LETTER

Translation Equivalence of Boolean Functions Expressed by Primitive Element*

Yindong CHEN[†a)], ***Member***, **Liu ZHANG**[†], ***Nonmember***, **Deng TANG**[††b)], ***Member***, ***and* Weihong CAI**[†], ***Nonmember***

SUMMARY In recent years, algebraic attacks and fast algebraic attacks have received a lot of attention in the cryptographic community. There are three Boolean functions achieving optimal algebraic immunity based on primitive element of F_{2^n}. The support of Boolean functions in [1]–[3] have the same parameter s, which makes us have a large number of Boolean functions with good properties. However, we prove that the Boolean functions are affine equivalence when s takes different values.

key words: *Boolean function, primitive element, affine equivalence*

1. Introduction

Boolean functions are the building blocks of many stream ciphers and various design criteria have been proposed for cryptographic Boolean functions in order to resist different kinds of attacks. Boolean functions should have balancedness, high nonlinearity, high algebraic degree, high algebraic immunity and good behavior against fast algebraic attacks. However, some Boolean functions with good cryptography are affine equivalence. Affine equivalence is a basic equivalence relation of Boolean functions, and affine equivalent functions have many similar cryptographic properties, such as nonlinearity, difference property and so on. We can also construct more excellent Boolean functions by using the affine equivalence relations of Boolean functions[4].

In [1], Carlet and Feng proposed an infinite excellent class of balanced functions with optimal algebraic immunity as well as with a very high nonlinearity. This is the first time that a Boolean function seems to satisfy all the cryptography necessities. After, Tu and Deng [3] constructed a class of $2m$-variable Boolean functions based on the additive decomposition which optimized most of the criteria, but had two drawbacks that the optimal algebraic immunity of them could only be proved assuming the correctness of a combinatorial conjecture, and the ability of them resisting fast algebraic attacks was bad. In [2], Tang adopted a similar technique, constructing a class of optimal algebraic immunity functions which also had other good properties and good immunity against fast algebraic attacks. The support of Boolean functions in [1]–[3] have the same parameter s, which makes us have a large number of Boolean functions with good properties. However, we prove that the Boolean functions are affine equivalence when s takes different values.

The letter is organized as follows. In Sect. 2, some preliminaries of Boolean functions are presented. In Sect. 3, we prove that the translation equivalence relation of support of C-F function. The translation equivalence relation of support in Tu-Deng function and T-C-T function are proved in Sect. 4. Finally, Sect. 5 concludes this letter.

2. Preliminaries

Let F_2^n be the vector space of n-tuples over the field $F_2 = \{0, 1\}$ of two elements, and F_{2^n} be the finite field of order 2^n. A Boolean function of n variables is a function from F_2^n into F_2. Denote by B_n the set of all the Boolean function of n variables. The basic representation of a Boolean function $f(x_1, \ldots, x_n)$ is by its truth table, i.e.,

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

Note that F_{2^n} is isomorphic to F_2^n through the choice of some basic of F_{2^n} over F_2. For convenience, we shall represent the truth table of Boolean function as

$$[f(0), f(1), f(\alpha), \ldots, f(\alpha^{2^n-2})],$$

where α is a primitive element of F_{2^n}.

The Boolean function over F_{2^n} can be uniquely expressed by a univariate polynomial

$$f(x) = \sum_{i=0}^{2^n-1} \alpha_i x^i,$$

and $f = f^2$ implies that $\alpha_0, \alpha_{2^n-1} = 0$ and $\alpha_i^2 = \alpha_{2i \pmod{2^n-1}}$ for every $i = 1, \ldots, 2^n - 2$.

Besides when n is even, the Boolean function of n-variable can be viewed over $F_{2^{n/2}}^2$ and uniquely expressed

Manuscript received August 20, 2018.
Manuscript revised November 23, 2018.

[†]The authors are with the College of Engineering, Shantou University, and the Guangdong Provincial Key Laboratory of Digital Signal and Image Processing Techniques, China.

[††]The author is with School of Mathematics, Southwest Jiaotong University, and the Guangxi Key Laboratory of Cryptography and Information Security, China.

