ARTICLE IN PRESS

Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

A characterization of balanced Boolean functions with optimal algebraic immunity

Xie Tao

Faculty of Mathematic and Statistic, Hubei Normal University, Huangshi, 435002, China

ARTICLE INFO

Article history:
Received 5 July 2017
Received in revised form 13 March 2018
Accepted 21 March 2018
Available online xxxx

Keywords:
Algebraic immunity
Boolean function
Schur function
Annihilator
Nonlinearity

ABSTRACT

In this paper, we characterize balanced Boolean functions with optimal algebraic immunity by Schur functions. By applying this characterization, three classes of balanced Boolean functions with optimal algebraic immunity are constructed. Some examples of the constructed functions with other desired cryptographic properties are also presented.

1. Introduction

Boolean functions used in stream ciphers should satisfy some necessary cryptographic criteria, such as balancedness, a high algebraic degree and a high nonlinearity. In 2003, Courtois and Meier proposed algebraic attacks on stream ciphers [9]. As a result, algebraic immunity (AI) was proposed in [23] as a new design criterion of Boolean functions used in stream ciphers. Therefore it is important to construct Boolean functions with optimal AI and other good cryptographic properties.

Before 2008, researchers mainly focused on studying optimal AI n-variable Boolean functions defined in the n-dimensional vector space over the binary field $\mathbb{F}_2$ [2,3,5,7,10,11,18,19], where n is an integer with $n \geq 2$. However, it is difficult to measure other cryptographic properties of these functions. For example, in several constructions such as those proposed in [7] and [11], Krawtchouk polynomials were used to measure the nonlinearities of the constructed Boolean functions. In this way, only some rough bounds on nonlinearities are obtained and they are not high enough for Boolean functions used in stream ciphers. In 2008, an infinite class of balanced Boolean functions, Carlet–Feng functions, defined over the finite field $\mathbb{F}_{2^n}$ of 2^n elements was proposed, and the functions in this class were proved to satisfy all the main cryptographic criteria [6]. The cryptographic properties of the proposed functions can be efficiently identified since some tools in the areas such as coding theory and Gauss sums can be applied. This also motivated people to study optimal AI Boolean functions represented as univariate or bivariate polynomials over $\mathbb{F}_{2^n}$ [14,15,17,21,24–30,32].

For an integer $n \geq 2$, the n-variable Carlet–Feng function has the support set

$$\left\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^{n-1}-2}\right\},$$

where α is a primitive element of $\mathbb{F}_{2^n}$. The BCH bound can be used to prove that the Carlet–Feng function has optimal AI. To generalize the construction of Carlet–Feng functions, a natural idea is to find more integer vectors $(a_1, a_2, \ldots, a_{2^{n-1}-1})$ with $0 \leq a_1 < a_2 < \cdots < a_{2^{n-1}-1} \leq 2^n - 2$ such that the n-variable Boolean function with the support set

E-mail address: xietao1294@sina.com.

https://doi.org/10.1016/j.dam.2018.03.059
0166-218X/

$\{0, \alpha^{a_1}, \alpha^{a_2}, \ldots, \alpha^{a_{2^{n-1}-1}}\}$ has optimal AI and other desired cryptographic properties. However, the BCH bound is not necessarily valid when the integer vector does not satisfy $a_i = si + t$ for all $1 \le i \le 2^{n-1} - 1$, where s, t are nonnegative integers such that $(s, 2^n - 1) = 1$.

The purpose of this paper is to study the question mentioned above. A necessary and sufficient condition for a Boolean function having optimal AI is proposed by judging whether the values of a Schur function related to this Boolean function on some special vectors are equal to zero or not. The values of the Schur function on the vectors can be calculated by some corresponding determinants. With this characterization, three classes of Boolean functions with optimal AI are constructed. Some examples of the constructed functions with other cryptographic properties are also presented.

Very recently, a relation between the Schur function and AI is also discovered in [30]. Compared with their work, this paper discusses the method in more detail and proposes three constructions, which comprise functions affinely inequivalent to those in [6] and [28] on some finite fields of small degrees.

The remainder of this paper is organized as follows. In Section 2, we introduce some necessary concepts and results. In Section 3, a correspondence between balanced Boolean functions with optimal AI and Schur functions is established. Further, three constructions of balanced Boolean functions with optimal AI are proposed. In Section 4, some examples of the constructed functions with other cryptographic properties are given. Section 5 concludes the paper.

2. Preliminaries

2.1. Boolean functions and algebraic immunity

For a positive integer n, let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. A Boolean function in n variables is a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, and we denote by $\mathbb{B}_n$ the set of all n-variable Boolean functions. In the following discussion, for a set A, we use the symbol $|A|$ to denote its cardinality.

