Construction of Highly Nonlinear Resilient Boolean Functions Satisfying Strict Avalanche Criterion

WeiGuo Zhang and GuoZhen Xiao
(ISN Lab, Xidian University, Xi'an 710071, China)
Email: 29225355@qq.com

Abstract

A method is proposed to construct resilient Boolean functions on n variables (n even) satisfying strict avalanche criterion (SAC) with nonlinearity $> 2^{n-1} - 2^{n/2}$. A large class of cryptographic Boolean functions which were not known earlier are obtained.

Keywords: Boolean functions; nonlinearity; resiliency; strict avalanche criterion

1 Introduction

Boolean functions possessing multiple cryptographic criteria play an important role in the design of symmetric cryptosystems [5], [6], [2], [1], [4], [7], [10]. The following criteria for cryptographic Boolean functions are often considered: high nonlinearity, high resiliency, high algebraic degree and strict avalanche criterion (SAC). The tradeoffs among these criteria are difficult problems and have received lots of attention. To the best of our knowledge, the nonlinearity of the known constructed resilient Boolean functions satisfying SAC are not more than $2^{n-1} - 2^{\lfloor n/2 \rfloor}$ [5], [7]. In this paper, we present a method to obtain resilient Boolean functions on n variables (n even) satisfying SAC with nonlinearity $> 2^{n-1} - 2^{n/2}$.

2 Preliminaries

Let $\mathcal{B}_n$ denote the set of Boolean functions of n variables. A Boolean function $f(X_n) \in \mathcal{B}_n$ is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $X_n = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ 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 denote the additions over $\mathbb{F}_2$ by $\oplus$ and $\bigoplus_i$. For simplicity, we denote by $+$ the addition of vectors of $\mathbb{F}_2^n$. $f(X_n)$ is generally represented by its algebraic normal form (ANF):

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

where $\lambda_u \in \mathbb{F}_2,\ u = (u_1, \cdots, u_n)$. The algebraic degree of $f(X_n)$, 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. 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:

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

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

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

$f \in \mathcal{B}_n$ 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 [9], a spectral characterization of resilient functions has been presented.

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

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

In term of Walsh spectra, the nonlinearity of $f \in \mathcal{B}_n$ is given by [3]

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

The autocorrelation function of $f \in \mathcal{B}_n$ is defined by

$$C_f(\alpha) = \sum_{X_n \in \mathbb{F}_2^n} (-1)^{f(X_n) \oplus f(X_n + \alpha)} \tag{5}$$

The SAC was introduced by Webster and Tavares [8]. f satisfies SAC if

$$C_f(\alpha) = 0, \quad \text{for } wt(\alpha) = 1. \tag{6}$$

3 Construction

Construction: Let $n \geq 10$ be even, and let m be a nonnegative integers such that there exists an integer k with

$$k = \min_{m < s < n/2-1} \{s \mid 2^{n/2-s} \cdot \sum_{i=0}^{m} \binom{n/2}{i} \leq \sum_{j=m+1}^{s-m+1} \binom{s}{j}\}. \tag{7}$$

Let $T = \{c \in \mathbb{F}_2^k \mid m < wt(c) < n/2 - m\}$. For any $b \in \mathbb{F}_2^{n/2}$ with $0 \leq wt(b) \leq m$, let ψ_b: $\mathbb{F}_2^{n/2-k} \mapsto \mathbb{F}_2^k$ be an injective mapping such that

- $T_b = \{\psi_b(x') \mid x' \in \mathbb{F}_2^{n/2-k}\} \subset T$ for any $x' \in \mathbb{F}_2^{n/2-k}$;
- $\alpha' \in T_b$ if and only if $\overline{\alpha'} \in T_b$, where $\overline{\alpha'} = \alpha + (11 \cdots 1)$;
- If $b' \neq b$, then $T_b \bigcap T_{b'} = \emptyset$.

Let $S = \{b \in \mathbb{F}_2^{n/2} \mid m < wt(b) < n/2 - m\}$, and $\phi : S \mapsto S$ be a bijective mapping satisfying

$$\phi(\bar{b}) = \overline{\phi(b)}, \quad \text{for } wt(b) = m + 1. \tag{8}$$

Then for x, $y \in \mathbb{F}_2^{n/2}$, and $x = (x', x'') \in \mathbb{F}_2^{n/2-k} \times \mathbb{F}_2^k$ construct the function

$$f(y, x) = \bigoplus_{b \in \mathbb{F}_2^{n/2}} y^b \cdot g_b(x) \tag{9}$$

where

$$g_b(x) = \begin{cases} \psi_b(x')\cdot x'', & 0 \le wt(b) \le m \\ \phi(b)\cdot x, & m < wt(b) < n/2-m \\ \psi_{\overline{b}}(x')\cdot x'' \oplus \bigoplus_{i=1}^{n/2} x_i \oplus 1, & n/2-m \le wt(b) \le n/2. \end{cases} \tag{10}$$

Theorem: Let $f \in \mathbb{F}_2^n$ be given by the Construction. Then f the following statements holds:

- f is m-resilient;
- $N_f = 2^{n-1} - 2^{n/2-1} - 2^k$;
- f satisfies the SAC.

