l=1}^{2^k-1} \binom{2^k - 1}{j} \binom{2^k - 1}{l} x^{2^k-1-j}y^{2^k-1-l}a^j(\alpha^s a)^l \end{aligned}$$

It is easy to see $deg(h) \leqslant n-2$. Now consider the coefficient of $x^{2^k-1-1}y^{2^k-1-1}$

$$\sum_{a\notin A}\alpha^s a^2 = \alpha^s(\sum_{a\notin A} a)^2 = \alpha^s(\frac{1+\alpha^{2^{k-1}}}{1+\alpha})^2$$

which is apparently nonzero in $\mathbb{F}_{2^k}$, then $deg(h) = n-2$.

Owning to the similarity with Dillon's ps$^-$ function, f must have high nonlinearity, in fact, we can give a lower bound easily on nonlinearity from result in[10].

Proposition 3.4. *Let function f be defined as in 3.1, then $nl(f) \geqslant 2^{n-1} - 2^{k-1} - 3\cdot k\cdot 2^{\frac{k}{2}}ln2 - 7$.*

Proof. From the above proof we only need to consider

$$K_{(a,b)} = \sum_{(x,y)\in supp(f)}(-1)^{tr(ax+by)}$$

for (a,b) with $a\cdot b \neq 0$. By Carlet and K.Feng in [10], we know

$$|\sum_{x\in A}(-1)^{tr(\lambda x)}| \leqslant k\cdot 2^{\frac{k}{2}}ln2 + 2$$

then we can obtain an upper bound for $|K_{(a,b)}|$ easily:

1. $a + b\alpha^s = 0$, then

$$|K_{(a,b)}| \leqslant (2^{k-1}-1)(-1) + 2^{k-1} + 2\cdot(k\cdot 2^{\frac{k}{2}}ln2 + 2)$$

2. $a + b\alpha^i = 0$ for some i, $s < i < s + 2^{k-1}$, then

$$|K_{(a,b)}| \leqslant 2^{k-1} + 1 + 3\cdot(k\cdot 2^{\frac{k}{2}}ln2 + 2)$$

3. otherwise

$$|K_{(a,b)}| \leqslant -2^{k-1} + 1 + 3\cdot(k\cdot 2^{\frac{k}{2}}ln2 + 2)$$

Finally we get

$$nl(f) \geqslant 2^{n-1} - 2^{k-1} - 3\cdot k\cdot 2^{\frac{k}{2}}ln2 - 7$$

In fact, we can improve this lower bound according to the method in [23]. From the following table we can see the nonlinearity of f is satisfying:

n	$2^{n-1} - 2^{\frac{n}{2}-1}$	$nl(f)$
4	6	4
6	28	24
8	120	112
10	496	484
12	2016	1996
14	8128	8100
16	32640	32588
18	130816	130760

Maitra and Pasalic constructed a 8-variable, 1-resilient function with nonlinearity 116 in [20], which was maximal for 1-resilient functions. According the table, when $n = 8$ our f has nonlinearity 112, there is a minor difference, while from the conjecture proposed by Tu and Deng in [4], we discover that the algebraic immunity of our function is also satisfying. As a cornerstone of the tu-deng function, the conjecture attract many people's attention, some papers [12][13] try to attack this problem theoretically and some advances have been obtained, however, the complete proof remains to be mysterious. Here we briefly describe this conjecture:

Conjecture 3.5. *assume $k \in \mathbb{Z}$, $k > 1$, for every $x \in \mathbb{Z}$, we expand x as a binary string of length k, and denote the number of one's in the string by $w(x)$, for any $t \in \mathbb{Z}$, $0 < t < 2^k - 1$, let*

$$S_t = \{(a,b)|a,b \in \mathbb{Z}_{2^k-1}, a+b = t \ mod\ 2^k-1, w(a)+w(b) \leqslant k-1\}$$

then $|S_t| \leqslant 2^{k-1}$.

