On the Boolean functions With Maximum Possible Algebraic Immunity : Construction and A Lower Bound of the Count

Abstract. This paper gives a construction method which can get a large class of Boolean functions with maximum algebraic immunity(AI) from one such giving function. Our constructions get more functions than any previous construction. The cryptographic properties, such as balance, algebraic degree etc, of those functions are studied. It shows that we can construct Boolean functions with better cryptographic properties, which gives the guidance for the design of Boolean functions to resist algebraic attack, and helps to design good cryptographic primitives of cryptosystems. From these constructions, we show that the count of the Boolean functions with maximum AI is bigger than $2^{2^{n-1}}$ for n odd, bigger than $2^{2^{n-1}+\frac{1}{2}\binom{n}{\frac{n}{2}}}$ for n even, which confirms the computer simulation result that such boolean functions are numerous. As far as we know, this is the first bound about this count.

Key words: Algebraic Attack, Algebraic Degree, Algebraic Immunity, Annihilator, Balance, Boolean Functions, Nonlinearity

1 Introduction

Algebraic attack (that uses overdefined systems of multivariate equations to recover the secret key) has received a lot of attention recently [1, 2, 12, 13, 15–17, 23, 27] in studying security of the cryptosystems. This adds a new cryptographic property for designing Boolean functions to be used as building blocks in cryptosystems which is known as algebraic immunity(AI) [3–6, 8–11, 18–20, 26, 28].

Given an n-variable Boolean function f, different cases related to low degree multiples of f have been studied in [16, 27]. The main objective is to find out minimum (or low) degree annihilators of f and $1+f$, i.e, to find out minimum (or low) degree n-variable nonzero functions g such that $f*g=0$ and $(1+f)*g=0$. To mount the algebraic attack, one needs the low degree linearly independent annihilators [16, 27] of f and $1+f$.

W. Meier[27] points out that the algebraic immunity of a random balanced Boolean function with n variables is almost always at least equal to $0.22n$. C.Carlet[10], by heuristic indication and computer simulation, shows for a random balanced boolean function, it should have: for even n, AI is almost always equal to $\frac{n}{2}$; for odd n, AI is almost always greater than or equal to $\frac{n-1}{2}$. The algebraic immunities of power functions $tr(x^d)$ are considered in [10, 28], Y.Nawaz[28] give a upper bound of AI of any power functions.

Though there are increasing interest in construction of Boolean functions with good annihilator immunity [3–6, 9, 8, 18–20], So far there are only three known constructions [6, 9, 19, 20]([9]is an extension of [18, 19]) that can achieve maximum possible AI $\lceil \frac{n}{2} \rceil$, where n is the number of inputs to the function. But the constructed functions all lack certain cryptographic properties making them unsuitable to be used in a cryptosystem. A.Braeken[6] presents three classes of symmetric boolean functions on F_2^n with maximum AI for n even, and studies their properties. The heart of the construction in [19] was a function ϕ_{2k} on even $(2k)$ number of variables with maximum possible annihilator immunity k. The main problem with ϕ_{2k} is that no clear intuition has been provided how one can land into such a complicated structure. Further, the other cryptographic properties, such as weight, nonlinearity or algebraic degree of the function ϕ_{2k} are not very good and ϕ_{2k} are not balance[9, 19]. D. K. Dalai[20] first explains a generic construction idea of functions with maximum AI that comes from the basic theory, then studies the cryptographic properties of the constructions, such as nonlinearity, algebraic degree etc. Both the three papers have the same shortcoming, they construct too few such functions, D. K. Dalai[19] gets only one high dimension function from a low dimension function, D. K. Dalai[20] provides only symmetric functions with maximum possible AI, 1 for n odd and $2^{\binom{n}{\frac{n}{2}}}$ for n even, A.Braeken[6] provides also only symmetric boolean functions. Though the linear transformations on these functions can provide more such functions, but the linear transformations don't change the algebraic degree and nonlinearity, so they can't improve the cryptographic properties of these functions. As provide so few Boolean functions, they're not convenient for cryptographic use.

In this paper we give a construction method which can get a large class of Boolean functions with maximum AI from one such giving function. Our construction gets much more functions than any previous construction([6, 19, 20]). The cryptographic properties, such as balance, algebraic degree etc, of those functions are studied. It shows that we can construct Boolean functions with better cryptographic properties. As we provides more functions, it's more free to choose functions with better cryptographic properties. This gives the guidance for the design of Boolean functions to resist algebraic attack, and helps to design good cryptographic primitives of cryptosystems. By this construction, we can get a lower bound of the count of Boolean functions which have maximum AI. Though C.Carlet[10] indicates that boolean functions with maximum AI are numerous, but there is no theory result about it. As far as we know, what's we present in this paper is the first bound about this count.

The organization of the paper is as follows. In the following section we will give some preliminaries of the paper. In Section 3, we give a construction to get a large class of Boolean functions with maximum possible AI from one such giving function. Their cryptographic properties are studied in Section 4. In Section 5, we study the count of the Boolean functions with maximum possible AI and give a lower bound of that. Section 6 concludes the paper.