[*]The work is supported by the National Natural Science Foundation of China (No. 61103244, 61702318), the Science and Technology Planning Project of Guangdong Province (No. 2016B010124012, 2016B090920095), the Special Funds for Guangdong Science and Technology Innovation Strategy (longitudinal collaborative management direction, No. 180917104960489).

a) E-mail: ydchen@stu.edu.cn
b) E-mail: dtang@foxmail.com (Corresponding author)

DOI: 10.1587/transfun.E102.A.672

by a bivariate polynomial

$$f(x,y)=\sum_{i,j=0}^{2^{n/2}-1} a_{i,j}x^iy^j,$$

where $a_{i,j} \in F_{2^{n/2}}$ are such that $a_{i,j}^2 = a_{2i \pmod{2^{n/2}-1}, 2j \pmod{2^{n/2}-1}}$ for $1 \le i, j < 2^{n/2}-1$.

Definition 1. *The algebraic immunity $AI_n(f)$ of an n-variable Boolean function $f \in B_n$ is defined to the lowest degree of nonzero Boolean function g such that $f \cdot g = 0$ or $(f+1) \cdot g = 0$.*

Finally, two n-variable Boolean functions f and g are called affine equivalent if there exist an $n \times n$ invertible matrix A over F_2 and a vector $a \in F_2^n$ such that

$$f(X) = g(X \cdot A \oplus a),$$

where $X = (x_1, x_2, \dots, x_n) \in F_2^n$. Since two affine equivalent Boolean functions have the same algebraic degree, it can be seen that they also have the same algebraic immunity. Thus, algebraic immunity of Boolean functions is affine invariant.

Let the register generate an m-sequence of period $q-1$, and the sequence $\{s_t\}$ obey the recursion

$$\sum_{j=0}^{n} m_j s_{t+j} = 0, m_j \in F_2,$$

where $m_0 = m_n = 1$. That is, $m(x) = 1 + m_1x + \cdots + m_{n-1}x^{n-1} + x^n$ is its generator polynomial and is primitive. The (transpose) companion matrix M (we call it the generator matrix of the sequence) is

$$M = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 \\ m_0 & m_1 & \cdots & m_{n-2} & m_{n-1} \end{pmatrix}.$$

Let $(s_t, s_{t+1}, \dots, s_{t+n-1})^T$ denote the state of the register at time t. Then the next state is determined by

$$\begin{aligned}(s_{t+1}, s_{t+2}, \dots, s_{t+n})^T &= M(s_t, s_{t+1}, \dots, s_{t+n-1})^T \\ &= M^{t+1}(s_0, s_1, \dots, s_{n-1})^T\end{aligned}$$

If the initial state of the register is b, then the sequence can be represented by $S = (b, Mb, \dots, M^{q-2}b)$. Here b can be any nonzero n-dimensional column vector and hence there are exactly $q-1$ such S which correspond to $q-1$ different m-sequences. Let $b_0 = (1, 0, \dots, 0)^T$. Then these sequences can be represented by

$$S_k = (M^k b_0, M^{k+1}b_0, \dots, M^{k+q-2}b_0),$$

where $0 \le k \le q-2$.

Since the number of primitive polynomials of degree n is $\phi(q-1)/n$, there are $\phi(q-1)/n$ LFSRs generating m-sequences, and different LFSRs correspond to different sequences. Therefore, there are exactly $(q-1)\phi(q-1)/n$ m-sequences, and each sequence can be represented by

$$S_{j,k} = (M_j^k b_0, M_j^{k+1} b_0, \dots, M_j^{k+q-2} b_0),$$

where $1 \le j \le \phi(q-1)/n$. M_j is the generator matrix of the sequence and $1 \le k \le q-2$. Clearly, $M_j^k b_0$ is the initial state of the LFSR.

Let $T = F_2^n - \{\mathbf{0}\}$. Clearly, there are exactly two $f \in B_n$ such that $1_f \bigcap T = T_0$, where T_0 is a subset of T. We denote these two functions by f_1 and f_2. Then f_1 differs from f_2 only when $x = 0$ and $f_1 = f_2 + (x_1+1)(x_2+1)\dots(x_n+1)$. Given any LSFR, the keystream generated by using f_1 or f_2 as the filter function is the same. There, f_1 and f_2 can be viewed as the same function and we consider the set

$$B_n^* = B_n/\{0, (x_1+1)(x_2+1)\dots(x_n+1)\}.$$

Then any $f \in B_n^*$ can be represented by its support set in the form

$$1_f = \{M_j^{i_1} b_0, M_j^{i_2} b_0, \dots, M_j^{i_w} b_0\},$$

where M_j is the generator matrix of the register and $0 \le i_1 < i_2 < \dots < i_w \le q-2$.

