Construction of Odd-variable Boolean Functions with Optimum Algebraic Immunity

Zhichao Zhang
State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications
Beijing, China 100876
E-mail: zhichao1234@bupt.edu.cn

Zheng Huang
State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications
Beijing, China 100876
E-mail: huang2003@hotmail.com

Jie Zhang
School of Sciences
Beijing University of Posts and Telecommunications
Beijing, China 100876
E-mail: zhj503@gmail.com

Qiaoyan Wen
State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications
Beijing, China 100876
E-mail:wqy@bupt.edu.cn

***Abstract*—Recently, algebraic attacks becomes a major attack method to threat to cryptography security. In order to resist algebraic attacks, algebraic immunity as a Boolean function cryptographic property has been put out. This makes that Boolean functions should have high algebraic immunity to resist algebraic attacks. In this paper, a specific decomposition method of the space $GF(2)^n$ is proposed. By the method, we construct a class of odd number of variables Boolean functions with optimal algebraic immunity.**

Keywords- Algebraic attacks; Algebraic immunity; Boolean functions; Affine subspace

I. INTRODUCTION

In recent years, algebraic attacks [1]—[3] have received more and more attention in studying security of the cryptosystems. In order to resist algebraic attacks, Meier [5] presented a new cryptographic property of Boolean function—algebraic immunity. The algebraic immunity of a Boolean function expresses its ability to resist standard algebraic attack. Thus the algebraic immunity of Boolean function used in cryptosystem should be sufficiently high.

Courtois and Meier [4], [5] show that, for any n-variable Boolean function, its algebraic immunity is upper bounded by $\lceil \frac{n}{2} \rceil$. If the bound is achieved, we say the Boolean function have optimum algebraic immunity, referred to as MAI function. Obviously, a Boolean function with optimum algebraic immunity has strongest ability to resist standard algebraic attack. Therefore, the construction of Boolean functions with optimum algebraic immunity is of great importance. Therefore, many cryptographers are interested in construction of Boolean functions with good algebraic immunity, and gives a series of research results [6]—[11].

Carlet [7] has given a general method of constructing Boolean function with optimal algebraic immunity based on the flat theory, but the article do not give the specific classification method. In [12], a specific classification method was proposed.

In this paper, we also give a specific decomposition method for the linear space, and then we can get the linear subspaces which meet certain specific nature. Then the linear subspaces to be processed, we can get an affine space set which has specific properties. According to Carlet's research conclusions, we can get a class of odd number of variables Boolean functions with optimal algebraic immunity. Advantages of the specific method of the space decomposition are simple, intuitive and easy to operate, and easy to implement. If the affine subspace set are different, we can get different Boolean functions with optimal algebraic immunity. Thus we can continue to study different Boolean functions with optimal algebraic immunity other cryptography properties.

II. PROCEDURE FOR PAPER SUBMISSION

Let $F_2 = \{0,1\}$ be the finite field with two elements. Then a Boolean function on n variables is a mapping from F_2^n into F_2. Denote as B_n the set of all n-variable Boolean functions. The basic 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,

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

Any Boolean function has another unique representation as a multivariate polynomial over F_2, called the algebraic normal form (ANF):

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

Published by Atlantis Press, Paris, France.

where the coefficients $a_0, a_i, a_{ij}, \cdots, a_{12\cdots n} \in F_2$.

The algebraic degree $\deg(f)$ of f is the number of variables in the highest order term with nonzero coefficient.

The Hamming weight $wt(f)$ of a Boolean function f on n variables is the size of the support $\mathrm{supp}(f) = \{x \in F_2^n : f(x) = 1\}$ of the function. We denote $1_f = \mathrm{supp}(f)$ and $0_f = F_2^n \setminus \mathrm{supp}(f)$. The support and offset of a vector

$\mathrm{supp}(a)$ is the situation number of value 1 and 0's(e.g. $\mathrm{supp}(11010) = \{1,2,4\}$, $off(11010) = \{3,5\}$). We say that a Boolean function f is balanced if its truth table contains an equal number of 1's and 0's, that is, if its Hamming weight equals 2^{n-1}.

Definition 1: Given $f \in B_n$, define

$$AN(f) = \{g \in B_n \mid f \cdot g = 0\}.$$

Any function $g \in AN(f)$ is called an annihilator of f.