2 Preliminaries

A Boolean function on n variables may be viewed as a mapping from $V_n = \{0,1\}^n$ into $V_1 = \{0,1\}$ and define B_n as the set of all n-variable Boolean functions. One of the standard representation of a Boolean function $f(x_1, \cdots, x_n)$ is by the output column of its truth table, i.e., a binary string of length 2^n,

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

The set of $x \in V_n$ for which $f(x) = 1$ (respectively $f(x) = 0$) is called the on set (respectively off set), denoted by $S_1(f)$ (respectively $S_0(f)$). We say that a Boolean function f is balanced if the truth table contains an equal number of 1's and 0's. The Hamming weight of a binary string S is the number of ones in the string. This number is denoted by $wt(S)$. The Hamming distance between two strings, S_1 and S_2 is denoted by $d(S_1, S_2)$ and is the number of places where S_1 and S_2 differ. Note that $d(S_1, S_2) = wt(S_1 + S_2)$(by abuse of notation, we also use $+$ to denote the $GF(2)$ addition, i.e., the XOR).

Any Boolean function has a unique representation as a multivariate polynomial over $GF(2)$, called the algebraic normal form (ANF),

$$f(x_1, \cdots, x_n) = a_0 + \sum_{1 \leq i \leq n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{i,j} x_i x_j + \cdots + a_{12\cdots n} x_1 x_2 \cdots x_n$$

where the coefficients $a_0, a_i, a_{i,j}, \cdots, a_{12\cdots n} \in \{0,1\}$. The algebraic degree $deg(f)$, is the number of variables in the highest order term with nonzero coefficient. A Boolean function is affine if there exists no term of degree > 1 in the ANF and the set of all affine functions is denoted $A(n)$. An affine function with constant term equal to zero is called a linear function.

It is known that a Boolean function should be of high algebraic degree to be cryptographically secure [22]. Further, it has been identified recently, that it should not have a low degree multiple [16]. The algebraic attack (see [16, 27] and the references in these papers) is getting a lot of attention recently. To resist algebraic attacks, the Boolean functions used in the cryptosystems should be chosen properly.

Definition 1. *[20] 1. Given $f \in B_n$, a nonzero function $g \in B_n$ is called an annihilator of f if $f * g = 0$. By $AN(f)$ we mean the set of annihilators of f.*

2.Given $f \in B_n$, the AI of f, denoted by $AI(f) = deg(g)$, where $g \in B_n$ is the minimum degree nonzero function such that either $f * g = 0$ or $(1 + f) * g = 0$.

It is known [16, 27] that for $f \in B_n$, $AI(f) \leq \lceil \frac{n}{2} \rceil$and in [6, 9, 19, 20] constructions achieving the maximum value were presented. In this paper we will present how to get much more such functions from one such function.

In this paper, we use $\binom{n}{m}$ to note the binomial coefficients: choose m elements from n elements, use $|S|$ to note the number of the elements of a set S.

3 The construction of boolean functions with maximum possible AI

Let $f \in B_n$ and consider that f has an annihilator g of degree d. Let the ANF of $g = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1\le i<j\le n} a_{i,j} x_i x_j + \cdots + \sum_{1\le i_1<\cdots<i_d\le n} a_{i_1,\cdots,i_d} x_{i_1}\cdots x_{i_d}$. Note that $f(x) = 1$ implies $g(x) = 0$. So, we will be able to get linear equations from $g(x) = 0$ on the a's in ANF of g. That is we will get $wt(f)$ homogeneous linear equations on the a's. Solving the system of linear homogeneous equations, we can find out annihilators g of degree $\le d$ on nontrivial solutions. (In case of a trivial solution we will get all the a's equal to zero, i.e., $g(x) = 0$, which is not acceptable as we are interested in nonzero $g(x)$.) Here, we have $\sum_{i=0}^{d} \binom{n}{i}$ variables and $wt(f)$ equations. Let us denote the coefficient matrix of this system of equations by $S_1^d(f)$, then $S_1^d(f)$ has $wt(f)$ many rows and $\sum_{i=0}^{d} \binom{n}{i}$ many columns, and denote the $j(1 \le j \le wt(f))$ row vector of $S_1^d(f)$ as $\{u_j = (1, c_1, c_2, \cdots, c_n, c_{i_1}c_{i_2}, \cdots, c_{i_1}\cdots c_{i_d})\}$. Then u_js' dimensions are all $\sum_{i=0}^{d} \binom{n}{i}$. So $S_1^d(f)$ also can be seen as a vector set of u_j, that is $S_1^d(f) = \{(1, c_1, c_2, \cdots, c_n, c_{i_1}c_{i_2}, \cdots, c_{i_1}\cdots c_{i_d})|(c_1, c_2, \cdots, c_n) \in \{0,1\}^n, f(c_1, c_2, \cdots, c_n) = 1\}$. Note r as the rank of the matrix $S_1^d(f)$, it's also the rank of the vector set $S_1^d(f)$, then it should have $r \le min\{wt(f), \sum_{i=0}^{d} \binom{n}{i}\}$. Then we have:

Proposition 1. *f has no annihilator of degree $\le d$ if and only if $r = \sum_{i=0}^{d} \binom{n}{i}$.*

Let $f' = 1 + f$, we can get the vector set $S_0^d(f) = \{(1, a_1, a_2, \cdots, a_n, a_{i_1}a_{i_2}, \cdots, a_{i_1}\cdots a_{i_d})|(a_1, a_2, \cdots, a_n) \in \{0,1\}^n, f(a_1, a_2, \cdots, a_n) = 0\}$, which has $2^n - wt(f)$ vectors(each vector is $\sum_{i=0}^{d} \binom{n}{i}$ dimension). The rank of $S_0^d(f)$, $r' \le min\{2^n - wt(f), \sum_{i=0}^{d} \binom{n}{i}\}$.

