Discrete Applied Mathematics 167 (2014) 25–32

Contents lists available at ScienceDirect

Discrete Applied Mathematics

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

Note

Balanced Boolean functions with optimum algebraic degree, optimum algebraic immunity and very high nonlinearity

Qichun Wang *, Chik How Tan

Temasek Laboratories, National University of Singapore, 117411, Singapore

ARTICLE INFO

Article history:
Received 30 July 2012
Received in revised form 11 November 2013
Accepted 16 November 2013
Available online 2 December 2013

Keywords:
Boolean function
Algebraic immunity
Nonlinearity

ABSTRACT

It is a difficult challenge to construct Boolean functions with good cryptographic properties. In this paper, we construct an infinite class of even-variable balanced functions with optimum algebraic degree, optimum algebraic immunity and very high nonlinearity (higher than all other known balanced functions with optimum algebraic immunity). For any balanced Boolean function with optimum algebraic immunity, it is still unknown what is the highest nonlinearity possible. We achieve a higher nonlinearity than previous methods which gives a new lower bound on the maximum possible nonlinearity of balanced Boolean functions with optimum algebraic immunity.

1. Introduction

In recent years, algebraic attacks have received a lot of attention in the cryptographic community. To resist algebraic attacks, Boolean functions used in stream ciphers should have high algebraic immunity. It is known that the maximum possible algebraic immunity of an n-variable Boolean function is $\lceil \frac{n}{2} \rceil$ [7].

Many classes of Boolean functions with optimum algebraic immunity have been introduced [1,4,10,11,17,18,22,23,26,29]. However, none of them has a good nonlinearity. In [5,13], an infinite class of n-variable balanced functions with optimum algebraic degree, optimum algebraic immunity and good nonlinearity was investigated. The lower bound on nonlinearity for this class of functions is $2^{n-1} - \frac{2^{n/2+1}}{\pi} \ln(\frac{4(2^n-1)}{\pi})$. However, this is not enough to resist fast correlation attacks [16,21]. In [24,27,31,33], more balanced Boolean functions with optimum algebraic degree, optimum algebraic immunity and good nonlinearity were investigated, their nonlinearity is good but not high too. In [28], Tu and Deng introduced an infinite class of even-variable balanced functions with optimum algebraic degree, optimum algebraic immunity and provably high nonlinearity. The lower bound on its nonlinearity is $2^{n-1} - 2^{n/2-1} - 2^{n/4}\frac{n}{2}\ln 2 - 1$, which is the best lower bound up to now.

In this paper, we construct an infinite class of even-variable Boolean functions with good cryptographic properties: balancedness, optimum algebraic degree, optimum algebraic immunity and very high nonlinearity. The lower bound on its nonlinearity is

$$\begin{cases} 2^{2k-1} - \dfrac{1}{2}\displaystyle\sum_{i=0}^{s} 2^{2^i} - 1, & \text{if } k = 2^s, \\ 2^{2k-1} - \dfrac{1}{2}\displaystyle\sum_{i=0}^{s} 2^{(2r-1)2^i} - 2^{r-1} - 2, & \text{if } k = (2r-1)2^s, \end{cases}$$

where $k = \frac{n}{2}$. Clearly, this bound is better than the bound given in [28].

* Corresponding author. Tel.: +65 85552483; fax: +65 68726840.
E-mail addresses: qcwang@fudan.edu.cn, tslwq@nus.edu.sg (Q. Wang), tsltch@nus.edu.sg (C.H. Tan).

0166-218X/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dam.2013.11.014

The paper is organized as follows. In Section 2, the necessary background is established. We introduce an infinite class of balanced functions with good cryptographic properties in Section 3. Section 4 concludes this paper.

2. Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2$. A Boolean function f of n variables is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, and it can be represented by the output column of its truth table, i.e.,

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

We denote B_n as the set of all n-variable Boolean functions.