3. Translation Equivalence Relation of Support of C-F Function

Carlet and Feng constructed a class of Boolean functions with optimal algebraic immunity based on primitive elements of finite fields and univariate representation of Boolean function.

Construction 1 ([1]). *Let n be an integer greater than 1 and α be a primitive element of F_{2^n}. If f is an n-variable Boolean function whose support is*

$$\{0, \alpha^s, \alpha^{s+1}, \dots, \alpha^{s+2^{n-1}-2}\},$$

where $0 \le s < 2^n - 1$ is an integer, then f has optimal algebraic immunity $\lceil n/2 \rceil$.

There is a parameter s in the support of the C-F function. When we take different values of s, the supports of C-F function are also different, and the corresponding Boolean function is also different. Therefore, based on this construction method, we can get a large number of optimal algebraic immune Boolean functions. However, we find that when s takes different values, Boolean functions obtained are affine equivalent, and its algebraic degree, algebraic immunity and nonlinearity are invariant.

Later on, the authors gave a method of constructing Boolean functions with optimal algebraic immunity by companion matrixes of primitive polynomials over F_2 in [6]. Their main result is completely equivalent to the following one which replaces companion matrixes of primitive polynomial by binary m-sequences.

Construction 2 ([6]). *Let n be an integer greater than 1 and $\underline{s} = (s_t)_{t \ge 0}$ be an m-sequence of order n. If an n-variable Boolean function f whose support is*

$$\{\boldsymbol{0}\} \cup \{s_t, s_{t+1}, \ldots, s_{t+n-1} | 0 \le t \le 2^{n-1} - 2\},$$

where $\boldsymbol{0}$ *denotes the all-zero vector in* F_2^n*, then f has optimal algebraic immunity* $\lceil n/2 \rceil$.

In fact, the author has proved that both Construction 1 and the Construction 2 are the same in the sense of affine equivalence in [7].

Lemma 1 ([7])**.** *Let n be an integer greater than 1 and* $m(x)$ *be a primitive polynomial of degree n over* F_2*. If* $\alpha \in F_{2^n}$ *is a root of* $m(x)$ *and* $\underline{s} = (s_t)_{t \ge 0} \in G(m(x))$ *is a nonzero sequence, then there exists a basis* $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ *of* F_{2^n} *such that*

$$s_t\beta_0 \oplus s_{t+1}\beta_1 \oplus \cdots \oplus s_{t+n-1}\beta_{n-1} = \alpha^t, t \ge 0.$$

Lemma 2 ([8])**.** *Let* $f \in Bn$ *and*

$$1_f = \{M_1^{k_1+i_1} b_0, M_1^{k_1+i_2} b_0, \ldots, M_1^{k_1+i_w} b_0\},$$

where M_1 *is the generator matrix of the sequence and* $0 \le i_1 < i_2 < \ldots < i_w \le q-2$*. Clearly, any* $g \sim f$ *can be represented by*

$$1_g = \{M_j^{k_2+i_1} b_0, M_j^{k_2+i_2} b_0, \ldots, M_j^{k_2+i_w} b_0\},$$

where $1 \le j \le \phi(q-1)/n$*,* M_j *is a generator matrix and* $0 \le k_2 \le q-2$*.*

Theorem 1. *Let n be an integer greater than 1 and α be a primitive element of* F_{2^n}*. If f is an n-variable Boolean function whose support is*

$$\{0, \alpha^s, \alpha^{s+1}, \ldots, \alpha^{s+2^{n-1}-2}\},$$

where $0 \le s < 2^n - 1$ *is an integer. When s takes different values, Boolean functions obtained are affine equivalent.*

Proof. From Lemma 1, we can know every α^t in the support of C-F function has a non-zero sequence $\{s_t, s_{t+1}, \ldots, s_{t+n-1}\}$ corresponding to it. Let $(s_t, s_{t+1}, \ldots, s_{t+n-1})^T$ denote the state of the register at time t. Then the next state is determined by

$$\begin{aligned}(s_{t+1}, s_{t+2}, \ldots, s_{t+n})^T &= M(s_t, s_{t+1}, \ldots, s_{t+n-1})^T \\ &= M^{t+1}(s_0, s_1, \ldots, s_{n-1})^T\end{aligned}$$