Similarly, we have:

Proposition 2. *$f' = 1 + f$ has no annihilator of degree $\le d$ if and only if $r' = \sum_{i=0}^{d} \binom{n}{i}$.*

Note $d_0 = \lceil \frac{n}{2} \rceil$-1, $r_0 = \sum_{i=0}^{d_0} \binom{n}{i}$, $I = S_0^{d_0}(f) \cup S_1^{d_0}(f)$, then $I = \{(1, c_1, c_2, \cdots, c_n, c_{i_1}c_{i_2}, \cdots, c_{i_1}\cdots c_{i_{\lceil \frac{n}{2}\rceil -1}})|(c_1, c_2, \cdots, c_n) \in \{0,1\}^n\}$, and obviously I is a subset of $V_{r_0} = \{0,1\}^{r_0}$. Then from Proposition 1 and Proposition 2, we should have:

Proposition 3. *Let $f \in B_n$, then $AI_n(f) = \lceil \frac{n}{2} \rceil$ if and only if $r(S_0^{d_0}(f)) = r(S_1^{d_0}(f)) = r_0$.*

As $S_0^{d_0}(f) \cup S_1^{d_0}(f) = I$, $S_0^{d_0}(f) \cap S_1^{d_0}(f) = \emptyset$, the problem to construct a boolean function with maximum AI is the problem, as Proposition 3 shows, to cut I into two disjoint subsets whose ranks are both r_0; and the count of boolean functions with maximum AI, is the count of different cut methods of I.

Proposition 4. *[7] Let $f \in B_n$(n odd) be balanced function and it does not have any annihilator with algebraic degree $< \lceil \frac{n}{2} \rceil$. Then $1 + f$ has no annihilator with algebraic degree $< \lceil \frac{n}{2} \rceil$. Consequently, $AI_n(f) = \lceil \frac{n}{2} \rceil$.*

Proposition 5. *Let $f \in B_n$(n odd), then $AI_n(f) = \lceil \frac{n}{2} \rceil$ if and only if f is balanced and $r(S_1^{d_0}(f)) = 2^{n-1}$.*

Proof. When n is odd, $d_0 = \lceil \frac{n}{2} \rceil - 1 = \frac{n-1}{2}$, $r_0 = \sum_{i=0}^{d_0} \binom{n}{i} = 2^{n-1}$.

If $AI_n(f) = \lceil \frac{n}{2} \rceil$, f must to be balanced and $r(S_1^{d_0}(f)) = r(S_0^{d_0}(f)) = r_0 = 2^{n-1}$;

If $r(S_1^{d_0}(f)) = 2^{n-1}$, then f does not have any annihilator with algebraic degree $< \lceil \frac{n}{2} \rceil$; As f is balanced, then by the above proposition, we have $AI_n(f) = \lceil \frac{n}{2} \rceil$. □

So, when n is odd, the problem to construct a boolean function with maximum AI is the problem to choose 2^{n-1} distinct elements from I to form a r_0 rank subset; and the count of boolean functions with maximum AI, is the count of different choose methods of the subsets.

By the above observation, to construct a boolean function with maximum possible AI, we need to construct two bases of $F_2^{r_0}$. As the direct construction is too difficult, we can go from two initial bases to get new bases. From this thought, we have the following theorem.

Theorem 1. *If we have two bases of a vector space of dimension n, then for any i elements in the first base, there exist i elements in the second base such that if we interchange the i elements of the first base with those of the second one, we still have two bases.*

To prove this theorem, Let's first prove two lemmas.

Lemma 1. *The elementary collum transformations don't change the linear relations of matrix A's column vector groups, that is to say: the elementary column transformations change A's linear independent column vector groups to linear independent vector groups; and change A's linear dependent column vector groups to linear dependent vector groups.*

Proof. Let A is a $m \times n$ matrix, P is a n order reversible square matrix, so it need only to prove:

$AX = 0$ has nonzero solution $\Leftrightarrow$ $(AP)X = 0$ has nonzero solution.

This is true. Because, if $AX = 0$ has nonzero solution X_0, then $(AP)X = 0$ has nonzero solution $P^{-1}X_0$. If $(AP)X = 0$ has nonzero solution X_0, then $AX = 0$ has nonzero solution PX_0. □

Lemma 2. *Let A is a n order reversible square matrix, then any s columns(rows) $r_1, \cdots, r_s$ of A, among all the s order minor determinants of these s columns(resp. rows), there exists at least one nonzero s order minor determinants, and its corresponding residue minor determinants is also nonzero.*

Proof. Make the Laplace transformation on these columns $r_1, \cdots, r_s$, then

$$|A| = \Sigma_{j_1 \cdots j_s} D \begin{pmatrix} r_1 \cdots r_s \\ j_1 \cdots j_s \end{pmatrix} (-1)^{r_1 + \cdots + r_s + j_1 + \cdots + j_s} M \begin{pmatrix} r_1 \cdots r_s \\ j_1 \cdots j_s \end{pmatrix}$$

$\sum$ of above formula represents the sum of all different s rows(columns) $j_1 \cdots j_s$. From the above formula, it can easy seen that there exist at least one $j_1 \cdots j_s$ st.

$$D\begin{pmatrix} r_1 \cdots r_s \\ j_1 \cdots j_s \end{pmatrix} M \begin{pmatrix} r_1 \cdots r_s \\ j_1 \cdots j_s \end{pmatrix} \neq 0$$

□

Now we prove the theorem 1.