Proof: Let $\alpha \in \mathbb{F}_2^{n/2}$ where $\alpha' \in \mathbb{F}_2^{n/2-k}$ and $\alpha'' \in \mathbb{F}_2^k$. Let

$$\Gamma_1 = \{g_b \mid b \in \mathbb{F}_2^{n/2}, m < wt(b) < n/2-m\}.$$

For any $g_b \in \Gamma_1$, we have

$$\begin{aligned} W_{g_b}(\alpha) &= \sum_{x\in\mathbb{F}_2^{n/2}} (-1)^{\phi(b)\cdot x \oplus \alpha\cdot x} && (11) \\ &= \begin{cases} 2^n, & \alpha = \phi(b) \\ 0, & \text{otherwise.} \end{cases} && (12) \end{aligned}$$

Let

$$\Gamma_2 = \{g_b \mid b \in \mathbb{F}_2^{n/2}, 0 \le wt(b) \le m\}.$$

For any $g_b \in \Gamma_2$, we have

$$\begin{aligned} W_{g_b}(\alpha) &= \sum_{x\in\mathbb{F}_2^{n/2}} (-1)^{\psi_b(x')\cdot x'' \oplus \alpha'\cdot x' \oplus \alpha''\cdot x''} && (13) \\ &= \sum_{x'\in\mathbb{F}_2^{n/2-k}} (-1)^{\alpha'\cdot x'} \sum_{x''\in\mathbb{F}_2^k} (-1)^{(\psi_b(x')+\alpha'')\cdot x''} && (14) \\ &= \begin{cases} \pm 2^k, & \alpha'' \in T_b \\ 0, & \text{otherwise.} \end{cases} && (15) \end{aligned}$$

Let

$$\Gamma_3 = \{g_b \mid b \in \mathbb{F}_2^{n/2}, n/2-m \le wt(b) \le n/2\}.$$

For any $g_b \in \Gamma_3$, we have

$$W_{g_b}(\alpha) = \begin{cases} \pm 2^k, & \alpha'' \in T_{\overline{b}} \\ 0, & \text{otherwise.} \end{cases} \tag{16}$$

For α, $\beta \in \mathbb{F}_2^{n/2}$, and $\alpha = (\alpha', \alpha'') \in \mathbb{F}_2^{n/2-k} \times \mathbb{F}_2^k$, we have

$$\begin{aligned} W_f(\beta,\alpha) &= \sum_{(y,x)\in\mathbb{F}_2^n} (-1)^{f(y,x)\oplus(\beta,\alpha)\cdot(y,x)} && (17) \\ &= \sum_{b\in\mathbb{F}_2^{n/2}} (-1)^{\beta\cdot b} \sum_{x\in\mathbb{F}_2^{n/2}} (-1)^{g_b(x)\oplus\alpha\cdot x} && (18) \\ &= \sum_{b\in\mathbb{F}_2^{n/2}} (-1)^{\beta\cdot b} W_{g_b}(\alpha) && (19) \\ &= U_1 + U_2 + U_3 && (20) \end{aligned}$$

where

$$U_i = \sum_{g_b \in \Gamma_i} (-1)^{\beta \cdot b} W_{g_b}(\alpha), \quad i = 1, 2, 3. \tag{21}$$

Obviously, Γ_1, Γ_2 and Γ_3 are sets of disjoint spectra functions. So we have $U_1 \in \{0, \pm 2^{n/2}\}$, $U_2 \in \{0, \pm 2^k\}$, and $U_3 \in \{0, \pm 2^k\}$. Thus,

$$\max_{(\beta,\alpha)\in\mathbb{F}_2^n} |W_f(\beta, \alpha)| = 2^{n/2} + 2^{k+1}. \tag{22}$$

From (4), $N_f = 2^{n-1} - 2^{n/2-1} - 2^k$.

Thanks to the Lemma, for any $b \in \mathbb{F}_2^{n/2}$, $g_b(x)$ is an m-resilient Boolean function. Then $f(y, x)$ is an m-resilient function.