If the initial state of the register is b_0, then the sequence can be represented by $(s_{t+1}, s_{t+2}, \ldots, s_{t+n}) = (M^t b_0, M^{t+1} b_0, \ldots, M^{t+n-1} b_0)$. Since

$$s_t\beta_0 \oplus s_{t+1}\beta_1 \oplus \cdots \oplus s_{t+n-1}\beta_{n-1} = \alpha^t, t \ge 0,$$

it follows that

$$M^t b_0 \beta_0 \oplus M^{t+1} b_0 \beta_1 \oplus \cdots \oplus M^{t+n-1} b_{n-1} \beta_0 = \alpha^t, t \ge 0.$$

So, we can represent the C-F function as

$$1_f = \{0\} \cup \{M_1^{i+s} b_0 | i = 0, 1, \ldots, 2^{n-1} - 2, 0 \le s < 2^n - 1\}.$$

From Lemma 2, we can know that given an LFSR and its generator matrix M_1, let $f_1 \in B_n^*$ and

$$1_{f_1} = \{M_1^i b_0 | i = 0, 1, \ldots, 2^{n-1} - 1\}.$$

Clearly, any $g \sim_L f_1$can be represented by

$$1_g = \{M_1^{s+i} b_0 | i = 0, 1, \ldots, 2^{n-1} - 1\},$$

where M_1 is a generator matrix and $0 \le s < 2^n - 1$. Finally, we can get that when $0 \le s < 2^n - 1$ takes different values, the C-F functions are affine equivalent.

4. Translation Equivalence Relation of Support of Tu-Deng Function and T-C-T Function

Tu.Z and Deng.Y [3] constructed a class of bent function with optimal algebraic immunity, which belongs to the class PS^- defined by Dillon. By modifying the truth table, this function can be changed into a balanced Boolean function. Its nonlinearity is slightly reduced, but it has the optimal algebraic immunity. However, in this article, the focus of our study is the affine equivalence.

Construction 3 ([3])**.** *Let* $n = 2k$ *and α be a primitive element of* F_{2^k}*. The Boolean function* $g : F_{2^k} \to F_2$ *is defined as*

$$\mathrm{supp}(g) = \{1 = \alpha^s, \alpha^{s+1}, \ldots, \alpha^{2^{k-1}+s-1}\}.$$

Let Boolean function $f : F_{2^k} \times F_{2^k} \to F_2$ *be defined as*

$$f(x, y) = g(x/y).$$

Theorem 2. *Let* $n = 2k$ *and β be a primitive element of* F_{2^n}*.The Boolean function* $f : F_{2^k} \times F_{2^k} \to F_2$ *be defined as*

$$f(x, y) = g(x/y),$$

the support of Boolean function f can be written

$$\mathrm{supp}(f) = \{\beta^{(2^k+1)(i+s)} + \beta^{2^k-1} \cdot \beta^{(2^k+1)j}\},$$

where $i \in (0, 2^k), j \in (0, 2^k), (i-j) \pmod{2^k - 1} \in (0, 2^{k-1} - 1),$ $0 \le s < 2^k - 1$ *is an integer.*

Proof. We assume that α be a primitive element of F_{2^k} and β be a primitive element of F_{2^n}, so $\alpha = \beta^{(2^n-1)/(2^k-1)} = \beta^{2^k+1}$. By Construction 3, we can assume $x = \alpha^i, y = \alpha^j$, so

$$f(x, y) = f(\alpha^i, \alpha^j) = g(\alpha^{i-j})$$

and $x = \beta^{(2^k+1)i}, y = \beta^{(2^k+1)j}$. Let w be any element in $F_{2^n}/F_{2^{n/2}}$. The pair$(1, w)$ is a basis of the $F_{2^{n/2}}$-vectorspace F_2^n. Hence, we have $F_{2^n} = F_{2^{n/2}} + wF_{2^{n/2}}$. Let $w = \beta^{(2^n-1)/(2^k+1)} = \beta^{2^k-1}$, so $f(x, y) = f(\alpha^i, \alpha^j) = f(\alpha^i + w\alpha^j)$. By support of g, we can know $g(\alpha^{i-j}) = 1$ when $(i-j) \pmod{2^k - 1} \in (0, 2^{k-1} - 1)$. Finally, we can know that the support of f is

$$\mathrm{supp}(f) = \{\beta^{(2^k+1)i} + \beta^{2^k-1} \cdot \beta^{(2^k+1)j}\}.$$

Inspired by Tu-Deng function, the author [2] proposed two classed of Boolean functions of $n = 2k$ variables, with very good cryptographic properties based on the function $g(xy)$ instead of $g(x/y)$, where $k \geq 2$. The functions in the first class are unbalanced, with Hamming weight $2^{n-1} - 2^{k-1}$, algebraic degree $n - 2$, and high nonlinearity.