Proof. Let the two bases are $\alpha_1, \cdots, \alpha_n$ and $\beta_1, \cdots, \beta_n$, now set

$$A = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}, B = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$$

then A, B are all n order reversible square matrix, so there exist a reversible square matrix P, st. $AP = E$ is the element square matrix, note

$$B_1 = BP = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix}$$

then take any s rows from E, however we can assume these are the first s rows, then apply lemma 2 to B_1, take the last $n-s$ columns, then there exist $n-s$ rows $i_1, \cdots, i_{n-s}$, st.

$$D\begin{pmatrix} r_1 \cdots r_s \\ j_1 \cdots j_s \end{pmatrix} \neq 0, M \begin{pmatrix} r_1 \cdots r_s \\ j_1 \cdots j_s \end{pmatrix} \neq 0$$

So the first s rows of E and $i_1, \cdots, i_{n-s}$ rows of B_1 form a base, and the last $n-s$ rows of E and the rest s rows of B_1 also form a base.

Then from lemma 1, the first s rows of A and $i_1, \cdots, i_{n-s}$ rows of B form a base, and the rest rows of them also form a base. □

For convenience use nextly, we general Theorem 1 to two vector groups:

Theorem 2. *Let K be a field, $A = \{\alpha_1, \cdots, \alpha_s\}$, $B = \{\beta_1, \cdots, \beta_t\}$, $\alpha_j (1 \leq j \leq s), \beta_k (1 \leq k \leq t) \in K^n$, $s \geq t \geq n$, $r(A) = r(B) = n$, $1 \leq i \leq t$, then any i elements in B, there exist i elements in A st. if we exchange these elements with A and B, and we note the new sets as $A^{'}, B^{'}$, then $r(A^{'}) = r(B^{'}) = n$.*

Proof. For convenience, we assume the i elements in B is $\{\beta_1, \cdots, \beta_i\}$, and $r(\{\alpha_1, \cdots, \alpha_n\}) = n$.

Note $r^{'} = r(\{\beta_1, \cdots, \beta_i\})$, then $r^{'} \leq i$, now we take a maximum linear independent vector group from $\{\beta_1, \cdots, \beta_i\}$, assume they are $\{\beta_1, \cdots, \beta_{r^{'}}\}$, then we can extend them to a base of K^n. Now by Theorem 1, there exist $r^{'}$ elements in $\{\alpha_1, \cdots, \alpha_n\}$ such that we exchange these $r^{'}$ elements, we also have two bases of K^n.

For $\{\beta_{r^{'}+1}, \cdots, \beta_i\}$, we take any $i - r^{'}$ elements from $\{\alpha_{n+1}, \cdots, \alpha_s\}$, exchange them, this won't change the rank of each vector group. So we have $r(A^{'}) = r(B^{'}) = n$. □

Now we can use Theorem 1 and Theorem 2 to construct boolean functions with maximum AI:

Theorem 3. *Let $f \in B_n(n$ odd$)$, $AI_n(f) = \lceil \frac{n}{2} \rceil$. Let $S_0^{d_0}(f) = \{u_1, \cdots, u_{r_0}\}$, $S_1^{d_0}(f) = \{v_1, \cdots, v_{r_0}\}$, i is a fixed number and $1 \leq i \leq r_0$, $u_s = (1, a_1^s, a_2^s, \cdots, a_n^s, a_{i_1}^s a_{i_2}^s, \cdots, a_{i_1}^s \cdots a_{i_{d_0}}^s) \in S_0^{d_0}(f)$, $s = 1, \cdots, i$, for any i elements $v_s = (1, b_1^s, b_2^s, \cdots, b_n^s, b_{i_1}^s b_{i_2}^s, \cdots, b_{i_1}^s \cdots b_{i_{d_0}}^s) \in S_1^{d_0}(f)$, $s = 1, \cdots, i$. Let*

$$g_{(b_1^s, b_2^s, \cdots, b_n^s)}(x_1, x_2, \cdots, x_n)$$
$$= \begin{cases} f(x_1, x_2, \cdots, x_n) + 1, & (x_1, x_2, \cdots, x_n) = (a_1^s, a_2^s, \cdots, a_n^s), (b_1^s, b_2^s, \cdots, b_n^s), s = 1, \cdots, i \\ f(x_1, x_2, \cdots, x_n), & \text{else} \end{cases}$$

then there exist at least one $g_{(b_1^s, b_2^s, \cdots, b_n^s)}(x_1, x_2, \cdots, x_n)$ such that $AI_n(g) = \lceil \frac{n}{2} \rceil$.

Proof. By Proposition 3 and Theorem 1, It's easy to come to this conclusion. □

Theorem 4. *Let $f \in B_n(n$ even$)$, $AI_n(f) = \lceil \frac{n}{2} \rceil$. Let $S_0^{d_0}(f) = \{u_1, \cdots, u_k\}$, $S_1^{d_0}(f) = \{v_1, \cdots, v_l\}$, and assume $k \geq l$. i is a fixed number and $1 \leq i \leq l$, $u_s = (1, a_1^s, a_2^s, \cdots, a_n^s, a_{i_1}^s a_{i_2}^s, \cdots, a_{i_1}^s \cdots a_{i_{d_0}}^s) \in S_0^{d_0}(f)$, $s = 1, \cdots, i$, for any i elements $v_s = (1, b_1^s, b_2^s, \cdots, b_n^s, b_{i_1}^s b_{i_2}^s, \cdots, b_{i_1}^s \cdots b_{i_{d_0}}^s) \in S_1^{d_0}(f)$, $s = 1, \cdots, i$. Let*

$$g_{(b_1^s, b_2^s, \cdots, b_n^s)}(x_1, x_2, \cdots, x_n)$$
$$= \begin{cases} f(x_1, x_2, \cdots, x_n) + 1, & (x_1, x_2, \cdots, x_n) = (a_1^s, a_2^s, \cdots, a_n^s), (b_1^s, b_2^s, \cdots, b_n^s), s = 1, \cdots, i \\ f(x_1, x_2, \cdots, x_n), & \text{else} \end{cases}$$

then there exist at least one $g_{(b_1^s, b_2^s, \cdots, b_n^s)}(x_1, x_2, \cdots, x_n)$ such that $AI_n(g) = \lceil \frac{n}{2} \rceil$.