Any Boolean function $f \in B_n$ can be uniquely represented as a multivariate polynomial in $\mathbb{F}_2[x_1,\dots,x_n]$,

$$f(x_1,\dots,x_n) = \sum_{K\subseteq\{1,2,\dots,n\}} a_K \prod_{k\in K} x_k, \quad a_K \in \mathbb{F}_2,$$

which is called its algebraic normal form (ANF). The algebraic degree of f, denoted by deg(f), is the number of variables in the highest order term with nonzero coefficient a_K.

A Boolean function is *affine* if there exists no term of degree strictly greater than 1 in the ANF and the set of all affine functions is denoted by A_n.

Let

$$1_f = \{x \in \mathbb{F}_2^n | f(x) = 1\}, \qquad 0_f = \{x \in \mathbb{F}_2^n | f(x) = 0\},$$

be the support of a Boolean function f and its complement respectively. The cardinality of 1_f is called the *Hamming weight* of f, and denoted by $wt(f)$. The *Hamming distance* between two functions f and g is the Hamming weight of $f+g$, and will be denoted by $d(f,g)$. We say that an n-variable Boolean function f is *balanced* if $wt(f) = 2^{n-1}$.

Let $f \in B_n$. The *nonlinearity* of f is the minimum distance between f and the set of all n-variable affine functions, i.e.,

$$nl(f) = \min_{g\in A_n} d(f,g).$$

The nonlinearity of an n-variable Boolean function is bounded above by $2^{n-1} - 2^{n/2-1}$, and a function is said to be *bent* if it achieves this bound. Clearly, bent functions exist only for even n and it is known that the algebraic degree of a bent function is bounded above by $\frac{n}{2}$ [2,9,12,25].

For any $f \in B_n$, a nonzero function $g \in B_n$ is called an *annihilator* of f if $fg = 0$, and the *algebraic immunity* of f, denoted by $\mathcal{AI}(f)$, is the minimum value of d such that f or $f+1$ admits an annihilator of degree d [20]. It is known that the algebraic immunity of an n-variable Boolean function is bounded above by $\lceil \frac{n}{2} \rceil$ [7]. To resist algebraic attacks, a Boolean function should have a high algebraic immunity.

The *Walsh transform* of a given function $f \in B_n$ is the integer-valued function over $\mathbb{F}_2^n$ defined by

$$W_f(\omega) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+\omega\cdot x},$$

where $\omega \in \mathbb{F}_2^n$ and $\omega\cdot x$ is an inner product, that is, $\omega\cdot x = \omega_1x_1 + \omega_2x_3 + \cdots + \omega_nx_n$. It is easy to see that a Boolean function f is balanced if and only if $W_f(0) = 0$. Moreover, the nonlinearity of f can be determined by

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{\omega\in\mathbb{F}_2^n} |W_f(\omega)|.$$

Let $g_1(x_1,\dots,x_n), g_2(x_1,\dots,x_n) \in B_n$. In terms of ANF, we define then

$$g_1 \parallel g_2 = (x_{n+1}+1)g_1 + x_{n+1}g_2 \in B_{n+1},$$

where $\parallel$ denotes the concatenation of two Boolean functions. Let $x = (x_1,\dots,x_k)$ and $y = (y_1,\dots,y_k)$. Any function $f(x,y) \in B_{2k}$ can be written as

$$f(x,z_0)c \parallel f(x,z_1) \parallel \cdots \parallel f(x,z_{2^k-1}),$$

where $z_i = (i_0,\dots,i_{k-1})$ and $i = \sum_{j=0}^{k-1} i_j2^j$, for $0 \le i \le 2^k-1$ and $i_j \in \mathbb{F}_2$. That is,

$$f(x,y) = \sum_{i=0}^{2^k-1} f(x,z_i)\prod_{j=1}^{k}(y_j + i_{j-1} + 1).$$

For example, let $f(x,y) \in B_4$. Then

$$f(x,y) = f(x,0,0) \parallel f(x,1,0) \parallel f(x,0,1) \parallel f(x,1,1).$$

In terms of ANF, we have $f(x,y) =$

$$f(x,0,0)(y_1+1)(y_2+1) + f(x,1,0)y_1(y_2+1) + f(x,0,1)(y_1+1)y_2 + f(x,1,1)y_1y_2.$$