Next we prove that f satisfies SAC.

$$\begin{aligned} C_f(\beta, \alpha) &= \sum_{(y,x)\in\mathbb{F}_2^n} (-1)^{f(y,x)\oplus f(y+\beta,x+\alpha)} && (23) \\ &= \sum_{(y,x)\in\mathbb{F}_2^n} (-1)^{\bigoplus_b y^b \cdot g_b(x) \oplus \bigoplus_b (y+\beta)^b \cdot g_b(x+\alpha)} && (24) \end{aligned}$$

When $wt(\beta, \alpha) = 1$, to obtain $C_f(\beta, \alpha)$, there exist two cases to be considered:

Case 1: $wt(\beta) = 0$ and $wt(\alpha) = 1$. We have

$$\begin{aligned} C_f(\beta, \alpha) &= \sum_{(y,x)\in\mathbb{F}_2^n} (-1)^{\bigoplus_b y^b (g_b(x)\oplus g_b(x+\alpha))} && (25) \\ &= \sum_{b\in\mathbb{F}_2^{n/2}} \sum_{x\in\mathbb{F}_2^{n/2}} (-1)^{g_b(x)\oplus g_b(x+\alpha)} && (26) \\ &= 2^{n/2} \sum_{b\in S} (-1)^{\phi(b)\cdot\alpha} + \sum_{b\in\mathbb{F}_2^{n/2}\setminus S} C_{g_b}(\alpha) && (27) \end{aligned}$$

Note that

$$\sum_{b\in S} (-1)^{\phi(b)\cdot\alpha} = 0 \tag{28}$$

and for any $b \in \mathbb{F}_2^{n/2} \setminus S$

$$C_{g_b}(\alpha) = 0 \tag{29}$$

We have $C_f(\beta, \alpha) = 0$.

Case 2: $wt(\beta) = 1$ and $wt(\alpha) = 0$. In this case,

$$C_f(\beta, \alpha) = \sum_{b\in\mathbb{F}_2^{n/2}} \sum_{x\in\mathbb{F}_2^{n/2}} (-1)^{g_b(x)\oplus g_{b+\beta}(x)}. \tag{30}$$

1) Let $E_1 = \{b \in \mathbb{F}_2^{n/2} | \ 0 \le wt(b) \le m, 0 \le wt(b + \beta) \le m\}$. When $b \in E_1$, we have

$$g_b(x) \oplus g_{b+\beta}(x) = (\psi_b(x') + \psi_{b+\beta}(x')) \cdot x'' \tag{31}$$

Since $T_b \bigcap T_{b+\beta} = \emptyset$, for any $x' \in \mathbb{F}_2^{n/2-k}$, $\psi_b(x') + \psi_{b+\beta}(x') \neq \mathbf{0}$ Thus, $g_b(x) \oplus g_{b+\beta}(x)$ is a balanced function. So we have

$$\sum_{b \in E_1} \sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{g_b(x) \oplus g_{b+\beta}(x)} = 0 \tag{32}$$

2) Let $E_2 = \{b \in \mathbb{F}_2^{n/2} |\ m < wt(b) < n/2 - m, m < wt(b+\beta) < n/2 - m\}$. When $b \in E_2$, we have

$$g_b(x) \oplus g_{b+\beta}(x) = (\phi(b) + \phi(b+\beta)) \cdot x \tag{33}$$

Since ϕ is an injective mapping, $\phi(b) + \phi(b+\beta) \neq \mathbf{0}$. Thus, $g_b(x) \oplus g_{b+\beta}(x)$ is a balanced linear function. So

$$\sum_{b \in E_2} \sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{g_b(x) \oplus g_{b+\beta}(x)} = 0. \tag{34}$$

3) Let $E_3 = \{b \in \mathbb{F}_2^{n/2} |\ wt(b) = m, wt(b+\beta) = m+1\}$ and $E_3' = \{b \in \mathbb{F}_2^{n/2} |\ wt(b) = n/2 - m, wt(b+\beta) = n/2 - m - 1\}$. Obviously, $b \in E_3$ if and only if $\overline{b} \in E_3'$. For any $\overline{b} \in E_3'$, we have

$$g_{\overline{b}}(x) = \psi_b(x') \cdot x'' \oplus \bigoplus_{i=1}^{n/2} x_i \oplus 1 \tag{35}$$

and

$$g_{\overline{b}+\beta}(x) = \phi(\overline{b}+\beta) \cdot x \overset{(8)}{=} \overline{\phi(b+\beta)} = \phi(b+\beta) \oplus \bigoplus_{i=1}^{n/2} x_i \tag{36}$$

So

$$g_{\overline{b}}(x) + g_{\overline{b}+\beta}(x) = g_b(x) + g_{b+\beta}(x) \oplus 1 \tag{37}$$

i.e.