Proof. By Proposition 3 and Theorem 2, It's easy to come to this conclusion. □

Construction 1 *Let $f \in B_n(n$ odd$)$, $AI_n(f) = \lceil \frac{n}{2} \rceil$. Let $S_0^{d_0}(f) = \{u_1, \cdots, u_{r_0}\}$, $S_1^{d_0}(f) = \{v_1, \cdots, v_{r_0}\}$, i is a fixed number and $1 \leq i \leq r_0$, $u_s = (1, a_1^s, a_2^s, \cdots, a_n^s, a_{i_1}^s a_{i_2}^s, \cdots, a_{i_1}^s \cdots a_{i_{d_0}}^s) \in S_0^{d_0}(f)$, $s = 1, \cdots, i$, Then there exist i elements $v^s = (1, b_1^s, b_2^s, \cdots, b_n^s, b_{i_1}^s b_{i_2}^s, \cdots, b_{i_1}^s \cdots b_{i_{d_0}}^s) \in S_1^{d_0}(f)$, $s = 1, \cdots, i$. Let*

$$g_{(b_1^s, b_2^s, \cdots, b_n^s)}(x_1, x_2, \cdots, x_n)$$
$$= \begin{cases} f(x_1, x_2, \cdots, x_n) + 1, & (x_1, x_2, \cdots, x_n) = (a_1^s, a_2^s, \cdots, a_n^s), (b_1^s, b_2^s, \cdots, b_n^s), s = 1, \cdots, i \\ f(x_1, x_2, \cdots, x_n), & \text{else} \end{cases}$$

then $AI_n(g) = \lceil \frac{n}{2} \rceil$.

Construction 2 *Let $f \in B_n(n$ even$)$, $AI_n(f) = \lceil \frac{n}{2} \rceil$. Let $S_0^{d_0}(f) = \{u_1, \cdots, u_s\}$, $S_1^{d_0}(f) = \{v_1, \cdots, v_t\}$, and assume $s \geq t$. i is a fixed number and $1 \leq i \leq t$, $u_s = (1, a_1^s, a_2^s, \cdots, a_n^s, a_{i_1}^s a_{i_2}^s, \cdots, a_{i_1}^s \cdots a_{i_{d_0}}^s) \in S_0^{d_0}(f)$, $s = 1, \cdots, i$, then there exist* *i elements* $v^s = (1, b_1^s, b_2^s, \cdots, b_n^s, b_{i_1}^s b_{i_2}^s, \cdots, b_{i_1}^s \cdots b_{i_{d_0}}^s) \in S_1^{d_0}(f)$, $s = 1, \cdots, i$. *Let*

$$g_{(b_1^s, b_2^s, \cdots, b_n^s)}(x_1, x_2, \cdots, x_n)$$

$$= \begin{cases} f(x_1, x_2, \cdots, x_n) + 1, & (x_1, x_2, \cdots, x_n) {=} (a_1^s, a_2^s, \cdots, a_n^s), (b_1^s, b_2^s, \cdots, b_n^s), s = 1, \cdots, i \\ f(x_1, x_2, \cdots, x_n), & \quad\quad\quad\quad\quad\quad\quad\quad \textit{else} \end{cases}$$

then $AI_n(g) = \lceil \frac{n}{2} \rceil$.

The constructions in [6, 20] provides only symmetric boolean functions, and [20] provides only one Boolean function with maximum AI when n is odd, and $2^{\binom{n}{\frac{n}{2}}}$ Boolean functions with maximum AI when n is even. The construction in [19] can provide only one high dimension maximum AI Boolean function from a low dimension maximum AI Boolean function, this number is very small. Our constructions can provide much more functions than any former construction. And among these functions, we can use various methods to find some that have good cryptographic properties, which is good for cryptographic use.

4 Balance and Algebraic Degree of Our Constructions

This part we will discuss the cryptographic properties of the Boolean functions which we constructed in last section.

Construction 1 and Construction 2 both interchange i elements of $S_1(f)$ with i elements of $S_0(f)$, so they both keep the weight of the function, thus surely keep the balance.

Now we discuss the algebraic degrees of our constructed boolean functions. Since we inverse $2i$ values of f, it can be seen as to add a weight $2i$ boolean function to f. Now let's note $\triangle_t(x_1, \cdots, x_n) \in B_n$ a boolean function with t, we discuss it's algebraic degree.

First let's show a lemma.

Lemma 3. *[24] Let* $f \in B_n$, $deg(f) = d$, *then* $2^{n-d} \leq wt(f) \leq 2^n - 2^{n-d}$.

Proposition 6. *Let* $\triangle_2(x_1, \cdots, x_n) \in B_n$, $wt(\triangle_2(x_1, \cdots, x_n)) = 2$, *then* $deg(\triangle_2(x_1, \cdots, x_n)) = n - 1$.

