LETTER

On the Construction of Balanced Boolean Functions with Strict Avalanche Criterion and Optimal Algebraic Immunity

Deng TANG[†,††a)], ***Member***

SUMMARY Boolean functions used in the filter model of stream ciphers should have balancedness, large nonlinearity, optimal algebraic immunity and high algebraic degree. Besides, one more criterion called strict avalanche criterion (SAC) can be also considered. During the last fifteen years, much work has been done to construct balanced Boolean functions with optimal algebraic immunity. However, none of them has the SAC property. In this paper, we first present a construction of balanced Boolean functions with SAC property by a slight modification of a known method for constructing Boolean functions with SAC property and consider the cryptographic properties of the constructed functions. Then we propose an infinite class of balanced functions with optimal algebraic immunity and SAC property in odd number of variables. This is the first time that such kind of functions have been constructed. The algebraic degree and nonlinearity of the functions in this class are also determined.

key words: *Boolean function, balancedness, algebraic immunity, strict avalanche criterion, nonlinearity*

1. Introduction

Boolean functions play a central role in the security of stream ciphers. To resist all the known attacks on each model of stream cipher, Boolean functions used in stream ciphers must satisfy several criteria (hopefully, all) simultaneously. The following criteria of cryptographic Boolean functions are mandatory [1], [2]: balancedness, high nonlinearity, high algebraic degree, optimal algebraic immunity, and good immunity to fast algebraic attacks. Besides, one more criterion can be also considered: the *strict avalanche criterion* (SAC). In this paper, Boolean functions with SAC property are called SAC Boolean functions for short.

Up to now, there are many classes of balanced Boolean functions with optimal algebraic immunity which have been proposed, for instance in [3]–[20]. However, none of them has the SAC property. In this paper, we construct an infinite class of balanced SAC Boolean functions in odd number of variables with optimal algebraic immunity, which is the first time that such functions have been constructed. We also determine the algebraic degree and nonlinearity of the functions in this class.

The organization of the remainder of this paper is as follows. In Sect. 2, the notations and the necessary preliminaries required for the subsequent sections are reviewed. In Sect. 3, we fist recall a known method for constructing SAC Boolean functions and then present a construction of balanced SAC Boolean functions. The cryptographic properties of the constructed functions are considered. Sect. 4 proposes an infinite class of Balanced SAC functions with optimal algebraic immunity in odd number of variables. Finally, Sect. 5 concludes the paper.

Manuscript received March 2, 2019.

[†]The author is with School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China.

[††]The author is with the Guangxi Key Laboratory of Cryptography and Information Security, Guilin 541000, China.

a) E-mail: dtang@foxmail.com

DOI: 10.1587/transfun.E102.A.1321

2. Preliminaries

Let $\mathbb{F}_2^n$ be the vector space of n-tuples over the finite field $\mathbb{F}_2$. For any positive integer n, we shall denote by $\mathbf{0}_n$ (respectively $\mathbf{1}_n$) the all-zero vector (respectively all-one vector) of $\mathbb{F}_2^n$. A *Boolean function* in n variables is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Denote by $\mathcal{B}_n$ the set of all the 2^{2^n} Boolean functions in n variables. The basic representation of an n-variable Boolean function f is by its *truth table*, i.e.,

$$f = [f(0,0,\cdots,0), f(1,0,\cdots,0), \cdots, f(1,1,\cdots,1)].$$

The *support* of f, denoted by $\mathrm{Supp}(f)$, is defined as the set $\{x \in \mathbb{F}_2^n \mid f(x) \neq 0\}$. The *Hamming weight* of f, denoted by $\mathrm{wt}(f)$, is defined as the Hamming weight of the truth table of f, or equivalently, the size of the support of f.

