

# Constructing Symmetric Boolean Functions with Maximum Algebraic Immunity

Keqin Feng, Feng Liu, Longjiang Qu, Lei Wang

**Abstract**—Symmetric Boolean functions with even variables  $2k$  and maximum algebraic immunity  $AI(f) = k$  have been constructed in A. Braeken's thesis [3]. In this correspondence we show more constructions of such Boolean functions including the generalization of a result in [3] and prove a conjecture raised in [3].

**Index Term:** Symmetric Boolean functions, algebraic immunity.

## I. INTRODUCTION

In recent years algebraic attack has become an important method in cryptographic analyzing stream and block cipher systems, see [1, 2, 6, 7, 8]. A new cryptographic property for designing Boolean functions to resist this kind of attack, called algebraic immunity, has been introduced and studied in [3, 4, 5, 9, 10, 11, 12].

Let  $B_n$  and  $SB_n$  be the rings of the Boolean functions and the symmetric Boolean functions respectively with  $n$  variables  $x_1, x_2, \dots, x_n$ . For  $f \in B_n$ , the algebraic immunity of  $f$ , denoted by  $AI(f)$ , is defined to be the smallest degree of non-zero  $g \in B_n$  such that  $fg = 0$  or  $(1+f)g = 0$ . It is proved in [8, 11] that  $AI(f) \leq \lceil n/2 \rceil$  for all  $f \in B_n$ . One of the interesting problems is to determine the Boolean functions with maximum algebraic immunity. In this paper, we present some symmetric Boolean functions with maximum  $AI$ .

A symmetric Boolean function  $f \in SB_n$  can be characterized by a vector

$$v_f = (v_f(0), v_f(1), \dots, v_f(n)) \in F_2^{n+1}$$

where  $v_f(i) = f(x)$  for  $x \in F_2^n$  with Hamming weight  $w(x) = i$ . It is proved in [12] that for odd  $n = 2k+1 \geq 3$ , there are only two symmetric Boolean functions  $f$  and  $1+f$  in  $SB_n$  with maximal  $AI(= k+1)$  where  $v_f = (\underbrace{1, 1, \dots, 1}_{k+1}, \underbrace{0, 0, \dots, 0}_{k+1})$ .

On the other hand, there exists plenty of symmetric Boolean functions  $f \in SB_n$  with maximum  $AI(f) = k$  when  $n = 2k$  is even. At first we have the following general fact which

K.Q. Feng, F. Liu are with the Department of Mathematics, Tsinghua University, Beijing, 100084, P.R. China (e-mails: kfeng@math.tsinghua.edu.cn; lgsat@163.com). The work of K.Feng was supported by the National Science Research Program of China(NO.2004 CB 3180004) and the State Key Lab. on Information Security(SKLOIS) of China.

L.J. Qu is with the Department of Mathematics and System Science, Science College, National University of Defence Technology, ChangSha, 410073, and National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, P.R.China. (e-mail:ljqu\_happy@hotmail.com) The work of L.J. Qu was supported by the Natural Science Foundation of China(NO.60573028, 60803156) and the open research fund of National Mobile Communications Research Laboratory of Southeast University(W200807).

L. Wang is with the Department of Mathematics, Georgia Tech. USA(e-mail:wanglei07@gmail.com).

says that the algebraic immunity is an invariant under affine transformations.

*Lemma 1.1:* Let  $f, f' \in B_n$  be Boolean functions with  $n$  variables  $x = (x_1, \dots, x_n)$ ,  $f'(x) = f(xA + c)$ , where  $c \in F_2^n$  and  $A$  is an invertible  $n \times n$  matrix over  $F_2$ . Then  $AI(f) = AI(f')$ .

For  $n = 2k$ , there are four affine transformations in  $SB_n$ :

$$\begin{aligned} (x_1, \dots, x_n) &\mapsto (x_1, \dots, x_n); \\ (x_1, \dots, x_n) &\mapsto (x_1 + \sigma_1, \dots, x_n + \sigma_1); \\ (x_1, \dots, x_n) &\mapsto (x_1 + 1, \dots, x_n + 1); \\ (x_1, \dots, x_n) &\mapsto (x_1 + \sigma_1 + 1, \dots, x_n + \sigma_1 + 1). \end{aligned}$$

where  $\sigma_1 = x_1 + \dots + x_n$ . Thus we have the following result:

*Lemma 1.2:* Let  $f \in SB_n$ ,  $n = 2k$ , and

$$\begin{aligned} f_1(x_1, \dots, x_n) &= f(x_1 + 1, \dots, x_n + 1); \\ f_2(x_1, \dots, x_n) &= f(x_1 + \sigma_1, \dots, x_n + \sigma_1); \\ f_3(x_1, \dots, x_n) &= f(x_1 + \sigma_1 + 1, \dots, x_n + \sigma_1 + 1). \end{aligned}$$

Then  $f_1, f_2, f_3 \in SB_n$ ,  $AI(f_1) = AI(f_2) = AI(f_3) = AI(f)$ , and for each  $0 \leq i \leq n$ , we have:

$$\begin{aligned} v_{f_1}(i) &= v_f(n - i); \\ v_{f_3}(n - i) &= v_{f_2}(i) = \begin{cases} v_f(i), & \text{if } 2|i \\ v_f(n - i), & \text{if } 2 \nmid i \end{cases} \quad \square \end{aligned}$$

Also, for each  $f \in SB_n$ , we have  $1+f \in SB_n$  and  $AI(1+f) = AI(f)$ . Since  $v_f(i) = v_{1+f}(i) + 1$  ( $0 \leq i \leq n$ ), from now on we may assume that  $v_f(0) = 1$ .

In A. Braeken's thesis [3](also see [4]) the following symmetric Boolean functions with maximum algebraic immunity have been constructed.