Definition 2: Given $f \in B_n$, we define its algebraic immunity, denote by $AI(f)$, as the minimum degree of all nonzero annihilators of f and of $f+1$, i.e. $AI(f) = \min\{\deg(g) \mid 0 \neq g \in AN(f) \cup AN(f+1)\}$.

Definition 3: Let A be a linear subspace of F_2^n with dimension k, s is a non-zero vector of F_2^n. The set

$S = \{s + a, a \in A\}$ is called a k dimension flat (affine subspace).

Proposition 1: [7] Let k be any positive integer such that $k \le \lceil \frac{n}{2} \rceil$. A sufficient condition for a function f to have no non-zero annihilator of degree strictly less than k is that there exists a sequence of flats (i.e. of affine subspaces of F_2^n) $(A_i)_{1 \le i \le r}$ of dimensions at least k, such that: $\forall i \le r, card(A_i \setminus [\bigcup_{j<i} A_j \cup \mathrm{supp}(f)]) \le 1$ (1)

$$F_2^n \setminus \mathrm{supp}(f) \subseteq \bigcup_{i \le r} A_i \quad (2)$$

Corollary 1:[7] Let n be odd. Let $A_i, i = 1, \cdots 2^{n-1}$ be a sequence of affine subspaces of F_2^n, of dimensions at least $\frac{n+1}{2}$, and such that, for every $i = 1, \cdots, 2^{n-1}$, the set $A_i \setminus \bigcup_{j<i} A_j$ is non-empty. Then, for any choice of an element b_i in each set $A_i \setminus \bigcup_{j<i} A_j$, the Boolean function of support $B = \{b_i; i = 1, \cdots 2^{n-1}\}$ and the function of support $F_2^n \setminus B$ are balanced functions of optimum algebraic immunity $\frac{n+1}{2}$.

III. CONSTRUCTION OF ODD-VARIABLE BOOLEAN

In this section, we consistently let $n = 2k+1$

Construction 1: construct 2^{n-1} linear subspaces.

Step 1: In F_2^n, list the full vectors whose weight are greater than or equal to $k+1$, a total of 2^{n-1}.

Step 2: First we order these vectors from left to right according to their weights. For the same weight vectors, we arrange sequentially from left to right according to the corresponding binary size from small to big, credited as $\{a_1, a_2, \cdots a_{2^{2k}}\}$

Let $a_i = (x_{in} x_{in-1} \cdots x_{i1}), 1 \le i \le 2^{2k}$ $x_{ij} (1 \le j \le n)$

Step 3: In a_i, we selected the k-th element $x_{ij} = 1$, where j is relatively small, denoted as $x_{i1'}, x_{i2'}, \cdots, x_{ik'}$.

Let $h_{i1} = (00\cdots 0 x_{i1'} 0 \cdots 00)$

$h_{i2} = (00\cdots 0 x_{i2'} 0 \cdots 00)$

...

$h_{ik} = (00\cdots 0 x_{ik'} 0 \cdots 00)$

In a_i, let $x_{i1'}, x_{i2'}, \cdots, x_{ik'} = 0$, get $a_{i'} = (x_{in} \cdots 000)$.

Let $h_{ik+1} = a_{i'}$.

In this way, we get a set of base $h_{i1}, h_{i2}, \cdots, h_{ik+1}$ for $W_i, (1 \le i \le 2^{2k})$

*Step 4 :*Let $W_i = L(h_{i1}, h_{i2}, \cdots h_{ik+1})$, $1 \le i \le 2^{2k}$, then we get 2^{n-1} linear subspaces. In W_i, we order these vectors from left to right according to their weights. For the same weight vector, we arrange sequentially from left to right according to the corresponding binary size from small to big. Finally $a_i, (1 \le i \le 2^{n-1})$ obviously is the only biggest vector in W_i.

Construction 2: Construction of $2^{n-1} = 2^{2k}$ affine subspaces.

First ,we select $\forall \alpha \in F_2^n, \alpha \neq 0$,

Second , let $A_i = W_i \oplus \alpha = \{\beta \oplus \alpha \mid \forall \beta \in W_i\}$,

$1 \le i \le 2^{2k}$, note $b_i = a_i \oplus \alpha$.

Finally, get $2^{n-1} = 2^{2k}$ affine subspaces $A_i, 1 \le i \le 2^{2k}$.

Construction 3: Construction of Boolean function $f(x)$

Let $\mathrm{supp}(f(x)) = \{b_i \mid 1 \le i \le 2^{n-1} = 2^{2k}\}$.