Using the same proof techniques, we can prove that f defined in 3.1 is at least algebraic immunity suboptimal, first we introduce a simple lemma:

Lemma 3.6. *For every $0 < t < 2^k - 1$, the modular equation $a+b = t \ mod\ 2^k-1, w(a)+w(b) = k-1$ has at least one pair of solution.*

Proof. At first we observe that, if t and t' belong to a same cyclotomic coset $mod\ 2^k - 1$, then the modular equations for t and t' have exactly the same number of solutions. Without loss of generality we suppose t have following forms:

$$t = \underbrace{11\cdots1}_{n_1}\underbrace{00\cdots0}_{n_2}\underbrace{1\cdots1}_{n_3}\underbrace{0\cdots0}_{n_4}\cdots\cdots\underbrace{1\cdots1}_{n_{2r-1}}\underbrace{0\cdots0}_{n_{2r}}$$

In order to prove the lemma, we only need to construct a pair of a, b to be a solution. If $0 \leqslant a, b < 2^k - 1$ satisfy $a + b = t \quad mod \ \ 2^k - 1$, then $w(a) + w(b) = w(t) + s$, in which s represents the number of carry when doing the modular addition. Using this relation we can construct a pair (a, b) satisfying conditions, let

$$a = \underbrace{\cdots}_{n_1-1}0\underbrace{1\cdots1}_{n_2}\underbrace{\cdots}_{n_3-1}0\underbrace{1\cdots1}_{n_4}\cdots\cdots\underbrace{\cdots}_{n_{2r-1}-1}\ 0\underbrace{0\cdots1}_{n_{2r}}0$$

$$b = \underbrace{\cdots}_{n_1-1}0\underbrace{0\cdots1}_{n_2}\underbrace{\cdots}_{n_3-1}0\underbrace{0\cdots1}_{n_4}\cdots\cdots\underbrace{\cdots}_{n_{2r-1}-1}\ 0\underbrace{0\cdots1}_{n_{2r}}0$$

It's not difficult to verify that (a, b) is a solution.

Proposition 3.7. *Let $n = 2k$, then the algebraic immunity of function f in 3.1 is at least suboptimal i.e $AI_n(f) \geqslant k - 1$.*

Proof. We need to prove that both $f, f + 1$ have no annihilators with degrees $\leqslant k - 2$. Let a non-zero Boolean function $h(x, y) : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ satisfy $deg(h) < k$ and $f \cdot h = 0$.

We will prove h = 0. Observe that h can be written as a polynomial of two variables on F_2^k as

$$h(x,y) = \sum_{i,j} h_{i,j} x^i y^j$$

By $deg(h) \leqslant k-2$ we have $h_{i,j} = 0$ $w(i) + w(j) \geqslant k-1$.

$$h(x, \gamma x) = \sum_{i,j} h_{i,j} x^i (\gamma x)^j = \sum_{t=0}^{2^k-1} h_t(\gamma) x^t$$

in which

$$h_t(\gamma) = \sum_{i+j=tmod2^k-1} h_{i,j}\gamma^j, w(i) + w(j) \leqslant k-2$$

Since $h(x,y)$ annihilates f, then $h_t(\gamma) = 0$ for $\gamma = \alpha^i$,$s+1 \leqslant i \leqslant s+2^{k-1}-1$, in other words, $h_t(\gamma)$ has consecutively $2^{k-1}-1$ roots, by BCH theorem[9], the number of nonzero coefficients in $h_t(\gamma)$ should be larger than or equal to 2^{k-1}. While according to the conjecture in [4] and lemma 3.6, if let

$$S'_t = \{(a,b)|a,b \in \mathbb{Z}_{2^k-1}, a+b = t\ mod\ 2^k-1, w(a)+w(b) \leqslant k-2\}$$

then $|S'_t| \leqslant 2^{k-1}-1$, a contradiction happens, then $h(x,y) = 0$. A proof for $f+1$ is completely similar. Then $AI_n(f) \geqslant k-1$.

Remark 3.8. *Although we only prove the algebraic immunity of f is suboptimal, by computer investigation we discover that when the number of variables n equals to* $6, 8, 10, 12$, *the algebraic immunity of f is always optimal. We have tried to prove it, unfortunately we don't succeed, we will leave it as an open problem.*

4 Conclusion

In this paper, we construct an infinite class of boolean functions when the number of variables n is even, which seems to meet all the main criteria for designing boolean functions: 1-resilient, algebraic degree optimal, having high nonlinearity and at least suboptimal algebraic immunity under the assumption of conjecture in [4]. We believe that this class of functions are of both theoretical and practical importance.