*Lemma 1.3:* Let  $n = 2k \geq 4$  and  $f \in SB_n$ . We denote  $s_{k-i} = e_{k-i} + e_{k+i}$  where  $e_j$  ( $0 \leq j \leq n$ ) is a vector in  $F_2^{n+1}$  such that its  $j^{\text{th}}$  position is 1 and the other positions are 0. Then  $AI(f) = k$  under one of the following conditions:

- (1) ([3]Theorem4.1.30)  $v_f = (\underbrace{11\dots1}_k \underbrace{a00\dots0}_k)$ ,  $a \in F_2$ ;
- (2) ([3]Theorem4.1.31)  $v_f = (\underbrace{11\dots1}_k \underbrace{00\dots01}_k)$ ;
- (3) ([3]Theorem4.1.32)  $v_f = (\underbrace{11\dots1}_{k+1} \underbrace{00\dots0}_k) + s_{k-4}$   
and  $4 \leq k \leq 11$ ;
- (4) ([3]Theorem4.1.33)  $v_f = (\underbrace{11\dots1}_{k+1} \underbrace{00\dots0}_k) + s_0$

$$\text{and } \binom{2k}{k} \equiv 2 \pmod{4}.$$

**Remark:** It is well-known that for each positive integer  $m$  and  $a \geq 0$  satisfying  $2^a | m!$  and  $2^{a+1} \nmid m!$ , we have  $a = \sum_{i \geq 1} \lfloor \frac{m}{2^i} \rfloor$ .

From this fact and  $\binom{2k}{k} = \frac{(2k)!}{k!k!}$ , we can see that the condition that  $\binom{2k}{k} \equiv 2 \pmod{4}$  in Lemma 1.3(4) is equivalent to  $k = 2^l$  for some  $l \geq 0$ .

Based on computation, A. Braeken raised the following conjecture in [3]:

*Conjecture 1.4:* Let  $f \in SB_n$ ,  $n = 2k \geq 4$ ,  $1 \leq i \leq \lfloor k/2 \rfloor$ . If  $\binom{k+t-i}{t} \equiv 1 \pmod{2}$  for all  $t$ ,  $1 \leq t \leq i$ , and

$$v_f = \underbrace{(11\dots 100\dots 0)}_k + e_{n-i}$$

then  $AI(f) = k$ .

In the next section we will present more symmetric Boolean functions  $f \in SB_{2k}$  with maximum  $AI(f) (= k)$ . Particularly we generalize Lemma 1.3(3) and prove Conjecture 1.4. It is not hard to see that our approach in next section can be used to prove all results in Lemma 1.3 in an uniform way.

## II. RESULTS AND PROOFS

Firstly we introduce a combinatorial result given by Wilson [13] which we need to prove our results.

For each  $i$ ,  $0 \leq i \leq n$ , we define

$$T_i = \{a \in F_2^n | w(a) = i\}$$

where  $w(a)$  is the Hamming weight of  $a$ . For  $a = (a_1, \dots, a_n)$ ,  $b = (b_1, \dots, b_n)$  and  $d = (d_1, \dots, d_n) \in F_2^n$ , we define

$$\begin{aligned} a \preceq b &\Leftrightarrow a_i \leq b_i, \quad (1 \leq i \leq n) \\ a \prec b &\Leftrightarrow a \preceq b \text{ and } a \neq b \\ d = a \vee b &\Leftrightarrow d_i = \max\{a_i, b_i\}, \quad (1 \leq i \leq n) \end{aligned}$$

*Lemma 2.1:* (Wilson[13]) Suppose that  $i \leq \min\{j, n-j\}$  and  $M = (m_{ba})_{a \in T_i, b \in T_j}$  be the  $\binom{n}{j} \times \binom{n}{i}$  matrix over  $F_2$  where

$$m_{ba} = \begin{cases} 1, & \text{if } a \preceq b \\ 0, & \text{otherwise} \end{cases}$$

Then the  $F_2$  rank of  $M$  is

$$\text{rank}(M) = \sum_{0 \leq t \leq i, \binom{j-t}{i-t} \equiv 1 \pmod{2}} \left[ \binom{n}{t} - \binom{n}{t-1} \right]$$

where we assume  $\binom{n}{-1} = 0$ . Particularly,  $\text{rank}(M) = \binom{n}{i}$  if and only if  $\binom{j-t}{i-t} \equiv 1 \pmod{2}$  for all  $t$ ,  $0 \leq t \leq i$ .  $\square$

To determine the value of  $\binom{n}{k} \pmod{2}$ , Lucas formula is a powerful tool. Let

$$n = \sum_{j=0}^l n_j 2^j, k = \sum_{j=0}^l k_j 2^j, (n_j, k_j \in \{0, 1\})$$

$k \preceq n$  means that for all  $j$  ( $0 \leq j \leq l$ ),  $k_j \leq n_j$ . Then Lucas formula says

$$\begin{aligned} \binom{n}{k} &\equiv \binom{n_0}{k_0} \binom{n_1}{k_1} \cdots \binom{n_l}{k_l} \pmod{2} \\ &\equiv \begin{cases} 1 \pmod{2}, & \text{if } k \preceq n \\ 0 \pmod{2}, & \text{otherwise} \end{cases} \end{aligned}$$

Each Boolean function  $g(x) = g(x_1, \dots, x_n) \in B_n$  can be expressed by

$$g(x) = \sum_{a \in F_2^n} c_g(a) x^a \quad (c_g(a) \in F_2)$$

where for  $a = (a_1, \dots, a_n) \in F_2^n$ ,  $x^a$  is defined as  $x^a = x_1^{a_1} \cdots x_n^{a_n}$ . If we assume  $0^0 = 1$ , then for any  $b = (b_1, \dots, b_n) \in F_2^n$ , we have  $a \preceq b \Leftrightarrow b^a = 1$ . Therefore

$$g(b) = \sum_{a \in F_2^n, a \preceq b} c_g(a)$$

For  $f, g \in B_n$ ,  $fg = 0$  if and only if for each  $a \in F_2^n$ ,  $f(a) = 1 \Rightarrow g(a) = 0$ . If  $f \in SB_n$ , then  $fg = 0$  if and only if for each  $i$ , ( $0 \leq i \leq n$ ),  $v_f(i) = 1 \Rightarrow g(a) = 0$  for all  $a \in T_i$ .

After these preliminary observations, we show our first result which is a generalization of Lemma 1.3(3).

*Theorem 2.2:* Let  $f \in SB_n$ ,  $n = 2k \geq 4$  such that  $2^i \leq k \leq 3 \cdot 2^i - 1$  for some  $i \geq 0$ . If  $v_f = \underbrace{(11\dots 1)}_k \alpha \underbrace{00\dots 0}_k + s_{k-2^i}$

( $\alpha \in F_2$ ), then  $AI(f) = k$ .