Construction 4 ([2]). *Let $n = 2k > 4$. Let α be a primitive element of the finite field F_{2^k}. Set $\Delta = \{\alpha^s, \ldots, \alpha^{2^{k-1}+s-1}\}$ where $0 \leq s < 2^k - 1$ is an integer. Then Boolean function $f \in B_n$ as follows:*

$$f(x, y) = g(xy),$$

where the support of Boolean function g is Δ.

Theorem 3. *Let $n = 2k$ and β be a primitive element of F_{2^n}. The Boolean function $f : F_{2^k} \times F_{2^k} \to F_2$ be defined as*

$$f(x, y) = g(xy),$$

the support of Boolean function f can be written

$$\mathrm{supp}(f) = \{\beta^{(2^k+1)(i+s)} + \beta^{2^k-1} \cdot \beta^{(2^k+1)j}\},$$

where $i \in (0, 2^k)$, $j \in (0, 2^k)$, $(i + j) \pmod{2^k - 1} \in (0, 2^{k-1} - 1)$, $0 \leq s < 2^k - 1$ is an integer.

Proof. The proof is the similar to the Theorem 2.

Theorem 4. *When s takes different values, T-C-T functions are affine equivalent. Meanwhile, Tu-Deng function are also affine equivalent.*

Proof. We first prove that the T-C-T functions are equivalent when s takes different values. The support of T-C-T function f can be written

$$\mathrm{supp}(f) = \{\beta^{(2^k+1)(i+s)} + \beta^{2^k-1} \cdot \beta^{(2^k+1)j}\}.$$

We can see each element in the support of the T-C-T function as the two part, separated by the plus sign. We let $Part_1 = \beta^{(2^k+1)(i+s)}$ and $Part_2 = \beta^{2^k-1} \cdot \beta^{(2^k+1)j}$. It is known from Theorem 1 that the Boolean functions obtained by $Part_1$ are affine equivalent when s takes different values. In addition,the use of the $Part_2$ only assigns the corresponding position in the $Part_2$ of the $Part_1$ to 1, increasing the number of 1 in the truth table. As long as the $Part_1$ is confirmed, the $Part_2$ is confirmed. So the $Part_2$ has no effect on the translational nature of the whole support set. Therefore, the T-C-T functions are affine equivalent when s takes different values. The same reason can be obtained Tu-Deng functions are also affine equivalent when s takes different values.

5. Conclusion

The letter studies the affine equivalent relation between the class of Boolean functions based on primitive elements of F_{2^n}. Although these three constructions do not possess a large number of Boolean functions with good properties, they have excellent properties. It is very helpful for us to construct Boolean functions by studying the affine equivalence relation of Boolean functions.

References

[1] C. Carlet and K. Feng, “An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity,” International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp.425–440, Springer-Verlag, 2008.

[2] 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.

[3] 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.

[4] L. Sun, F. Fu, and X. Guang, “On the nonlinearity and affine equivalence classes of C-F functions,” IEICE Trans. Fundamentals, vol.E99-A, no.6, pp.1251–1254, 2016.

[5] J. Zhang, B. Wu, Y. Chen, and Z. Liu, “Constructing 2 m-variable Boolean functions with optimal algebraic immunity based on polar decomposition of $F_{2^{2m}}$,” Int. J. Found. Comput. Sci., vol.25, no.5, pp.537–551, 2014.

[6] Q. Wang, J. Peng, and H. Kan, “Constructions of cryptographically significant Boolean functions using primitive polynomials,” IEEE Trans. Inf. Theory, vol.56, no.6, pp.3048–3053, 2010.

[7] H. Chen, T. Tian, and W. Qi, “On the affine equivalence relation between two classes of Boolean functions with optimal algebraic immunity,” Des. Codes Cryptogr., vol.67, no.2, pp.175–185, 2013.

[8] Q. Wang and T. Johansson, “On equivalence classes of Boolean functions,” Information Security and Cryptology - ICISC 2010, pp.311–324, Springer Berlin Heidelberg, 2010.