Theorem 1: The function $f(x)$ in construction 3 has optimal algebraic immunity.

Proof: Let $n = 2k+1$, $A_i (1 \le i \le 2^{2k})$ are $k+1$ dimensional affine subspaces. Because a_i is only a maximum weight vector in W_i, and a_i is different between each other, we should know that a_i is different from

$W_j (j < i)$ in an arbitrary vector. We get $W_i \setminus \bigcup_{j<i} W_j$ is non-empty, and $a_i \in W_i \setminus \bigcup_{j<i} W_j$, $1 \le i \le 2^{n-1}$.

According to $b_i = a_i \oplus \alpha$, then we can get for every $i = 1, \cdots, 2^{n-1}$, the set $A_i \setminus \bigcup_{j<i} A_j$ is non-empty, and $b_i \in A_i \setminus \bigcup_{j<i} A_j$.

We select $\mathrm{supp}(f(x)) = \{b_i \mid 1 \le i \le 2^{n-1} = 2^{2k}\}$, then the function $f(x)$ has optimal algebraic immunity according to *Corollary 1*.

Example 1: Let $n = 5$, specific Boolean function constructed as follows:

Step 1: In F_2^5, list the full vectors whose weight are greater than or equal to 3, a total of 16.

Step 2: First we order these vectors from left to right according to their weights. For the same weight vector, we arrange sequentially from left to right according to the corresponding binary size from small to big, credited as $\{a_1, a_2, \cdots a_{16}\}$, that

$a_1 = (00111)$, $a_2 = (01011)$, $a_3 = (01101)$, $a_4 = (01110)$, $a_5 = (10011)$, $a_6 = (10101)$, $a_7 = (10110)$, $a_8 = (11001)$,

$a_9 = (11010)$, $a_{10} = (11100)$, $a_{11} = (01111)$, $a_{12} = (10111)$, $a_{13} = (11011)$, $a_{14} = (11101)$, $a_{15} = (11110)$, $a_{16} = (11111)$

Let $a_i = (x_{i5} x_{i4} x_{i3} x_{i2} x_{i1}), 1 \le i \le 16$, $x_{ij}, (1 \le j \le n)$

In $a_i, (1 \le i \le 16)$, we selected the 2-th element $x_{ij} = 1$, where j is relatively small, denoted as $x_{i1'}, x_{i2'}$.

Let $h_{i1} = (0 \cdots x_{i1'} \cdots)$

$h_{i2} = (0 \cdots x_{i2'} \cdots)$

In a_i, we let $x_{i1'}, x_{i2'} = 0$, get $a_{i'} = (x_{i5} \cdots 0)$

Let $h_{i3} = a_{i'}$

In this way, we can get the following 16 groups of base vectors for $W_i, (1 \le i \le 16)$:

$h_{11} = (00001), h_{12} = (00010), h_{13} = (00100)$
$h_{21} = (00001), h_{22} = (00010), h_{23} = (01000)$
$h_{31} = (00001), h_{32} = (00100), h_{33} = (01000)$
$h_{41} = (00010), h_{42} = (00100), h_{43} = (01000)$
$h_{51} = (00001), h_{52} = (00010), h_{53} = (10000)$
$h_{61} = (00001), h_{62} = (00100), h_{63} = (10000)$
$h_{71} = (00010), h_{72} = (00100), h_{73} = (10000)$
$h_{81} = (00001), h_{82} = (01000), h_{83} = (10000)$
$h_{91} = (00010), h_{92} = (01000), h_{93} = (10000)$
$h_{101} = (00100), h_{102} = (01000), h_{103} = (10000)$
$h_{111} = (00001), h_{112} = (00010), h_{113} = (01100)$
$h_{121} = (00001), h_{122} = (00010), h_{123} = (10100)$
$h_{131} = (00001), h_{132} = (00010), h_{133} = (11000)$
$h_{141} = (00001), h_{142} = (00100), h_{143} = (11000)$
$h_{151} = (00010), h_{152} = (00100), h_{153} = (11000)$
$h_{161} = (00001), h_{162} = (00010), h_{163} = (11100)$

Let $W_i = L(h_{i1}, h_{i2}, h_{i3})$, $1 \le i \le 2^{2k} = 16$, then we get 16 linear subspaces. In W_i, we order these vectors from left to right according to their weights. For the same weight vector, we arrange sequentially from left to right according to the corresponding binary size from small to big. Finally $a_i, (1 \le i \le 16)$ obviously is the only biggest vector in W_i.