**Proof:** Suppose that  $fg = 0$  for some  $g \in B_n$  and  $\deg(g) \leq k-1$ , so we have that

$$g(x) = \sum_{a \in F_2^n, w(a) \leq k-1} c(a) x^a$$

From  $fg = 0$  we know that  $g(b) = 0$  for all  $b \in F_2^n$  such that

$$w(b) \in \{0, \dots, k-2^i-1, k-2^i+1, \dots, k-1, k+2^i\}$$

We need to show  $g = 0$ .

Firstly we claim that  $c(a) = 0$  for all  $a \in F_2^n$  such that  $w(a) \leq k-2^i-1$ . We prove this claim by induction on  $w(a)$ . From  $0 = g(0) = c(0)$  we know that  $c(a) = 0$  for  $w(a) = 0$ . Assume that for some  $l < k-2^i-1$  we have  $c(a) = 0$  for all  $a \in F_2^n$  such that  $w(a) \leq l$ . Now consider  $b \in F_2^n$  with  $w(b) = l+1$ . Because  $l+1 \leq k-2^i-1$ , we have  $g(b) = 0$ , then we have

$$0 = g(b) = \sum_{w(a) \leq k-1, a \preceq b} c(a) = c(b) + \sum_{w(a) \leq l, a \prec b} c(a) = c(b)$$

This completes the proof of the claim. Therefore

$$g(x) = \sum_{k-2^i \leq w(a) \leq k-1} c(a) x^a$$

Next we claim that for all  $b \in F_2^n$  such that  $k-2^i+1 \leq w(b) \leq k-1$ ,

$$c(b) = \sum_{w(a)=k-2^i, a \prec b} c(a) \quad (1)$$

We also prove this claim by induction on  $w(b)$ . If  $w(b) = k-2^i+1$ , then

$$\begin{aligned} 0 = g(b) &= \sum_{k-2^i \leq w(a) \leq k-1, a \preceq b} c(a) \\ &= c(b) + \sum_{w(a)=k-2^i, a \prec b} c(a) \end{aligned}$$

therefore  $c(b) = \sum_{w(a)=k-2^i, a \prec b} c(a)$ , so the claim is true for  $w(b) = k - 2^i + 1$ . Suppose  $k - 2^i + 1 \leq l < k - 1$  and the claim is true for all  $b \in F_2^n$  such that  $k - 2^i + 1 \leq w(b) \leq l$ . Now let  $w(b) = l + 1$ . Then

$$0 = g(b) = c(b) + \sum_{k-2^i \leq w(a) \leq l, a \prec b} c(a)$$

Therefore

$$c(b) = \sum_{w(a)=k-2^i, a \prec b} c(a) + \sum_{k-2^i+1 \leq w(a) \leq l, a \prec b} c(a)$$

and by induction hypothesis,

$$\begin{aligned} & \sum_{k-2^i+1 \leq w(a) \leq l, a \prec b} c(a) \\ &= \sum_{k-2^i+1 \leq w(a) \leq l, a \prec b} \sum_{w(a')=k-2^i, a' \prec a} c(a') \\ &= \sum_{w(a')=k-2^i, a' \prec b} c(a') \sum_{a: a' \prec a \prec b} 1 \\ &= \sum_{w(a')=k-2^i, a' \prec b} c(a') (2^{w(b)-w(a')} - 2) \equiv 0 \pmod{2} \end{aligned}$$

Therefore  $c(b) = \sum_{w(a)=k-2^i, a \prec b} c(a)$ . This completes the proof of the claim.

At last, for  $w(b) = k + 2^i$ , we have similarly

$$\begin{aligned} 0 &= g(b) = \sum_{k-2^i \leq w(a) \leq k-1, a \prec b} c(a) \\ &= \sum_{k-2^i \leq w(a) \leq k-1, a \prec b} \sum_{w(a')=k-2^i, a' \prec a} c(a') \\ &= \sum_{w(a')=k-2^i, a' \prec b} c(a') \sum_{k-2^i \leq w(a) \leq k-1, a' \prec a \prec b} 1 \end{aligned}$$

and

$$\begin{aligned} & \sum_{k-2^i \leq w(a) \leq k-1, a' \prec a \prec b} 1 \\ &= \sum_{\lambda=0}^{k-1-w(a')} \binom{w(b)-w(a')}{\lambda} = \sum_{\lambda=0}^{2^i-1} \binom{2^i+1}{\lambda} \\ &= 2^{2^i+1} - \frac{1}{2} \binom{2^i+1}{2^i} \equiv 1 \pmod{2} \end{aligned}$$

Therefore for all  $b \in F_2^n$  such that  $w(b) = k + 2^i$ ,

$$\sum_{w(a)=k-2^i, a \prec b} c(a) = 0, \quad (2)$$

which are  $\binom{2k}{k+2^i} = \binom{2k}{k-2^i}$  homogenous linear equations with  $\binom{2k}{k-2^i}$  variables  $\{c(a) | a \in F_2^n, w(a) = k - 2^i\}$ . The coefficient matrix is

$$M = (m_{ba})_{w(a)=k-2^i, w(b)=k+2^i}$$

where

$$m_{ba} = \begin{cases} 1, & \text{if } a \prec b \\ 0, & \text{otherwise} \end{cases}$$

Let  $l = k - 2^i$ , then  $0 \leq l < 2^{i+1}$ . For any  $t$  such that  $0 \leq t \leq l$ , we have  $0 \leq l - t \leq l < 2^{i+1}$  and

$$\binom{k+2^i-t}{k-2^i-t} = \binom{2^{i+1}+l-t}{2^{i+1}} \equiv 1 \pmod{2}$$

Then by Lemma 2.1 we know  $M$  is full rank and the linear equations (2) has only zero-solution:  $c(a) = 0$  for all  $a \in F_2^n$ ,  $w(a) = k - 2^i$ . Thus  $g = 0$  since all coefficients of  $g$  are zero by (1).