It is well-known that any Boolean function $f \in \mathcal{B}_n$ can be uniquely represented by the algebraic normal form (ANF), i.e., $f(x_1,\cdots,x_n) = \bigoplus_{u\in\mathbb{F}_2^n} a_u\Big(\prod_{j=1}^n x_j^{u_j}\Big)$, where $a_u \in \mathbb{F}_2$ and $u = (u_1,\cdots,u_n)$. It is well-known [1], [21] that

$$a_u = \sum_{v\preceq u} f(v), \tag{1}$$

where $v = (v_1,\cdots,v_n)$ and $v \preceq u$ means that $v_i \leq u_i$ for all $1 \leq i \leq n$. The *algebraic degree*, denoted by $\deg(f)$, is the maximal value of $\mathrm{wt}(u)$ such that $a_u \neq 0$, where the Hamming weight $\mathrm{wt}(u)$ of a binary vector $u \in \mathbb{F}_2^n$ is the number of its nonzero coordinates, or in other words, the size of its support $\{1 \leq i \leq n \mid u_i \neq 0\}$). A Boolean function is called an *affine function* if its algebraic degree is at most 1. The set of all affine functions is denoted by A_n.

The *nonlinearity* $nl(f)$ of a Boolean function $f \in \mathcal{B}_n$ is the minimum Hamming distance from f to all the affine functions A_n, i.e. $nl(f) = \min_{g\in A_n}(d_H(f,g))$, where $d_H(f,g)$ is the *Hamming distance* between f and g, i.e., $d_H(f,g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|$. The nonlinearity can also be computed by means of the Walsh transform of f. The *Walsh transform* of a Boolean function $f \in \mathcal{B}_n$ at a is defined as $W_f(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}$. It can be easily seen that f is balanced if and only if $W_f(\mathbf{0}_n) = 0$. By the Walsh transform the nonlinearity of a Boolean function $f \in \mathcal{B}_n$ can be computed as

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}|W_f(a)|.$$

For resisting the standard algebraic attack [22], a new cryptographic criterion for Boolean functions used in stream ciphers, called *algebraic immunity*, has been proposed.

Definition 1 ([23]). *Given two n-variable Boolean functions f and h, we say that h is an annihilator of f if $f(x)h(x) = fh = 0$. We denote by $AN(f)$ the set of nonzero annihilators of f. The algebraic immunity $AI(f)$ of Boolean function f is defined to be the minimum algebraic degree of $AN(f) \cup AN(f+1)$.*

It was proved in [22] that $AI(f) \le \lceil \frac{n}{2} \rceil$ for any n-variable Boolean function f. In this paper, a Boolean function f of n variables is said to have *optimal algebraic immunity* if it achieves this bound with equality, and to have *almost optimal algebraic immunity* if $AI(f) = \lceil \frac{n}{2} \rceil - 1$.

The autocorrelation function of a Boolean function f at a point α is defined as

$$C_f(\alpha) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+f(x+\alpha)}.$$

A Boolean function $f \in \mathcal{B}_n$ is said to satisfy strict avalanche criterion (SAC) [24] if

$$C_f(\alpha) = 0 \text{ for all } \mathrm{wt}(\alpha) = 1.$$

3. Balanced SAC Functions and Their Cryptographic Properties

In this section, we first recall a known method for constructing SAC Boolean functions and then study the main cryptographic properties of the Boolean functions generated by this method.

3.1 A Known Method for Constructing SAC Boolean Functions

For simplicity, we denote $x' = (x_1, \cdots, x_n)$ for a given vector $x = (x_1, \cdots, x_{n+1}) \in \mathbb{F}_2^{n+1}$ from now on.

We now recall a known method for constructing Boolean functions with SAC property, which was introduced in [25]. Let $\mu_0 \in \mathcal{B}_n$ be an arbitrary Boolean function of variables $x_1, \cdots, x_n$ and $\nu \in \mathcal{B}_n$ be the function $\mu_0(x) + \mathbf{1}_n \cdot x + c$, where $c \in \mathbb{F}_2$. It was proved in [25] that the function $h_0 \in \mathcal{B}_{n+1}$ on variables $x_1, \cdots, x_{n+1}$ of the form

$$h_0(x', x_{n+1}) = (1 + x_{n+1})\mu_0(x') + x_{n+1}\nu(x') \tag{2}$$

satisfies the SAC property.

3.2 Balanced SAC Functions and Their Cryptographic Properties

From cryptographic viewpoints, we are interested in the balanced SAC functions with optimal algebraic immunity, high algebraic degree, and high nonlinearity. According to (2), we shall get balanced SAC functions from the following construction.