$$\sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{g_b(x) \oplus g_{b+\beta}(x)} + \sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{g_{\overline{b}}(x) + g_{\overline{b}+\beta}(x)} = 0 \tag{38}$$

Thus

$$\sum_{b \in E_3 \cup E_3'} \sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{g_b(x) \oplus g_{b+\beta}(x)} = 0. \tag{39}$$

4) Let $E_4 = \{b \in \mathbb{F}_2^{n/2} |\ wt(b) = m+1, wt(b+\beta) = m\}$ and $E_4' = \{b \in \mathbb{F}_2^{n/2} |\ wt(b) = n/2 - m - 1, wt(b+\beta) = n/2 - m\}$. Similar to the derivation in 3), we have

$$\sum_{b \in E_4 \cup E_4'} \sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{g_b(x) \oplus g_{b+\beta}(x)} = 0. \tag{40}$$

Note that $E_1 \cup E_2 \cup E_3 \cup E_3' \cup E_4 \cup E_4' = \mathbb{F}_2^{n/2}$, we have

$$C_f(\beta, \alpha) \;\; = \;\; \sum_{b \in \mathbb{F}_2^{n/2}} \sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{g_b(x) \oplus g_{b+\beta}(x)} = 0, \quad \text{for } wt(\beta, \alpha) = 1. \tag{41}$$

Hence, f satisfies SAC. □

Table: Achieved nonlinearity $2^{n-1} - 2^{n/2-1} - 2^k$ for n-variable, m-resilient functions satisfying SAC.

$m = 1$																		
n	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50
k	6	7	7	8	8	9	9	10	11	11	12	12	13	13	14	14	15	15
$m = 2$																		
n	22	24	26	28	30	32	34	36	38	40	44	46	48	50	52	54	56	58
k	9	10	10	11	12	12	13	13	14	14	15	16	17	17	18	18	19	19
$m = 3$																		
n	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60
k	11	12	13	13	14	15	15	16	16	17	18	18	19	19	20	20	21	22
$m = 4$																		
n	32	34	36	38	40	42	44	48	50	52	54	56	58	60	62	64	66	68
k	14	15	16	16	17	17	18	19	20	21	21	22	22	23	24	24	25	25
$m = 5$																		
n	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64	66	68	70
k	16	17	18	18	19	20	20	21	22	22	23	24	24	25	25	26	27	27
$m = 6$																		
n	42	44	46	48	50	52	54	56	58	60	62	64	66	68	70	72	74	76
k	19	20	21	21	22	23	23	24	25	25	26	27	27	28	28	29	30	30
$m = 7$																		
n	46	48	50	52	54	56	58	60	62	64	66	70	72	74	76	78	80	82
k	21	22	23	24	24	25	26	26	27	28	28	30	30	31	31	32	33	33
$m = 8$																		
n	52	54	56	58	60	62	64	66	68	70	72	74	76	78	80	82	84	86
k	24	23	26	26	27	28	28	29	30	30	31	32	32	33	34	34	35	36
$m = 9$																		
n	56	58	60	62	64	66	68	70	72	74	76	78	80	82	84	86	88	90
k	26	27	28	29	29	30	31	31	32	33	33	34	35	35	36	37	37	38
$m = 10$																		
n	60	62	64	66	68	70	72	74	76	78	80	82	84	86	88	90	92	94
k	28	29	30	31	31	32	33	34	34	35	36	36	37	38	38	39	40	40

References

[1] S. Maitra and E. Pasalic, "A Maiorana-McFarland type construction for resilient functions on variables (n even) with nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$," Discrete Applied Mathematics, vol. 154, pp. 357-369, 2006.

[2] S. Maitra and E. Pasalic, "Further constructions of resilient Boolean functions with very high nonlinearity," IEEE Transations on Information Theory, vol. 48, no. 7, pp. 1825-1834, 2002.

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

[4] E. Pasalic, "Maiorana-McFarland class: degree optimization and algebraic properties," IEEE Transactions on Information Theory, vol. 52, no.10, pp.4581-4594, 2006.

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

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

[7] P. Stanica, S. H. Sung. Boolean functions with five controllable cryptographic properties. Designs, Codes and Cryptography, vol. 31, no. 2, pp.147-157, 2004.

[8] A. F. Webster and S. E. Tavares, "On the design of S-box," in Advances in Cryptology - CRYPTO'85 (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, 1986, vol. 218, pp. 523-524.

[9] GZ. 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.

[10] W. Zhang and G. Xiao, "Constructions of almost optimal resilient Boolean functions on large even number of variables," IEEE Transactions on Information Theory, vol. 55, no. 12, pp. 5822-5831, 2009.