References

[1] F. Armknecht, *Improving fast algebraic attacks*, FSE 2004, LNCS 3017, pp. 65–82, Springer.

[2] N. T. Courtois, *Fast algebraic attacks on stream ciphers with linear feedback*, Crypto 2003, LNCS 2729, pp. 176–194, Springer.

[3] N. T. Courtois, W. Meier, *Algebraic attacks on stream ciphers with linear feedback*, Eurocrypt 2003, LNCS 2656, pp. 345–359, Springer.

[4] Tu Z and Deng Y. *A Conjecture on Binary String and Its Applications on Constructing Boolean Functions of Optimal Algebraic Immunity.* Cryptology ePrint Archive, Report 2009/272, 2009. http://eprint.iacr. org/.

[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.* ASIACRYPT 2008, LNCS 5350: pages 425–440, Springer.

[6] W. Meier, E. Psalic, C. Carlet, *Algebraic attacks and decomposition of boolean functions,*Eurocrypt 2004, LNCS 3027 pp. 474–491, Springer.

[7] O.S. Rothaus, *On bent functions*, Journal of Combinatorial Theory, Series A, 20(1976), 300–305.

[8] J.F. Dillon. *Elementary Hadamard Difference Sets.* Ph.D thesis, University of Maryland, 1974.

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

[10] C. Carlet and K. Feng. *An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity.* ASIACRYPT 2008, LNCS 5350: pages 425–440, Springer.

[11] X. Guo-Zhen and J. Massey. *A spectral characterization of correlation immune combining functions.* IEEE Transactions on Information Theory, 34(3):569-571, May 1988.

[12] T. W. Cusick, Yuan Li, and Pantelimon Stanica. *On a combinatoric conjecture.* Cryptology ePrint Archive, Report 2009/554, 2009. http: //eprint.iacr.org/.

[13] Jean-Pierre Flori, Hugues Randriambololona, Grard Cohen and Sihem Mesnager *On a conjecture about binary strings distribution.* Cryptology ePrint Archive, Report 2010/170, 2010. http: //eprint.iacr.org/.

[14] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. *On correlation immune functions.* In Advances in Cryptology - CRYPTO'91, pages 86-100. Springer-Verlag, 1992.

[15] S. Chee, S. Lee, D. Lee, and S. H. Sung. *On the correlation immune functions and their nonlinearity.* In Advances in Cryptology, Asiacrypt 96, number 1163 in Lecture Notes in Computer Science, pages 232-243. Springer-Verlag, 1996.

[16] E. Filiol and C. Fontaine. *Highly nonlinear balanced Boolean functions with a good correlation-immunity.* In Advances in Cryptology - EUROCRYPT'98. Springer- Verlag, 1998.

[17] E. Pasalic and T. Johansson. *Further results on the relation between nonlinearity and resiliency of Boolean functions.* In IMA Conference on Cryptography and Coding, number 1746 in Lecture Notes in Computer Science, pages 35-45. Springer- Verlag, 1999.

[18] Palash Sarkar and Subhamoy Maitra. *Nonlinearity Bounds and Constructions of Resilient Boolean Functions.* Advances in Cryptology CRYPTO 2000, Springer- Verlag, 2000

[19] E. Pasalic, S. Maitra, T. Johansson and P. Sarkar *New Constructions of Resilient and Correlation Immune Boolean Functions Achieving Upper Bound on Nonlinearity.* Electronic Notes in Discrete Mathematics Volume 6, April 2001, Pages 158-167 WCC2001, International Workshop on Coding and Cryptography

[20] S Maitra, E Pasalic. *Further constructions of resilient Boolean functions with very high nonlinearity.* IEEE Transactions on Information Theory 48:77, 1825-1834.

[21] C.Carlet. *On a weakness of the Tu-Deng function and its repair.* Cryptology ePrint Archive, Report 2009/606, 2009. http://eprint.iacr. org/.

[22] T. Siegenthaler. *Correlation-immunity of nonlinear combining functions for cryptographic applications.* IEEE Transactions on Information Theory, IT-30(5):776-780, September 1984.

[23] 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