Construction 1. *Let $n \ge 2$ be a positive integer and $\mu_1 \in \mathcal{B}_n$ be a function such that $\mathrm{wt}(\mu_1 + \mathbf{1}_n \cdot x) \in \{\mathrm{wt}(\mu_1), 2^n - \mathrm{wt}(\mu_1)\}$. Then we construct the Boolean function $h_1 \in \mathcal{B}_{n+1}$ as follows*

$$h_1(x', x_{n+1}) = (1 + x_{n+1})\mu_1(x') + x_{n+1}(\mu_1(x') + \mathbf{1}_n \cdot x' + c),$$

where

$$c = \begin{cases} 0 & \text{if } \mathrm{wt}(\mu_1 + \mathbf{1}_n \cdot x') = 2^n - \mathrm{wt}(\mu_1) \\ 1 & \text{if } \mathrm{wt}(\mu_1 + \mathbf{1}_n \cdot x') = \mathrm{wt}(\mu_1) \end{cases}.$$

3.2.1 Balancedness, Algebraic Degree and Nonlinearity

We can see that the truth table of $h_1 \in \mathcal{B}_{n+1}$ is the concatenation of the truth tables of $\mu_1(x')$ and $\mu_1(x') + \mathbf{1}_n \cdot x' + c$. Therefore, $\mathrm{wt}(h_1) = \mathrm{wt}(\mu_1) + \mathrm{wt}(\mu_1(x') + \mathbf{1}_n \cdot x' + c) = \mathrm{wt}(\mu_1) + 2^n - \mathrm{wt}(\mu_1) = 2^n$. This implies that h_1 is balanced.

We can easily get the following theorem. Its proof is routine and we omit it here.

Theorem 1. *For every Boolean function $h_1 \in \mathcal{B}_{n+1}$, we have:*

$$nl(h_1) \ge 2nl(\mu_1) \text{ and}$$

$$\deg(h_1) = \begin{cases} \deg(\mu_1), & \text{if } \deg(\mu_1) \ge 2 \\ 2, & \text{if } \deg(\mu_1) < 2 \end{cases}.$$

3.2.2 Algebraic Immunity

We now show the relation from the viewpoints of algebraic immunity between h_1 and μ_1. To this end, we first give some preliminary results.

Lemma 1 ([26]). *Let n be an odd integer and f be a balanced Boolean function of n variables. Then, f has optimal algebraic immunity $\frac{n+1}{2}$ if and only if $AN(f)$ does not contain any function of degree strictly less than $\frac{n+1}{2}$.*

Lemma 2 ([27]). *Let g, h be two Boolean functions on variables $x_1, x_2, \cdots, x_n$ with $AI(g) = d_1$ and $AI(h) = d_2$. Let $f(x_1, \cdots, x_n, x_{n+1}) = (1 + x_{n+1})g(x') + x_{n+1}h(x') \in \mathcal{B}_{n+1}$. Then*

1) *if $d_1 \ne d_2$ then $AI(f) = \min\{d_1, d_2\} + 1$.*
2) *if $d_1 = d_2 = d$, then $d \le AI(f) \le d + 1$. Further, $AI(f) = d$ if and only if there exists $g_1, h_1 \in \mathcal{B}_n$ of algebraic degree d such that $\{gg_1 = 0, hh_1 = 0\}$ or $\{(1+g)g_1 = 0, (1+h)h_1 = 0\}$ and $\deg(g_1 + h_1) \le d - 1$.*

By Lemmas 1 and 2, we can easily deduce the following corollary.

Corollary 1. *Let n be an even number and $g, h \in \mathcal{B}_{n+1}$ be two Boolean functions such that* $\min\{d \mid d = \deg(s), 0 \neq s \in AN(g)\} = d_1$ *and* $\min\{d \mid d = \deg(s), 0 \neq s \in AN(h)\} = d_2$. *Let $f = (1 + x_{n+1})g + x_{n+1}h \in \mathcal{B}_{n+1}$. Then*

1) *if $d_1 \neq d_2$ then $AI(f) = \min\{d_1, d_2\} + 1$.*
2) *if $d_1 = d_2 = d$, then $d \leq AI(f) \leq d + 1$. Further, $AI(f) = d$ if and only if there exists $g_1, h_1 \in \mathcal{B}_n$ of algebraic degree d such that $\{gg_1 = 0, hh_1 = 0\}$ and* $\deg(g_1 + h_1) \leq d - 1$.