Proof. Let $\triangle_2(x_1, \cdots, x_n)$ is 1 at point $(a_1, \cdots, a_n)$ and $(b_1, \cdots, b_n)$, then

$$\begin{aligned} \triangle_2(x_1, \cdots, x_n) &= (x_1 + a_1 + 1) \cdots (x_n + a_n + 1) + (x_1 + b_1 + 1) \cdots (x_n + b_n + 1) \\ &= \textstyle\sum_{i=1}^n (a_i + b_i) \prod_{j=1, j \neq i}^n x_j + \cdots \end{aligned}$$

Because a_i can't all equal to b_i, then at least one $\prod_{j=1, j \neq i}^n x_j$ is exist, thus we have $deg(\triangle_2(x_1, \cdots, x_n)) = n - 1$. □

Then for the functions we constructed by Construction 1,2, when $i = 1$, that's we only change two elements of f, then we should have:

1. If $deg(f) < n-1$, then $deg(g) = n-1$;
2. If $deg(f) = n$, then $deg(g) = n$;
3. If $deg(f) = n-1$, then $deg(g) \leq n-1$;

If f is balance, then $deg(f) \leq n-1$, then we can always construct new functions with maximum algebraic degree for balance functions. So as we can see, in most instances, new functions by our constructions can have better algebraic agrees than the initial functions.

Proposition 7. *Let $\triangle_4(x_1,\cdots,x_n) \in B_n$, $wt(\triangle_4(x_1,\cdots,x_n)) = 4$, then $n-2 \leq deg(\triangle_4(x_1,\cdots,x_n)) \leq n-1$.*

Proof. First it should have $deg(\triangle_4(x_1,\cdots,x_n)) \leq n-1$ as $wt(\triangle_4(x_1,\cdots,x_n))$ is even. Then by Lemma 3, we should have $deg(\triangle_4(x_1,\cdots,x_n)) \geq n-2$. This comes to the result. □

Generally, we can have:

Proposition 8. *Let $\triangle_{2i}(x_1,\cdots,x_n) \in B_n$, $wt(\triangle_{2i}(x_1,\cdots,x_n)) = 2i$, then $n-1-\lfloor log_2 i \rfloor \leq deg(\triangle_{2i}(x_1,\cdots,x_n)) \leq n-1$.*

Proof. Similarly it should have $deg(\triangle_{2i}(x_1,\cdots,x_n)) \leq n-1$ as $wt(\triangle_{2i}(x_1,\cdots,x_n))$ is even. Then by Lemma 3, we should have $2i \geq 2^{n-deg(\triangle_{2i}(x_1,\cdots,x_n))}$, so $deg(\triangle_{2i}(x_1,\cdots,x_n)) \geq n-1-\lfloor log_2 i \rfloor$. This comes to the result. □

Then for the functions we constructed by Construction 1,2, we should have:

1. If $deg(f) < n-1-\lfloor log_2 i \rfloor$, then $deg(g) \geq n-1-\lfloor log_2 i \rfloor$;
2. If $deg(f) = n$, then $deg(g) = n$;
3. If $n-1-\lfloor log_2 i \rfloor \leq deg(f) \leq n-1$, then $deg(g) \leq n-1$;

For the functions constructed by construction 3 in Dalai[20],their algebraic degree are $2^{\lfloor log_2 n \rfloor}$. And Dalai[20] showed that linear transformation can provide more boolean functions with maximum AI, but linear transformation don't change the algebraic degree.

Let $t = \lfloor log_2 n \rfloor$, then for a function g we constructed in Construction 1:

1. If $n > 2^t + 1 + \lfloor log_2 i \rfloor$, then $deg(g) \geq n-1-\lfloor log_2 i \rfloor > 2^t = deg(f)$;
2. If $n = 2^t$, then $deg(g) = n = 2^t = deg(f)$;
3. If $2^t + 1 + \lfloor log_2 i \rfloor \geq n \geq 2^t + 1$, then $deg(g) \leq n-1$;

As we can see, in most instances, new functions by our constructions have better algebraic agree than the functions in Dalai[20]. If the initial function have a good algebraic degree, as we constructed a large class of functions, among them there must have some functions which have as high algebraic degree as the initial function. As in most instances, the degree of the initial Boolean function is changed, so they are not the linear transformation of the initial function. Thus we provide many more functions than Dalai[20], and in most instances, we get many functions with higher algebraic degree.

If we have a boolean function with maximum AI, but we don't be satisfied with it's other cryptographic properties, by our construction, we can get a large class of functions with maximum AI from this function, among which we can choose them freely, according to different cryptographic properties. So our constructions give the guidance for the design of Boolean functions to resist algebraic attack, and help to design good cryptographic primitives of cryptosystems.

5 An lower bound of the number of the Boolean functions with maximum AI

By our construction, and by Dalai[20] Construction 2, we can get an lower bound of the count of the Boolean functions that have the maximum AI. As far as we know, this is the first bound about this count.

First we show the Construction by Dalai[20]:

Construction 3 *[20] Let $f \in B_n$,*

1. If n is odd then

$$f(x_1, \cdots, x_n) = \begin{cases} 0, & \text{for } wt(x_1, \cdots, x_n) \leq \lceil \frac{n}{2} \rceil \\ 1, & \text{for } wt(x_1, \cdots, x_n) \geq \lceil \frac{n}{2} \rceil \end{cases}$$

2. If n is even then

$$f(x_1, \cdots, x_n) = \begin{cases} 0, & \text{for } wt(x_1, \cdots, x_n) < \lceil \frac{n}{2} \rceil \\ 1, & \text{for } wt(x_1, \cdots, x_n) > \lceil \frac{n}{2} \rceil \\ b \in \{0, 1\}, & \text{for } wt(x_1, \cdots, x_n) = \frac{n}{2} \end{cases}$$