If  $(1+f)g = 0$  for some  $g \in B_n$ ,  $\deg(g) \leq k-1$ , consider

$$\begin{aligned} f'(x_1, \dots, x_n) &= f(x_1 + 1, \dots, x_n + 1) + 1, \\ g'(x_1, \dots, x_n) &= g(x_1 + 1, \dots, x_n + 1) \end{aligned}$$

Then  $f'g' = 0$ ,  $g' \in B_n$ ,  $\deg(g') = \deg(g) \leq k-1$ ,  $f' \in SB_n$  and

$$v_{f'} = (\underbrace{11\dots 1}_k(\alpha+1)\underbrace{00\dots 0}_k) + s_{k-2^i}$$

By the proof above we get  $g' = 0$  so that  $g = 0$ . In summary, we have  $AI(f) = k$ .  $\square$

Next result is a proof of Conjecture 1.4.

**Theorem 2.3:** Let  $n = 2k \geq 4$ ,  $l \geq 1$ ,  $k = 2^l \cdot s + i$  for some  $s \geq 0$  and  $1 \leq i \leq 2^l - 1$ . Then for  $f \in SB_n$  with  $v_f = (\underbrace{11\dots 1}_k \underbrace{00\dots 0}_{k+1}) + e_{2k-i}$ , we have  $AI(f) = k$ .

**Remark:** It is easy to see by Lucas formula that the condition  $k = 2^l \cdot s + i$ ,  $1 \leq i \leq 2^l - 1$  in this theorem is equivalent to the condition  $\binom{k+t-i}{t} \equiv 1 \pmod{2}$  for  $1 \leq t \leq i$  in the Conjecture 1.4.

**Proof of Theorem 2.3:** If  $s = 0$ , then  $k = i$  and by Lemma 1.3(1) we know  $AI(f) = k$ . From now on we can assume  $s \geq 1$ .

Suppose that  $fg = 0$  where  $g \in B_n$  and  $\deg(g) \leq k-1$ . From  $v_f(i) = 1$  for  $0 \leq i \leq k-1$ , we know that  $g(a) = 0$  for all  $a \in F_2^n$  such that  $w(a) \leq k-1$ . Then we can show that all coefficients  $c(a)$  in  $g(x) = \sum_{w(a) \leq k-1} c(a)x^a$  are zero by the same argument in the proof of Theorem 2.2. Therefore  $g = 0$ .

Next we suppose that  $(1+f)g = 0$  where  $g \in B_n$  and  $\deg(g) \leq k-1$ . Consider

$$\begin{aligned} f'(x_1, \dots, x_n) &= f(x_1 + 1, \dots, x_n + 1) + 1, \\ g'(x_1, \dots, x_n) &= g(x_1 + 1, \dots, x_n + 1) \end{aligned}$$

Then  $f'g' = 0$ ,  $\deg(g') \leq k-1$ , so we can write  $g'$  as  $g'(x) = \sum_{w(a) \leq k-1} c(a)x^a$  and  $f' \in SB_n$  with  $v_{f'} = (\underbrace{11\dots 1}_{k+1} \underbrace{00\dots 0}_k) + e_i$ .

By similar argument in the proof of Theorem 2.2, we can show that:

- (1)  $c(a) = 0$ , when  $w(a) \leq i-1$ ;
- (2)  $c(b) = \sum_{w(a)=i, a \prec b} c(a)$ , when  $i+1 \leq w(b) \leq k-1$ ;
- (3)  $\sum_{w(a)=i, a \prec b} c(a) = 0$ , when  $w(b) = k$

Condition (3) presents  $\binom{2k}{k}$  homogenous equations over  $F_2$  with  $\binom{2k}{i}$  variables  $\{c(a) | a \in F_2^n, w(a) = i\}$  with coefficient

matrix  $M = (m_{ba})_{w(b)=k, w(a)=i}$ , where

$$m_{ba} = \begin{cases} 1, & \text{if } a \prec b \\ 0, & \text{otherwise} \end{cases}$$

From the assumption  $k = 2^l \cdot s + i$  and  $1 \leq i \leq 2^l - 1$ , we know that for  $0 \leq t \leq i$ ,

$$\begin{aligned} \binom{k-t}{i-t} &= \binom{k-t}{k-i} = \binom{2^l \cdot s + (i-t)}{2^l \cdot s} \\ &\equiv \binom{i-t}{0} \equiv 1 \pmod{2} \end{aligned}$$

As  $\min\{k, 2k-k\} = k > i$ , so by Lemma 2.1, the rank of  $M$  over  $F_2$  is  $\binom{2k}{i}$ , so that  $c(a) = 0$  for all  $a \in F_2^n$  such that  $w(a) = i$ . Then we have  $g' = 0$  and  $g = 0$ . This completes the proof of  $AI(f) = k$ .  $\square$

At the end of this paper, we present a new construction of symmetric Boolean functions  $f \in SB_{2k}$  with maximum algebraic immunity.

**Theorem 2.4:** Let  $n = 2k$  with  $4 \cdot 2^s \leq k < 5 \cdot 2^s$  for some  $s \geq 0$ . For the function  $f \in SB_n$  defined by

$$v_f = (\underbrace{11\dots 1}_k \underbrace{a00\dots 0}_k) + s_{k-3 \cdot 2^s} + s_{k-2^s} \quad (a \in F_2)$$

we have  $AI(f) = k$ .

**Proof:** For  $s = 0$ , we have  $k = 4$ . It can be verified directly that this theorem is true for  $s = 0$ . So from now on we assume  $s \geq 1$ . Let  $k = 2^{s+2} + d$ , then  $0 \leq d < 2^s$ .

Suppose that  $fg = 0$  for some  $g \in B_n$  such that  $\deg(g) \leq k-1$ . We will show that  $g = 0$  no matter  $a = 0$  or  $1$ . Let

$$g(x) = \sum_{w(a) \leq k-1} c(a)x^a$$

Firstly, we can prove the following two results by similar arguments used in the proof of Theorem 2.2:

- (1) For  $0 \leq w(a) < k - 3 \cdot 2^s$ , we have  $c(a) = 0$ ;
- (2) For  $k - 3 \cdot 2^s < w(a) < k - 2^s$ , we have

$$c(a) = \sum_{w(\beta)=k-3 \cdot 2^s, \beta \prec a} c(\beta)$$

Now we claim that

- (3) For  $k - 2^s < w(a) \leq k - 1$ ,  $c(a) = \sum_{w(\beta)=k-2^s, \beta \prec a} c(\beta)$ .