4. A Class of Balanced SAC Functions with Optimal Algebraic Immunity in Odd Variables

Let us first recall the definition of the majority function and introduce some basic known results on the majority function.

Definition 2. *An n-variable Boolean function f_0 on variables $x_1, x_2, \cdots, x_n$ defined by*

$$f_0(x) = \begin{cases} 0 & \text{if } \mathrm{wt}(x) < \lceil \frac{n}{2} \rceil \\ 1 & \text{if } \mathrm{wt}(x) \geq \lceil \frac{n}{2} \rceil \end{cases}$$

is called the majority function.

For any positive integer n, we define the Boolean function $f_1 \in \mathcal{B}_n$ as follows:

$$f_1(x) = \begin{cases} 0 & \text{if } \mathrm{wt}(x) \leq \lfloor \frac{n}{2} \rfloor \\ 1 & \text{otherwise} \end{cases}.$$

In [3], the authors have studied the cryptographic properties of f_1:

Lemma 3 ([3]). *The function $f_1 \in \mathcal{B}_n$ has the following cryptographic properties:*

1) $\deg(f_1) = 2^{\lfloor \log_2 n \rfloor}$;
2) $AI(f_1) = \lceil \frac{n}{2} \rceil$;
3) $nl(f_1) = 2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$.

Note that $f_0(x) = f_1(x + \mathbf{1}_n) + 1$ for even n and note that the algebraic immunity, algebraic degree and nonlinearity are affine invariant. Therefore, the majority function f_0 has the same these cryptographic properties as the function f_1.

We now present our construction and give their cryptographic properties.

Construction 2. *Let $n \geq 4$ be an even number. Let $\mu_2 \in \mathcal{B}_n$ be the majority function f_0 on variables $x_1, x_2, \cdots, x_n$. Then we construct the Boolean function $f_2 \in \mathcal{B}_{n+1}$ as follows*

$$f_2(x_1, \cdots, x_{n+1}) = (1 + x_{n+1})\mu_2 + x_{n+1}(\mu_2 + l + c),$$

where

$$c = \begin{cases} 0 & \text{if } n = 2 \pmod 4 \\ 1 & \text{if } n = 0 \pmod 4 \end{cases}$$

and $l = \mathbf{1}_n \cdot x'$.

By (2), we can see that the functions $f_2 \in \mathcal{B}_{n+1}$ generated by Construction 2 satisfy the SAC. In what follows, we will discuss the balancedness, nonlinearity, algebraic immunity, and algebraic degree of f_2, respectively.

4.1 Balancedness

First, we consider the balancedness of f_2. To this end, we need some preliminary results. For any positive integer n and a fixed $\omega \in \mathbb{F}_2^n$ with $\mathrm{wt}(\omega) = k$, we have

$$\sum_{\mathrm{wt}(x)=i} (-1)^{\omega \cdot x} = \sum_{j=0}^{i} (-1)^j \binom{k}{j} \binom{n-k}{i-j} = K_i(k, n),$$

where $K_i(x, n)$ is the Krawtchouk polynomial [28]. The following two lemmas about Krawtchouk polynomial will be useful to prove the balancedness of f_2.

Lemma 4 ([28]). *The Krawtchouk polynomials have the following properties.*

1. *$K_i(k, n) = (-1)^i K_i(n - k, n)$;*
2. *$\binom{n}{k} K_i(k, n) = \binom{n}{i} K_k(i, n)$.*

Lemma 5 ([8]). *The equality*

$$\sum_{i=0}^{r} K_i(k, n) = K_r(k - 1, n - 1)$$

holds for $0 \leq r \leq n$ and $n, k \geq 1$.