Theorem 5. *Note $S_n = \{f \in B_n | AI_n(f) = \lceil \frac{n}{2} \rceil\}$,*

1. If n is odd then

$$|S_n| \geq 2^{2^{n-1}},$$

2. If n is even then

$$|S_n| \geq 2^{2^{n-1}+\frac{1}{2}\binom{n}{\frac{n}{2}}}.$$

Proof. Use our constructions on Dalai[16]'s Construction:

1. For n is odd, there is only one function in Dalai's construction, note it as f_0. For f_0, use our construction 1, for $1 \leq i \leq r_0$ we change i elements with $S_0(f)$ and $S_1(f)$, they are all distinct, total we will have $2^{r_0} = 2^{2^{n-1}}$ distinct functions, so we will have $|S_n| \geq 2^{2^{n-1}}$;

2. For n is even, consider a function f_1 from Dalai's Construction,

$$f_1(x_1, \cdots, x_n) = \begin{cases} 0, & \text{for } wt(x_1, \cdots, x_n) < \lceil \frac{n}{2} \rceil \\ 1, & \text{for } wt(x_1, \cdots, x_n) \geq \lceil \frac{n}{2} \rceil \end{cases}$$

As $AI(f_1) = \lceil \frac{n}{2} \rceil$, then by Proposition 3, we know $S_0^{d_0}(f_1) = \{(1, x_1, \cdots, x_n, x_{i_1}x_{i_2}, \cdots, x_{i_1} \cdots x_{i_{d_0}}) | wt(x_1, \cdots, x_n) < \lceil \frac{n}{2} \rceil\}$ forms a base of the vector space $F_2^{r_0}$. And by the function f_2 from Dalai's Construction,

$$f_2(x_1, \cdots, x_n) = \begin{cases} 0, & \text{for } wt(x_1, \cdots, x_n) \leq \lceil \frac{n}{2} \rceil \\ 1, & \text{for } wt(x_1, \cdots, x_n) > \lceil \frac{n}{2} \rceil \end{cases}$$

Similarly we have $S_1^{d_0}(f_2) = \{(1, x_1, \cdots, x_n, x_{i_1}x_{i_2}, \cdots, x_{i_1}\cdots x_{i_{d_0}})|wt(x_1, \cdots, x_n) > \lceil\frac{n}{2}\rceil\}$ also forms a base of the vector space $F_2^{r_0}$.

Now let f_t be any function from Dalai's construction, then by Theorem 2, for any i, $1 \leq i \leq r_0$, any i elements of $\{(x_1, \cdots, x_n)|wt(x_1, \cdots, x_n) < \lceil\frac{n}{2}\rceil\}$, there exist i elements of $\{(x_1, \cdots, x_n)|wt(x_1, \cdots, x_n) > \lceil\frac{n}{2}\rceil\}$, such that exchange these elements, we still have two bases, so we still have $AI(f_t^{'}) = \lceil\frac{n}{2}\rceil$. Then for any $\{(x_1, \cdots, x_n)|wt(x_1, \cdots, x_n) = \lceil\frac{n}{2}\rceil\}$, fix them to a value 0 or 1, this step we have $2^{(\binom{n}{\frac{n}{2}})}$ choice methods. Next for any choice, we still have $2^{r_0} = 2^{2^{n-1}-\frac{1}{2}\binom{n}{\frac{n}{2}}}$ distinct functions, together we will have $2^{2^{n-1}+\frac{1}{2}\binom{n}{\frac{n}{2}}}$ distinct functions. So $|S_n| \geq 2^{2^{n-1}+\frac{1}{2}\binom{n}{\frac{n}{2}}}$. □

In view of cryptography, the balanced Boolean functions are most important Boolean functions. A.Canteaut pointed in [7] that determining the proportion of the balanced Boolean functions of n variables with optimal algebraic immunity is still an open problem. Now we show a first result about this open problem.

Theorem 6. *Note* $T_n = \{f \in B_n|AI_n(f) = \lceil\frac{n}{2}\rceil, wt(f) = 2^{n-1}\}$,

1. If n is odd then

$$|T_n| \geq 2^{2^{n-1}},$$

2. If n is even then

$$|T_n| \geq \binom{\binom{n}{\frac{n}{2}}}{\frac{1}{2}\binom{n}{\frac{n}{2}}} 2^{2^{n-1}-\frac{1}{2}\binom{n}{\frac{n}{2}}}.$$

Proof. Use our constructions on Dalai[16]'s Construction:

1. For n is odd, as every function with maximum AI must to be balance, so the conclusion is convenient;

2. For n is even, for any $\{(x_1, \cdots, x_n)|wt(x_1, \cdots, x_n) = \lceil\frac{n}{2}\rceil\}$, fix half of them to the value 0, and fix the other half to the value 1, this step we have $\binom{\binom{n}{\frac{n}{2}}}{\frac{1}{2}\binom{n}{\frac{n}{2}}}$ choice methods. Next for any choice, we still have $2^{r_0} = 2^{2^{n-1}-\frac{1}{2}\binom{n}{\frac{n}{2}}}$ distinct functions, together we will have $\binom{\binom{n}{\frac{n}{2}}}{\frac{1}{2}\binom{n}{\frac{n}{2}}}2^{2^{n-1}-\frac{1}{2}\binom{n}{\frac{n}{2}}}$ distinct functions. So $|T_n| \geq \binom{\binom{n}{\frac{n}{2}}}{\frac{1}{2}\binom{n}{\frac{n}{2}}}2^{2^{n-1}-\frac{1}{2}\binom{n}{\frac{n}{2}}}$. Thus prove the theorem. □

6 Conclusion

In this paper we give a construction method which can get a class of Boolean functions with maximum AI from one such giving function. Our constructions get more functions than any previous construction. The cryptographic properties, such as balance, algebraic degree etc, of those functions are studied. It shows that we can construct Boolean functions with better cryptographic properties, which gives the guidance for the design of Boolean functions to resist algebraic attack, and helps to design good cryptographic primitives of cryptosystems. From the construction, we get a lower bound of the count of Boolean functions which have maximum AI. As far as we know, this is the first bound about this count.