The list is as follows:

$W_1 = \{00000, 00001, 00010, 00100, 00011, 00101, 00110, 00111\}$
$a_1 = (00111)$
$W_2 = \{00000, 00001, 00010, 01000, 00011, 01001, 01010, 01011\}$
$a_2 = (01011)$
$W_3 = \{00000, 00001, 00100, 01000, 00101, 01001, 01100, 01101\}$
$a_3 = (01101)$
$W_4 = \{00000, 00010, 00100, 01000, 00110, 01010, 01100, 01110\}$
$a_4 = (01110)$
$W_5 = \{00000, 00001, 00010, 10000, 00011, 10001, 10010, 10011\}$
$a_5 = (10011)$
$W_6 = \{00000, 00001, 00100, 10000, 00101, 10001, 10100, 10101\}$
$a_6 = (10101)$
$W_7 = \{00000, 00010, 00100, 10000, 00110, 10010, 10100, 10110\}$
$a_7 = (10110)$
$W_8 = \{00000, 00001, 01000, 10000, 01001, 10001, 11000, 11001\}$
$a_8 = (11001)$
$W_9 = \{00000, 00010, 01000, 10000, 01010, 10010, 11000, 11010\}$
$a_9 = (11010)$
$W_{10} = \{00000, 00100, 01000, 10000, 01100, 10100, 11000, 11100\}$
$a_{10} = (11100)$
$W_{11} = \{00000, 00001, 00010, 00011, 01100, 01101, 01110, 01111\}$
$a_{11} = (01111)$
$W_{12} = \{00000, 00001, 00010, 00011, 10100, 10101, 10110, 10111\}$
$a_{12} = (10111)$
$W_{13} = \{00000, 00001, 00010, 00011, 11000, 11001, 11010, 11011\}$
$a_{13} = (11011)$
$W_{14} = \{00000, 00001, 00100, 00101, 11000, 11001, 11100, 11101\}$
$a_{14} = (11101)$
$W_{15} = \{00000, 00010, 00100, 00110, 11000, 11010, 11100, 11110\}$
$a_{15} = (11110)$
$W_{16} = \{00000, 00001, 00010, 00011, 11100, 11101, 11110, 11111\}$
$a_{16} = (11111)$

We select $\alpha = (00001)$.

Let $A_i = W_i \oplus \alpha = \{\beta \oplus \alpha \,|\, \forall \beta \in W_i\}$ $1 \le i \le 2^{2k} = 16$,

$b_i = a_i \oplus \alpha$

Finally, we get 16 affine subspaces. as follows:

$A_1 = \{00001, 00000, 00011, 00101, 00010, 00100, 00111, 00110\}$

$b_1 = (00110)$

$A_2 = \{00001, 00000, 00011, 01001, 00010, 01000, 01011, 01010\}$

$b_2 = (01010)$

$A_3 = \{00001, 00000, 00101, 01001, 00100, 01000, 01101, 01100\}$

$b_3 = (01100)$

$A_4 = \{00001, 00011, 00101, 01001, 00111, 01011, 01101, 01111\}$

$b_4 = (01111)$

$A_5 = \{00001, 00000, 00011, 10001, 00010, 10000, 10011, 10010\}$

$b_5 = (10010)$

$A_6 = \{00001, 00000, 00101, 10001, 00100, 10000, 10101, 10100\}$

$b_6 = (10100)$

$A_7 = \{00001, 00011, 00101, 10001, 00111, 10011, 10101, 10111\}$

$b_7 = (10111)$

$A_8 = \{00001, 00000, 01001, 10001, 01000, 10000, 11001, 11000\}$

$b_8 = (11000)$

$A_9 = \{00001, 00011, 01001, 10001, 01011, 10011, 11001, 11011\}$

$b_9 = (11011)$

$A_{10} = \{00001, 00101, 01001, 10001, 01101, 10101, 11001, 11101\}$

$b_{10} = (11101)$

$A_{11} = \{00001, 00000, 00011, 00010, 01101, 01100, 01111, 01110\}$

$b_{11} = (01110)$

$A_{12} = \{00001, 00000, 00011, 00010, 10101, 10100, 10111, 10110\}$

$b_{12} = (10110)$

$A_{13} = \{00001, 00000, 00011, 00010, 11001, 11000, 11011, 11010\}$

$b_{13} = (11010)$

$A_{14} = \{00001, 00000, 00101, 00100, 11001, 11000, 11101, 11100\}$

$b_{14} = (11100)$

$A_{15} = \{00001, 00011, 00101, 00111, 11001, 11011, 11101, 11111\}$

$b_{15} = (11111)$

$A_{16} = \{00001, 00000, 00011, 00010, 11101, 11100, 11111, 11110\}$

$b_{16} = (11110)$

Let $\mathrm{supp}(f(x)) = \{b_i \,|\, 1 \le i \le 2^{n-1} = 2^{2k} = 16\} =$

$\{00110, 01010, 01100, 01111, 10010, 10100, 10111,$

$11000, 11011, 11101, 01110, 10110, 11010, 11100, 11111, 11110\}$

The function $f(x)$ has optimal algebraic immunity according to *Theorem 1*, $AI(f(x)) = 3$.

IV. CONCLUSION

In this paper, we give a specific decomposition method for the linear space, and then we get a class of odd number of variables Boolean functions with optimal algebraic immunity. In order to better resist the existing attack, Boolean function used in cryptosystem not only should have higher algebraic immunity degree, but also need to have some other cryptographic properties. Boolean functions constructed in this paper only consider its optimal algebraic immunity, without considering other cryptographic properties. With the change of the affine subspace, the constructed optimal algebraic immunity of Boolean functions will change, and other cryptographic properties of the corresponding Boolean function are also not the same. Therefore, in order to Boolean functions have better cryptographic properties, how to improve the constructor is pending further study.

Acknowledgment

This work is supported by NSFC (Grant Nos. 61272057, 61202434, 61170270, 61100203, 61003286, 61121061), the Fundamental Research Funds for the Central Universities (Grant No. 2012RC0612, 2011YB01).

REFERENCES

[1] Courtois N, Merier W, “Algebraic attacks on stream ciphers with linear feedback,” In: Advances in Cryptology-EUROCRYPT 2003, LNCS 2656. Berlin, Heideberg: Springer, 2003. 345-359.

[2] Courtois N, “Fast algebraic attacks on stream ciphers with linear feedback,” In: Advances in Cryptology-CRYPTO 2003, LNCS 2729. Berlin, Heidelberg: Springer, 2003. 176-194.

[3] Armknecht F, Krause M, “Algebraic attacks on combiners with memeory,” In: Advances in Cryptology-CRYPTO 2003, LNCS 2729. Berlin, Heidelberg: Springer,2003. 162-175.

[4] N. Courtois and W. Meier, “Algebraic Attacks on Stream Ciphers with Linear Feedback,” Advances in Cryptology-Eurocrypt 2003, Berlin: Springer- Verlag, 2003, 345-359

[5] W. Meier, E. Pasalic, and C. Carlet, “Algebraic attacks and decomposition of Boolean functions,” Advances in Cryptology-Eurocrypt 2004, Berlin: Springer-Verlag, 2004, 474-491

[6] Braeken A, Preneel B, “On the algebraic immunity of symmetric Boolean functions.,” In: Progress in Cryptology-INDOCRYPT 2005, LNCS 3797. Berlin, Heidelberg: Springer, 2005. 35—48

[7] Carlet C, “A method of construction of balanced functions with optimum algebraic immunity,” Available at http://eprint.iacr.org/2006/149

[8] Dalai D K, Gupta K C, Maitra S, “Cryptographically significant Boolean functions: Construction and analysis in terms of algebraic immunity,”In: FSE 2005, LNCS 3557. Berlin, Heidelberg: Springer, 2005. 98—111

[9] Dalai D K, Maitra S, Sarkar S, “Basic theory in construction of Boolean functions with maximum possible annihilator immunity,” In: Designs, Codes and Cryptography. Heidelberg: Springer. 2006, 40(1): 41—58

[10] Li N, Qi W F, “Construction and count of Boolean functions of an odd number of variables with maximum algebraic immunity,” Available at http://arxiv.org/abs/cs.CR/0605139

[11] Qu L J, Feng G Z, Li C, “On the Boolean functions with maximum possible algebraic immunity: construction and a lower bound of the count,” http://eprint.iacr.org/2005/449

[12] Claude Carlet, Xiangyong Zeng, Chunlei Li, Lei Hu, “Further properties of several classes of Boolean functions with optimum algebraic immunity,” In: Des. Codes Cryptogr. (2009) 52:303–338