Theorem 2. *Let f_2 be an $(n+1)$-variable Boolean function given by Construction 2, then f_2 is a balanced SAC Boolean function.*

Proof. It follows from Sect. 3.1 that f_2 has the SAC property. So we only need to prove that f_2 is balanced. Note that $W_{\mu_2+l+c}(\mathbf{0}_n) = (-1)^c W_{\mu_2}(\mathbf{1}_n)$. Then we have

$$W_{f_2}(\mathbf{0}_{n+1}) = \begin{cases} W_{\mu_2}(\mathbf{0}_n) + W_{\mu_2}(\mathbf{1}_n) = 0, n = 2 \mod 4 \\ W_{\mu_2}(\mathbf{0}_n) - W_{\mu_2}(\mathbf{1}_n) = 0, n = 0 \mod 4. \end{cases}$$

We can easily get that $W_{\mu_2}(\mathbf{0}_n) = -\binom{n}{n/2}$ and $W_{\mu_2+1}(\mathbf{1}_n) = -2 \sum_{i=0}^{n/2-1} K_i(n, n)$. Then by Lemma 5 we have $\sum_{i=0}^{n/2-1} K_i(n, n) = K_{n/2-1}(n - 1, n - 1)$. Moreover, by item 1 of Lemma 4, we have

$$K_{n/2-1}(n - 1, n - 1) = (-1)^{n/2-1} K_{n/2-1}(0, n - 1).$$

Therefore, we get that

$$\begin{aligned} W_{\mu_2+1}(\mathbf{1}_n) &= (-1)^{n/2} 2 K_{n/2-1}(0, n - 1) \\ &= (-1)^{n/2} 2 \binom{n-1}{n/2-1} \\ &= (-1)^{n/2} \binom{n}{n/2}. \end{aligned}$$

This implies that

$$W_{\mu_2}(\mathbf{1}_n) = (-1)^{n/2+1} \binom{n}{n/2} = (-1)^c \binom{n}{n/2}.$$

By the above discussion, we conclude that $W_{f_2}(\mathbf{0}_{n+1}) = 0$ and therefore $f_2 \in \mathcal{B}_{n+1}$ is a balanced SAC function. This completes the proof. □

4.2 Nonlinearity

Theorem 3. *Let f_2 be an (n+1)-variable Boolean function generated by Construction 2. Then we have $nl(f_2) = 2^n - \binom{n}{n/2}$.*

Proof. For any $\alpha = (\alpha', \alpha_{n+1}) \in \mathbb{F}_2^{n+1}$, we have

$$W_{f_2}(\alpha) = W_{\mu_2}(\alpha') + (-1)^{c+\alpha_{n+1}} W_{\mu_2}(\mathbf{1}_n + \alpha'). \qquad (3)$$

Then we have $|W_{f_2}(\alpha)| \leq 2|W_{\mu_2}(\alpha')|$ for every $\alpha = (\alpha', \alpha_{n+1}) \in \mathbb{F}_2^{n+1}$. By Lemma 3 we have $\max_{\alpha' \in \mathbb{F}_2^n} |W_{\mu_2}| = 2\binom{n-1}{n/2} = \binom{n}{n/2}$. Then we have $\max_{\alpha \in \mathbb{F}_2^{n+1}} |W_{f_2}(\alpha)| \leq 2\binom{n}{n/2}$. Furthermore, by (3) we can see that $W_{f_2}(\mathbf{0}_n, 1) = W_{\mu_2}(\mathbf{0}_n) - (-1)^c W_{\mu_2}(\mathbf{1}_n)$. Recall from the proof of Theorem 2 that $W_{\mu_2}(\mathbf{0}_n) = -\binom{n}{n/2}$ and $W_{\mu_2}(\mathbf{1}_n) = (-1)^c\binom{n}{n/2}$. Thus, we have $W_{f_2}(1, \mathbf{0}_n) = -2\binom{n}{n/2}$. So we have $\max_{\alpha \in \mathbb{F}_2^{n+1}} |W_{f_2}(\alpha)| = 2\binom{n}{n/2}$ and hence $nl(f_2) = 2^n - \binom{n}{n/2}$. □

4.3 Algebraic Immunity and Algebraic Degree

Lemma 6. *Let n be an even integer and f_0 be the majority function. Then $AI(f_0) = n/2$. Furthermore, f_0 has no nonzero annihilators of algebraic degrees strictly less that $n/2 + 1$.*

Proof. It suffices to prove that $f_0'(x_1, \cdots, x_n) = f_0(x_1 + 1, \cdots, x_n + 1)$ has no nonzero annihilator with algebraic degree less than $n/2 + 1$ since if there exists a nonzero function g of degree strictly less than $n/2+1$ such that $f_0' g = 0$ then we have $f_0 g' = 0$ where $g'(x_1, \cdots, x_n) = g(x_1 + 1, \cdots, x_n + 1)$.