Let α be a primitive element of $\mathbb{F}_{2^n}$. A Boolean function $f \in \mathbb{B}_n$ can be defined by its truth table, namely the binary string of length 2^n which lists all of its output values, $[f(0), f(1), f(\alpha), \ldots, f(\alpha^{2^n-2})]$. The *support set* of a Boolean function $f \in \mathbb{B}_n$ is defined as $\mathrm{supp}(f) = \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$, and the *Hamming weight* $wt(f)$ of f is the cardinality of its support set. Similarly, the zero set is defined as $\mathrm{zero}(f) = \{x \in \mathbb{F}_{2^n} \mid f(x) = 0\}$. If the cardinalities of $\mathrm{supp}(f)$ and $\mathrm{zero}(f)$ are the same, i.e., $wt(f) = 2^{n-1}$, f is called *balanced*. The *Hamming distance* $d_H(f, g)$ between two Boolean functions f and g is the Hamming weight of their difference $f + g$ (by abuse of notation, we use $+$to denote the addition on $\mathbb{F}_2$, i.e., the XOR) and defined as $d_H(f, g) = |\{x \in \mathbb{F}_{2^n} | f(x) + g(x) = 1\}|$.

A Boolean function f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ can be uniquely expressed as $f(x) = \sum_{i=0}^{2^n-1} \alpha_i x^i$ in terms of a univariate polynomial, where $\alpha_0, \alpha_{2^n-1} \in \mathbb{F}_2$, $\alpha_i \in \mathbb{F}_{2^n}$ for $1 \le i \le 2^n - 2$ such that $(\alpha_i)^2 = \alpha_{2i \pmod{2^n-1}}$. The *algebraic degree* $\deg(f)$ of f is defined to be the largest integer $wt(k)$ with $\alpha_k \neq 0$, where $wt(k)$ (called the *weight* of k) is the number of nonzero coefficients in the binary representation of k. A Boolean function is *affine* if it has algebraic degree at most 1, and the set of all affine functions is denoted by $\mathbb{A}_n$. For other properties of univariate representations of Boolean functions, see [4,20,24].

The *Walsh transform* of $f \in \mathbb{B}_n$ at $\omega \in \mathbb{F}_{2^n}$ is defined by

$$W_f(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+tr(\omega x)},$$

where $tr(x) = x + x^2 + \cdots + x^{2^{n-1}}$ is the *absolute trace function* over $\mathbb{F}_{2^n}$. The *Walsh spectrum* of f is the multi-set of all values of its Walsh transform. The *nonlinearity* of a function $f \in \mathbb{B}_n$ is its distance from the set of all n-variable affine functions, i.e., $nl(f) = \min_{g \in \mathbb{A}_n}(d_H(f, g))$. This parameter can also be expressed by means of its Walsh spectrum as

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

Definition 1. For $f \in \mathbb{B}_n$, define $AN(f) = \{g \in \mathbb{B}_n \mid f \cdot g = 0\}$. Any function $g \in AN(f)$ is called an *annihilator* of f. The *algebraic immunity* (*AI*) of f is the minimum degree of all the nonzero annihilators of f and of all those of $f + 1$. We denote it by $AI(f)$.

The following lemma can be derived directly from Definition 1.

Lemma 1 ([8]). *For $f, g, h \in \mathbb{B}_n$,*
(i) if $g \in AN(f)$, then $\mathrm{supp}(f) \subseteq \mathrm{zero}(g)$ and $\mathrm{supp}(g) \subseteq \mathrm{zero}(f)$.
(ii) if $h \in AN(f + 1)$, then $\mathrm{zero}(f) \subseteq \mathrm{zero}(h)$ and $\mathrm{supp}(h) \subseteq \mathrm{supp}(f)$.

Lemma 2 ([8]). *For odd n, if a balanced n-variable Boolean function f does not have any nonzero annihilator with algebraic degree $< \frac{n+1}{2}$, then $f + 1$ has no nonzero annihilator with algebraic degree $< \frac{n+1}{2}$. Consequently, $AI(f) = \frac{n+1}{2}$.*

Lemma 3 ([5]). *For $f \in \mathbb{B}_n$, $AI(f) = \lceil \frac{n}{2} \rceil$ implies*
(i) f is balanced when n is odd;
(ii) $\sum_{i=0}^{\frac{n}{2}-1} \binom{n}{i} \le wt(f) \le \sum_{i=0}^{\frac{n}{2}} \binom{n}{i}$ when n is even.

Please cite this article in press as: T. Xie, A characterization of balanced Boolean functions with optimal algebraic immunity, Discrete Applied Mathematics (2018), https://doi.org/10.1016/j.dam.2018.03.059.