In fact, for  $w(a) = k - 2^s + 1$ , we have  $f(a) = 1$ , so that

$0 = g(a) = \sum_{\beta \prec a} c(\beta)$ . Therefore

$$\begin{aligned} c(a) &= \sum_{\substack{k-3 \cdot 2^s \leq w(\beta) \leq k-2^s \\ \beta \prec a}} c(\beta) \\ &= \sum_{\substack{w(\beta)=k-3 \cdot 2^s \text{ or } k-2^s \\ \beta \prec a}} c(\beta) + \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \beta \prec a}} c(\beta) \\ &= \sum_{\substack{w(\beta)=k-3 \cdot 2^s \text{ or } k-2^s \\ \beta \prec a}} c(\beta) \\ &\quad + \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \beta \prec a}} \sum_{\substack{w(\gamma)=k-3 \cdot 2^s \\ \gamma \prec \beta}} c(\gamma) \\ &= \sum_{\substack{w(\beta)=k-3 \cdot 2^s \text{ or } k-2^s \\ \beta \prec a}} c(\beta) \\ &\quad + \sum_{\substack{w(\gamma)=k-3 \cdot 2^s \\ \gamma \prec a}} c(\gamma) \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \gamma \prec \beta \prec a}} 1 \end{aligned}$$

But

$$\begin{aligned} &\sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \gamma \prec \beta \prec a}} 1 \\ &= \sum_{i=k-3 \cdot 2^s+1}^{k-2^s-1} \binom{w(a) - w(\gamma)}{i - w(\gamma)} = \sum_{j=1}^{2^{s+1}-1} \binom{2^{s+1}+1}{j} \\ &= 2^{2^{s+1}+1} - 1 - 1 - (2^{s+1}+1) \equiv 1 \pmod{2} \end{aligned}$$

Therefore  $c(a) = \sum_{\substack{w(\beta)=k-2^s \\ \beta \prec a}} c(\beta)$  for  $w(a) = k - 2^s + 1$ .

Now we assume that for some  $l \leq k - 1$ , Claim (3) is true for all  $a$  such that  $k - 2^s + 1 \leq w(a) \leq l - 1$ . If  $w(a) = l$ , then

$$\begin{aligned} c(a) &= \sum_{\substack{k-3 \cdot 2^s \leq w(\beta) \leq l-1 \\ \beta \prec a}} c(\beta) \\ &= \sum_{\substack{w(\beta)=k-3 \cdot 2^s \text{ or } k-2^s \\ \beta \prec a}} c(\beta) + A + B \end{aligned}$$

where

$$A = \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \beta \prec a}} c(\beta), \quad B = \sum_{\substack{k-2^s < w(\beta) \leq l-1 \\ \beta \prec a}} c(\beta)$$

By Claim (2) we have

$$\begin{aligned} A &= \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \beta \prec a}} \sum_{\substack{w(\gamma)=k-3 \cdot 2^s \\ \gamma \prec \beta}} c(\gamma) \\ &= \sum_{\substack{w(\gamma)=k-3 \cdot 2^s \\ \gamma \prec a}} c(\gamma) \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \gamma \prec \beta \prec a}} 1 \end{aligned}$$

Because

$$\begin{aligned} \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \gamma \prec \beta \prec a}} 1 &= \sum_{i=k-3 \cdot 2^s+1}^{k-2^s-1} \binom{w(a) - w(\gamma)}{i - w(\gamma)} \\ &= \sum_{j=1}^{2^{s+1}-1} \binom{l - k + 3 \cdot 2^s}{j} \end{aligned}$$

and  $k-2^s+1 \leq l \leq k-2$ , we have  $2^{s+1}+1 \leq l-k+3 \cdot 2^s \leq 2^{s+1}+2^s-2$ . By Lucas formula

$$\begin{aligned} & \sum_{j=1}^{2^{s+1}-1} \binom{l-k+3 \cdot 2^s}{j} \\ \equiv & 1 + \sum_{j=0}^{2^{s+1}-1} \binom{l-k+3 \cdot 2^s - 2^{s+1}}{j} \\ \equiv & 1 + \sum_{j=0}^{2^{s+1}-1} \binom{l-k+2^s}{j} \equiv 1 \pmod{2} \end{aligned}$$

Therefore we have  $A = \sum_{\substack{w(\gamma)=k-3 \cdot 2^s \\ \gamma < a}} c(\gamma)$ .

On the other hand, by assumption, we have

$$\begin{aligned} B &= \sum_{\substack{k-2^s < w(\beta) \leq l-1 \\ \beta < a}} \sum_{\substack{w(\gamma)=k-2^s \\ \gamma < \beta}} c(\gamma) \\ &= \sum_{\substack{w(\gamma)=k-2^s \\ \gamma < a}} c(\gamma) \sum_{\substack{k-2^s < w(\beta) \leq l-1 \\ \gamma < \beta < a}} 1 \\ &= \sum_{\substack{w(\gamma)=k-2^s \\ \gamma < a}} c(\gamma) (2^{w(a)-w(\gamma)} - 2) \equiv 0 \pmod{2} \end{aligned}$$

Thus, Claim (3) is true for  $w(a) = l$ .