Assume that g is an annihilator of f_0' with $\deg(g) \leq n/2$. Let the ANF of $g(x)$ be

$$g(x) = \bigoplus_{u \in \mathbb{F}_2^n, \mathrm{wt}(u) \leq n/2} a_u \Big(\prod_{j=1}^{n} x_j^{u_j} \Big).$$

Since g is an annihilator of f_0', $g(x) = 0$ for every $x \in W^{\leq n/2}$. Then we have $a_u = 0$ for any $u \in \mathbb{F}_2^n$ with $\mathrm{wt}(u) \leq n/2$ by (1). This implies that $g = 0$ and hence f_0' has no nonzero annihilator with algebraic degree less than $n/2 + 1$. □

Theorem 4. *Let f_2 be an $(n+1)$-variable Boolean function given by Construction 2, then f_2 has optimal algebraic immunity.*

Proof. It was shown that the Boolean function $\mu_2(x) + l(x)$ has optimal algebraic immunity (see Item C-1 of Theorem 12 in [15]). This implies that $\mu_2(x) + l(x)$ has no nonzero annihilators of degrees strictly less than $n/2$. Moreover, it is follows from Lemma 6 that $\mu_2(x)$ has no nonzero annihilators of degrees strictly less than $n/2 + 1$. Assume that $\min\{d \mid d = \deg(s), 0 \neq s \in AN(\mu_2(x) + l(x))\} = n/2$. By item 1) of Corollary 1, we have $AI(f_2) = n/2 + 1$. If $\min\{d \mid d = \deg(s), 0 \neq s \in AN(\mu_2(x) + l(x))\} \geq n/2 + 1$, then by item 2) of Corollary 1 we have $AI(f_2) \geq n/2 + 1$ and hence $AI(f_2) = n/2 + 1$ since the $AI(f_2)$ is upper-bounded by $n/2 + 1$. □

We shall give the algebraic degree of f_2.

Theorem 5. *Let f_2 be an $(n+1)$-variable Boolean function generated by Construction 2. Then we have $\deg(f_2) = 2^{\lfloor \log_2 n \rfloor}$.*

Proof. By Theorem 1, we have $\deg(f_2) = \deg(\mu_2)$. Further, we have $\deg(f_2) = \deg(\mu_2) = 2^{\lfloor \log_2 n \rfloor}$, according to Lemma 3. □

5. Conclusion

In this paper, we proposed an infinite class of Balanced SAC functions with optimal algebraic immunity in odd number of variables and determined the algebraic degree and nonlinearity of the functions in this class. This is the first time that such functions have been constructed. This work was an attempt to construct balanced SAC Boolean functions with all desired cryptographic criteria and it would be very interesting to construct balanced SAC Boolean functions with optimal algebraic immunity and higher nonlinearity.

Acknowledgments

We wish to thank the anonymous reviewers for their detailed comments that improved the editorial as well as technical quality of this paper. The first author is supported by the National Natural Science Foundation of China (grants 61602394 and 61872435) and Guangxi Key Laboratory of Cryptography and Information Security (No. GCIS201724).

References

[1] C. Carlet, "Boolean functions for cryptography and error correcting codes," Boolean Models and Methods in Mathematics, Computer Science, and Engineering, vol.2, pp.257–397, 2010.
[2] C. Ding, G. Xiao, and W. Shan, The Stability Theory of Stream Ciphers, Springer, 1991.
[3] D.K. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity," Des. Codes Cryptogr., vol.40, no.1, pp.41–58, 2006.
[4] N. Li and W.F. Qi, "Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity," Advances in Cryptology–ASIACRYPT 2006, pp.84–98, Springer, 2006.
[5] S. Sarkar and S. Maitra, "Construction of rotation symmetric Boolean functions on odd number of variables with maximum algebraic immunity," Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, pp.271–280, Springer, 2007.
[6] N. Li, L. Qu, W.F. Qi, G. Feng, C. Li, and D. Xie, "On the construction of Boolean functions with optimal algebraic immunity," IEEE Trans. Inf. Theory, vol.54, no.3, pp.1330–1334, 2008.
[7] C. Carlet and K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," Advances in Cryptology-ASIACRYPT 2008,