References

1. F. Armknecht. Improving Fast Algebraic Attacks. In FSE 2004, number 3017 in Lecture Notes in Computer Science, pages 65-82. Springer Verlag, 2004.
2. L. M. Batten. Algebraic Attacks over GF(q). In Progress in Cryptology - INDOCRYPT2004, pages 84-91, number 3348, Lecture Notes in Computer Science, Springer-Verlag.
3. A. Botev. On algebraic immunity of some recursively given sequence of correlation immune functions. In Proceedings of XV international workshop on Synthesis and complexisty of control systems, Novosibirsk, October 18-23, 2004, pages 8-12 (in Russian).
4. A. Botev. On algebraic immunity of new constructions of filters with high nonlinearity. In Proceedings of VI international conference on Discrete models in the theory of control systems, Moscow, December 7-11, 2004, pages 227-230 (in Russian).
5. A. Botev and Y. Tarannikov. Lower bounds on algebraic immunity for recursive constructions of nonlinear filters. Preprint 2004.
6. A. Braeken and B. Preneel, On the algebraic immunity of symmetric boolean functions, To appear in Indocrypt 2005.
7. A. Canteaut. Open problems related to algebraic attacks on stream ciphers. In WCC 2005, pages 1-10, invited talk.
8. C. Carlet. Improving the algebraic immunity of resilient and nonlinear functions and constructing bent functions. IACR ePrint server, http://eprint.iacr.org, 2004/276.
9. C. Carlet, D. K. Dalai, K. C. Gupta and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. Preprint.
10. C. Carlet and P. Gaborit. On the construction of balanced Boolean functions with a good algebraic immunity. Proceedings of International Symposium on Information Theory 2005. To appear.
11. C. Carlet. On Bent and Highly Nonlinear Balanced/Resilient Functions and Their Algebraic Immunities, In AAECC2006, number 3857 in Lecture Notes in Computer Science, pages 1-28. Springer Verlag, 2006.
12. J. H. Cheon and D. H. Lee. Resistance of S-boxes against Algebraic Attacks. In FSE2004, number 3017 in Lecture Notes in Computer Science, pages 83-94. Springer Verlag, 2004.
13. J. Y. Cho and J. Pieprzyk. Algebraic Attacks on SOBER-t32 and SOBER-128. In FSE2004, number 3017 in Lecture Notes in Computer Science, pages 49-64. Springer Verlag,2004.
14. G. M. Constantine. Combinatorial Theory and Statistical Design. John Wiley Sons,1987.
15. N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In Advances in Cryptology - ASIACRYPT 2002, number 2501 in Lecture Notes in Computer Science, pages 267-287. Springer Verlag, 2002.
16. N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. In Advances in Cryptology - EUROCRYPT 2003, number 2656 in Lecture Notes in Computer Science, pages 345-359. Springer Verlag, 2003.

17. N. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In Advances in Cryptology - CRYPTO 2003, number 2729 in Lecture Notes in Computer Science, pages 176-194. Springer Verlag, 2003.
18. D. K. Dalai, K. C. Gupta and S. Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. In INDOCRYPT 2004, pages 92-106, number 3348, Lecture Notes in Computer Science, Springer-Verlag.
19. D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity. In FSE 2005. To be published in Lecture Notes in Computer Science, Springer-Verlag.
20. D. K. Dalai, S. Maitra and S. Sarkar. Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity. Cryptology ePrint Archive, http://eprint.iacr.org/, No. 2005/229, 15 July, 2005. To be published in Designs, Codes and Cryptography
21. J. F. Dillon. Elementary Hadamard Difference sets. PhD Thesis, University of Maryland,1974.
22. C. Ding, G. Xiao, and W. Shan. The Stability Theory of Stream Ciphers. Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.
23. D. H. Lee, J. Kim, J. Hong, J. W. Han and D. Moon. Algebraic Attacks on Summation Generators. In FSE 2004, number 3017 in Lecture Notes in Computer Science, pages34-48. Springer Verlag, 2004.
24. F. J. MacWillams and N. J. A. Sloane. The Theory of Error Correcting Codes. NorthHolland, 1977.
25. S. Maitra. Boolean functions with important cryptographic properties. PhD Thesis,Indian Statistical Institute, 2000.
26. S. Maitra and P. Sarkar. Maximum Nonlinearity of Symmetric Boolean Functions on Odd Number of Variables. IEEE Transactions on Information Theory, 48(9):2626-2630,September 2002.
27. W. Meier, E. Pasalic and C. Carlet. Algebraic attacks and decomposition of Boolean functions. In Advances in Cryptology - EUROCRYPT 2004, number 3027 in LectureNotes in Computer Science, pages 474-491. Springer Verlag, 2004.
28. Y.Nawaz, G.Gong, and K.Gupta. Upper Bounds on Algebraic Immunity of Power Functions. In FSE 2006. To be published in Lecture Notes in Computer Science, Springer-Verlag.