Now we claim that

(4) For  $w(a) = k+2^s$  and  $w(a) = k+3 \cdot 2^s$  we have

$$\sum_{\substack{w(\beta)=k-3 \cdot 2^s \\ \beta < a}} c(\beta) + \sum_{\substack{w(\beta)=k-2^s \\ \beta < a}} c(\beta) = 0$$

Assume that  $w(a) = k+2^s$ . From  $f(a) = 1$  we know that

$$\begin{aligned} 0 = g(a) &= \sum_{\substack{k-3 \cdot 2^s < w(\beta) \leq k-1 \\ \beta < a}} c(\beta) \\ &= \sum_{\substack{w(\beta)=k-3 \cdot 2^s, \text{ or } k-2^s \\ \beta < a}} c(\beta) + A + B \end{aligned}$$

where

$$\begin{aligned} A &= \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \beta < a}} c(\beta) \\ &= \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \beta < a}} \sum_{\substack{w(\gamma)=k-3 \cdot 2^s \\ \gamma < \beta}} c(\gamma) \\ &= \sum_{\substack{w(\gamma)=k-3 \cdot 2^s \\ \gamma < a}} c(\gamma) \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \gamma < \beta < a}} 1 \end{aligned}$$

By Lucas formula we can compute

$$\begin{aligned} \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \gamma < \beta < a}} 1 &= \sum_{i=k-3 \cdot 2^s+1}^{k-2^s-1} \binom{w(a)-w(\gamma)}{i-w(\gamma)} \\ &= \sum_{j=1}^{2^{s+1}-1} \binom{2^{s+2}}{j} \equiv 0 \pmod{2} \end{aligned}$$

Therefore  $A = 0$ . Similarly,

$$\begin{aligned} B &= \sum_{\substack{k-2^s < w(\beta) \leq k-1 \\ \beta < a}} c(\beta) = \sum_{\substack{k-2^s < w(\beta) \leq k-1 \\ \beta < a}} \sum_{\substack{w(\gamma)=k-2^s \\ \gamma < \beta}} c(\gamma) \\ &= \sum_{\substack{w(\gamma)=k-2^s \\ \gamma < a}} c(\gamma) \sum_{\substack{k-2^s < w(\beta) \leq k-1 \\ \gamma < \beta < a}} 1 \\ &= \sum_{\substack{w(\gamma)=k-2^s \\ \gamma < a}} c(\gamma) \sum_{j=1}^{2^s-1} \binom{2^{s+1}}{j} \equiv 0 \pmod{2} \end{aligned}$$

Therefore we know that Claim (4) is true for  $w(a) = k+2^s$ .

Now we assume that  $w(a) = k+3 \cdot 2^s$ . From  $f(a) = 1$  we know that

$$\begin{aligned} 0 = g(a) &= \sum_{\substack{k-3 \cdot 2^s \leq w(\beta) \leq k-1 \\ \beta < a}} c(\beta) \\ &= \sum_{\substack{w(\beta)=k-3 \cdot 2^s, \text{ or } k-2^s \\ \beta < a}} c(\beta) + A + B \end{aligned}$$

where

$$\begin{aligned} A &= \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \beta < a}} c(\beta) \\ &= \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \beta < a}} \sum_{\substack{w(\gamma)=k-3 \cdot 2^s \\ \gamma < \beta}} c(\gamma) \\ &= \sum_{\substack{w(\gamma)=k-3 \cdot 2^s \\ \gamma < a}} c(\gamma) \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \gamma < \beta < a}} 1 \end{aligned}$$

By Lucas formula we can compute

$$\begin{aligned} \sum_{\substack{k-3 \cdot 2^s < w(\beta) < k-2^s \\ \gamma < \beta < a}} 1 &= \sum_{i=k-3 \cdot 2^s+1}^{k-2^s-1} \binom{w(a)-w(\gamma)}{i-w(\gamma)} \\ &= \sum_{j=1}^{2^{s+1}-1} \binom{3 \cdot 2^{s+1}}{j} \equiv \sum_{j=1}^{2^{s+1}-1} \binom{3 \cdot 2^{s+1} - 2^{s+1}}{j} \\ &\equiv \sum_{j=1}^{2^{s+1}-1} \binom{2^{s+2}}{j} \equiv 0 \pmod{2} \end{aligned}$$

Therefore  $A = 0$ . Similarly,

$$\begin{aligned} B &= \sum_{\substack{k-2^s < w(\beta) \leq k-1 \\ \beta < a}} c(\beta) = \sum_{\substack{k-2^s < w(\beta) \leq k-1 \\ \beta < a}} \sum_{\substack{w(\gamma)=k-2^s \\ \gamma < \beta}} c(\gamma) \\ &= \sum_{\substack{w(\gamma)=k-2^s \\ \gamma < a}} c(\gamma) \sum_{\substack{k-2^s < w(\beta) \leq k-1 \\ \gamma < \beta < a}} 1 \\ &= \sum_{\substack{w(\gamma)=k-2^s \\ \gamma < a}} c(\gamma) \sum_{j=1}^{2^s-1} \binom{2^{s+2}}{j} = 0 \end{aligned}$$

Therefore  $B = 0$  and we know that Claim (4) is also true for  $w(a) = k+3 \cdot 2^s$ .

Recall that  $T_i$  is the set of  $a \in F_2^m$  with Hamming weight  $i$ . Then Claim (4) provides  $N = \binom{2k}{k+3 \cdot 2^s} + \binom{2k}{k+2^s}$  homogenous linear equations over  $F_2$  for  $\binom{2k}{k-3 \cdot 2^s} + \binom{2k}{k-2^s} = N$  variables  $\{c(\beta) \mid \beta \in T_{k-3 \cdot 2^s} \cup T_{k-2^s}\}$ . The coefficient matrix is

$$M = (m_{a,\beta})_{\substack{a \in T_{k+2^s} \cup T_{k+3 \cdot 2^s} \\ \beta \in T_{k-2^s} \cup T_{k-3 \cdot 2^s}}}$$

where

$$m_{a,\beta} = \begin{cases} 1, & \text{if } \beta \prec a \\ 0, & \text{otherwise} \end{cases}$$

We need to show that  $\det(M) = 1 \in F_2$ . Namely,  $M$  is an invertible matrix over  $F_2$ . For doing this we denote by  $M^T$  the transpose of the matrix  $M$  and consider

$$M^T M = (n_{\beta,\beta'}) = \begin{pmatrix} X & Y \\ Y^T & Z \end{pmatrix}$$

where  $X$  is a  $\binom{2k}{k-2^s} \times \binom{2k}{k-2^s}$  matrix and  $Z$  is a  $\binom{2k}{k-3 \cdot 2^s} \times \binom{2k}{k-3 \cdot 2^s}$  matrix. It is easy to see that

$$\begin{aligned} n_{\beta,\beta'} &= \sum_a m_{a,\beta} m_{a,\beta'} \\ &= \#\{a \in T_{k+2^s} \cup T_{k+3 \cdot 2^s} \mid \beta \prec a, \beta' \prec a\} \end{aligned}$$

We claim that

$$(5) \quad Z = 0, \quad X = I_{\binom{2k}{k-2^s}}, \quad Y Y^T = I_{\binom{2k}{k-3 \cdot 2^s}}.$$

Let  $Z = (z_{\beta,\beta'})$ ,  $Y = (y_{\beta,\beta'})$ ,  $X = (x_{\beta,\beta'})$ . Then

$$\begin{aligned} z_{\beta,\beta'} &= \#\{a \in F_2^n \mid w(a) = k + 2^s \text{ or } k + 3 \cdot 2^s, \\ &\quad \beta \prec a, \beta' \prec a\} \end{aligned}$$

for  $\beta = (\beta_1, \dots, \beta_n)$ ,  $\beta' = (\beta'_1, \dots, \beta'_n) \in T_{k-3 \cdot 2^s}$ .