pp.425–440, Springer, 2008.
[8] C. Carlet, X. Zeng, C. Li, and L. Hu, "Further properties of several classes of Boolean functions with optimum algebraic immunity," Des. Codes Cryptogr., vol.52, no.3, pp.303–338, 2009.
[9] Z. Tu and Y. Deng, "A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity," Des. Codes Cryptogr., vol.60, no.1, pp.1–14, 2011.
[10] D. Dong, S. Fu, L. Qu, and C. Li, "A new construction of Boolean functions with maximum algebraic immunity," Information Security, pp.177–185, Springer, 2009.
[11] S. Fu, C. Li, K. Matsuura, and L. Qu, "Construction of rotation symmetric Boolean functions with maximum algebraic immunity," Cryptology and Network Security, pp.402–412, Springer, 2009.
[12] Q. Wang, J. Peng, H. Kan, and X. Xue, "Constructions of cryptographically significant Boolean functions using primitive polynomials," IEEE Trans. Inf. Theory, vol.56, no.6, pp.3048–3053, 2010.
[13] X. Zeng, C. Carlet, J. Shan, and L. Hu, "More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks," IEEE Trans. Inf. Theory, vol.57, no.9, pp.6310–6320, 2011.
[14] S. Fu, L. Qu, C. Li, and B. Sun, "Balanced rotation symmetric Boolean functions with maximum algebraic immunity," IET Inf. Secur., vol.5, no.2, pp.93–99, 2011.
[15] J. Peng, Q. Wu, and H. Kan, "On symmetric Boolean functions with high algebraic immunity on even number of variables," IEEE Trans. Inf. Theory, vol.57, no.10, pp.7205–7220, 2011.
[16] S. Su and X. Tang, "Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity," Des. Codes Cryptogr., vol.71, no.2, pp.183–199, 2014.
[17] H. Wang, J. Peng, Y. Li, and H. Kan, "On $2k$-variable symmetric Boolean functions with maximum algebraic immunity k," IEEE Trans. Inf. Theory, vol.58, no.8, pp.5612–5624, 2012.
[18] S. Su, X. Tang, and X. Zeng, "A systematic method of constructing Boolean functions with optimal algebraic immunity based on the generator matrix of the Reed–Muller code," Des. Codes Cryptogr., vol.72, no.3, pp.653–673, 2014.
[19] D. Tang, C. Carlet, and X. Tang, "Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks," IEEE Trans. Inf. Theory, vol.59, no.1, pp.653–664, 2013.
[20] W. Zhang and E. Pasalic, "Improving the lower bound on the maximum nonlinearity of 1-resilient Boolean functions and designing functions satisfying all cryptographic criteria," Inform. Sciences, vol.376, pp.21–30, 2017.
[21] A. Canteaut and M. Videau, "Symmetric Boolean functions," IEEE Trans. Inf. Theory, vol.51, no.8, pp.2791–2811, 2005.
[22] N.T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," Advances in Cryptology–EUROCRYPT 2003, pp.345–359, Springer, 2003.
[23] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," Advances in Cryptology-EUROCRYPT 2004, pp.474–491, Springer, 2004.
[24] A. Webster and S.E. Tavares, "On the design of S-boxes," Advances in Cryptology–CRYPTO 1985 Proceedings, pp.523–534, Springer, 1986.
[25] A.M. Youssef, T. Cusick, P. Stănică, and S.E. Tavares, "New bounds on the number of functions satisfying the strict avalanche criterion," Third Annual Workshop on Selected Areas in Cryptography, Citeseer, 1996.
[26] A. Canteaut, "Open problems related to algebraic attacks on stream ciphers," Coding and cryptography, pp.120–134, Springer, 2006.
[27] C. Carlet, D.K. Dalai, K.C. Gupta, and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction," IEEE Trans. Inf. Theory, vol.52, no.7, pp.3105–3121, 2006.
[28] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Elsevier, 1977.