By the definition of  $\beta \vee \beta'$ , we know that

$$\beta \prec a, \beta' \prec a \Leftrightarrow (\beta \vee \beta') \prec a$$

and  $w(\beta \vee \beta') = k - 3 \cdot 2^s + \lambda$ ,  $0 \leq \lambda \leq k - 3 \cdot 2^s = 2^s + d$ . Therefore

$$\begin{aligned} z_{\beta,\beta'} &= \binom{2k - (k - 3 \cdot 2^s + \lambda)}{k + 2^s - (k - 3 \cdot 2^s + \lambda)} \\ &\quad + \binom{2k - (k - 3 \cdot 2^s + \lambda)}{k + 3 \cdot 2^s - (k - 3 \cdot 2^s + \lambda)} \\ &= \binom{k + 3 \cdot 2^s - \lambda}{k - 2^s} + \binom{k + 3 \cdot 2^s - \lambda}{k - 3 \cdot 2^s} \\ &= \binom{2^{s+2} + 2^{s+1} + 2^s + d - \lambda}{2^{s+1} + 2^s + d} \\ &\quad + \binom{2^{s+2} + 2^{s+1} + 2^s + d - \lambda}{2^s + d} \end{aligned}$$

From  $0 \leq \lambda \leq 2^s + d$ , we know  $0 \leq 2^s + d - \lambda < 2^{s+1}$ . Thus by Lucas formula one can get

$$z_{\beta,\beta'} \equiv \binom{2^s + d - \lambda}{2^s + d} + \binom{2^s + d - \lambda}{2^s + d} \equiv 0 \pmod{2}$$

which means  $z_{\beta,\beta'} = 0$  for all  $\beta, \beta' \in T_{k-3 \cdot 2^s}$ . Thus we get  $Z = 0$ .

Next we prove  $X = I_{\binom{2k}{k-2^s}}$ . For  $\beta, \beta' \in T_{k-2^s}$  we have  $w(\beta \vee \beta') = k - 2^s + \lambda$ ,  $0 \leq \lambda \leq k - 2^s = 2^{s+1} + 2^s + d$ . Therefore

$$\begin{aligned} x_{\beta,\beta'} &= \binom{2k - (k - 2^s + \lambda)}{k + 2^s - (k - 2^s + \lambda)} \\ &\quad + \binom{2k - (k - 2^s + \lambda)}{k + 3 \cdot 2^s - (k - 2^s + \lambda)} \\ &= \binom{k + 2^s - \lambda}{k - 2^s} + \binom{k + 2^s - \lambda}{k - 3 \cdot 2^s} \\ &= \binom{2^{s+2} + 2^s + d - \lambda}{2^{s+1} + 2^s + d} + \binom{2^{s+2} + 2^s + d - \lambda}{2^s + d} \end{aligned}$$

Then

$$\begin{aligned} &\binom{2^{s+2} + 2^s + d - \lambda}{2^{s+1} + 2^s + d} \equiv 1 \pmod{2} \\ \Leftrightarrow &2^{s+2} + 2^s + d - \lambda = 2^{s+1} + 2^s + b \\ &\quad \text{for some } b, b \geq d, 0 \leq b < 2^s \\ \Leftrightarrow &\lambda = 2^{s+1} + d - b \quad (b \geq d, 0 \leq b < 2^s) \end{aligned}$$

Moreover,

$$\begin{aligned} &\binom{2^{s+2} + 2^s + d - \lambda}{2^s + d} \equiv 1 \pmod{2} \\ \Leftrightarrow &2^{s+2} + 2^s + d - \lambda \in \{2^{s+2} + 2^s + d, 2^{s+1} + 2^s + b, \\ &\quad 2^s + b\} \text{ for some } b, b \geq d, 0 \leq b < 2^s \\ \Leftrightarrow &\lambda \in \{0, 2^{s+1} + d - b, 2^{s+2} + d - b\} \\ \Leftrightarrow &\lambda \in \{0, 2^{s+1} + d - b\} \text{ (Since } \lambda \leq 2^{s+1} + 2^s + d) \end{aligned}$$

From this we know that

$$x_{\beta,\beta'} = 1 \Leftrightarrow \lambda = 0 \Leftrightarrow \beta = \beta'$$

Thus  $X = I_{\binom{2k}{k-2^s}}$ .

At last we prove that  $Y^T Y = I_{\binom{2k}{k-3 \cdot 2^s}}$ . For  $\beta \in T_{k-2^s}$ ,  $\beta' \in T_{k-3 \cdot 2^s}$ ,  $w(\beta \vee \beta') = k - 2^s + \lambda$ , where  $0 \leq \lambda \leq k - 3 \cdot 2^s = 2^s + d$ . Then

$$\begin{aligned} y_{\beta,\beta'} &= \binom{2k - (k - 2^s + \lambda)}{k + 2^s - (k - 2^s + \lambda)} \\ &\quad + \binom{2k - (k - 2^s + \lambda)}{k + 3 \cdot 2^s - (k - 2^s + \lambda)} \\ &= \binom{k + 2^s - \lambda}{k - 2^s} + \binom{k + 2^s - \lambda}{k - 3 \cdot 2^s} \\ &= \binom{2^{s+2} + 2^s + d - \lambda}{2^{s+1} + 2^s + d} + \binom{2^{s+2} + 2^s + d - \lambda}{2^s + d} \\ &\equiv 0 + \binom{2^s + d - \lambda}{2^s + d} \equiv \binom{2^s + d - \lambda}{2^s + d} \pmod{2} \end{aligned}$$

Therefore

$$y_{\beta,\beta'} = 1 \Leftrightarrow \lambda = 0 \Leftrightarrow \beta' \prec \beta$$

Let  $Y^T Y = (b_{\beta_1, \beta_2})$ ,  $\beta_1, \beta_2 \in T_{k-3 \cdot 2^s}$ . Then

$$b_{\beta_1, \beta_2} = \#\{\beta \in T_{k-2^s} \mid \beta \succ (\beta_1 \vee \beta_2)\}$$

Let  $w(\beta_1 \vee \beta_2) = k - 3 \cdot 2^s + \lambda$ , then  $0 \leq \lambda \leq k - 3 \cdot 2^s = 2^s + d$  and

$$\begin{aligned} b_{\beta_1, \beta_2} &= \binom{2k - (k - 3 \cdot 2^s + \lambda)}{k - 2^s - (k - 3 \cdot 2^s + \lambda)} = \binom{k + 3 \cdot 2^s - \lambda}{k + 2^s} \\ &= \binom{2^{s+2} + 2^{s+1} + 2^s + d - \lambda}{2^{s+2} + 2^s + d} \\ &\equiv \binom{2^s + d - \lambda}{2^s + d} \pmod{2} \end{aligned}$$

Therefore

$$b_{\beta_1, \beta_2} = 1 \Leftrightarrow \lambda = 0 \Leftrightarrow \beta_1 = \beta_2$$

which means that  $Y^T Y = I_{\binom{2k}{k-3 \cdot 2^s}}$ .

This completes the proof of Claim (5).

From Claim (5) we get

$$M^T M = \begin{pmatrix} X & Y \\ Y^T & Z \end{pmatrix} = \begin{pmatrix} I & Y \\ Y^T & 0 \end{pmatrix}$$

Then from  $Y^T Y = I$  we know that  $M$  is invertible. So the equations in Claim (4) has only zero-solution, and then by Claim (2) and Claim (3) all the coefficients of  $g$  are zero, which means  $g = 0$ .

On the other hand, if  $(1 + f)h = 0$  for some  $h \in B_n$ ,  $\deg(h) \leq k - 1$ , let

$$\begin{aligned} f'(x_1, \dots, x_n) &= f(x_1 + 1, \dots, x_n + 1) + 1, \\ h'(x_1, \dots, x_n) &= h(x_1 + 1, \dots, x_n + 1) \end{aligned}$$

then  $f'h' = 0$ ,  $\deg(h') \leq k - 1$  and  $v_{f'}$  is the same as  $v_f$  except  $a$  being changed to  $a + 1$ . Thus  $h' = 0$  and then  $h = 0$ . This means that  $AI(f) = k$ .  $\square$

### Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions which have improved much both on the technical equality and on the editorial quality of this correspondence.

### REFERENCES

- [1] F. Armknecht, "Improving fast algebraic attacks", in Proc. Workshop on Fast Software Encryption (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2004, vol. 3017, pp. 65-82.
- [2] L.M. Batten, "Algebraic attacks over  $GF(q)$ ", in Progress in Cryptology-INDOCRYPT 2004 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2004, vol. 3348, pp. 84-91.
- [3] A. Braeken, "Cryptographic properties of Boolean functions and S-boxes". PhD thesis. [Online]. Available at URL <http://homes.esat.kuleuven.be/~abraeken/thesisAn.pdf>. Katholieke University. 2006.
- [4] A. Braeken and B. Preneel, "On the algebraic immunity of symmetric Boolean functions", in Indocrypt 2005 (Lecture Notes in Computer Science), Jul. 26, 2005, vol. 3797, pp. 35-48 [Online]. Available: <http://eprint.iacr.org/>.
- [5] C.Carlet, D.K.Dalai, K.C.Gupta and S.Maitra, "Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Constructions". IEEE Trans. Inf. Theory, vol. 52, no. 7, pp. 3105-3121, Jul. 2006.
- [6] N. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations", in Advances in Cryptology-ASIACRYPT 2002 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2002, vol. 2501, pp. 267 - 287.
- [7] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback", in Advances in Cryptology-EUROCRYPT 2003 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2003, vol. 2656, pp. 345-359.
- [8] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback", in Advances in Cryptology-CRYPTO 2003 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2003, vol. 2729, pp. 176-194.
- [9] D. K. Dalai, K. C. Gupta, and S. Maitra, "Results on algebraic immunity for cryptographically significant Boolean functions", in Indocrypt 2004 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2004, vol. 3348, pp. 92-106.
- [10] 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, Jul. 2006, Also, available [Online] at <http://eprint.iacr.org/>.
- [11] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions", in Advances in Cryptology-EUROCRYPT 2004 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2004, vol. 3027, pp. 474-491.
- [12] L.J. Qu, C. Li and K. Feng, "A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables". IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2908-2910, Aug. 2007.
- [13] R.M.Wilson, "A diagonal form for the incidence matrices of  $t$ -subsets vs  $k$ -subsets". European J.Combin.11(1990), 609-614.

Longjiang Qu received his B.A. degree in 2002 and Ph.D. degree in 2007 in mathematics from the National University of Defense Technology, Changsha, China. He is now a Lecturer with the Department of Mathematics and System Science, National University of Defense Technology of China. His research fields include cryptography and coding theory.

Keqin Feng graduated from the University of Science and Technology of China (USTC), Beijing, as a graduate student in 1968 (there was no degree system in China at that time). Since 1973, he has been with the Department of Mathematics at USTC, and then in the State Key Laboratory of Information Safety of USTC in Beijing. Now he is working in the Department of Mathematical Science, Tsinghua University, Beijing. His current research interests are coding theory, cryptography and algebraic number theory.

Feng Liu received his B.A. degree in 2000 from Zhengzhou Information and Engineering University(Mathematics). He is studying in Tsinghua University of China for PhD degree now.

Lei Wang received his B.A. degree in 2006 from Tsinghua University of China(Mathematics). He is studying for PhD degree in Georgia Tech. (USA) now.