Information Sciences 283 (2014) 94–106

Contents lists available at ScienceDirect

Information Sciences

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

Secondary constructions of highly nonlinear Boolean functions and disjoint spectra plateaued functions

Feng-rong Zhang [a],*, Claude Carlet [b], Yu-pu Hu [c], Tian-jie Cao [a]

[a] School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, PR China
[b] LAGA, UMR 7539, CNRS, Universities of Paris 8 and Paris 13, 93526 Saint-Denis cedex 02, France
[c] State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, PR China

ARTICLE INFO

Article history:
Received 31 July 2013
Received in revised form 25 April 2014
Accepted 9 June 2014
Available online 26 June 2014

Keywords:
Boolean function
Resilient function
Bent function
High nonlinearity

ABSTRACT

In this paper, we modify a generalized indirect sum construction to construct functions with high nonlinearity. By utilizing the modified construction, highly nonlinear functions in $(n+m)$ variables can be obtained from known bent functions in n variables and highly nonlinear functions in m variables. It is possible to obtain new $(n+15)$-variable functions with nonlinearity $2^{n+15-1} - 2^{(n+15-1)/2} + 20 \times 2^{n/2}$ and new 12-variable 2-resilient functions with nonlinearity 2000 and algebraic degree 8, which achieve optimal algebraic immunity. Moreover, the modified construction can also be used as an iterative construction of a quadruple of disjoint spectra plateaued functions. In addition, we present sufficient conditions for a quadruple of disjoint spectra plateaued functions to have no nonzero linear structure.

© 2014 Elsevier Inc. All rights reserved.

1. Introduction

Boolean functions play important roles in both conventional cryptography and error correcting codes [8]. Over the last decades, Boolean functions satisfying some particular cryptographic criteria (such as high nonlinearity and high algebraic immunity) have been studied [1,5,16,17,28,29,32,33].

In terms of constructions of Boolean functions, there are two kinds of constructions: primary constructions (designing functions without using known ones) and secondary constructions (designing functions with using known ones). Certainly, the constructions of resilient functions are no exception. The primary constructions mainly include Maiorana–McFarland's construction [1], its generalizations [5], Dobbertin's construction [14], and other constructions [15,33]. Besides, secondary constructions mainly include direct sum of functions [29], Siegenthaler's construction [29], Tarannikov's elementary construction [30], indirect sum of functions [6] and constructions without extension of the number of variables [7]. Many highly nonlinear functions can be constructed by using the above constructions. The constructions of plateaued functions (including bent functions) also include primary constructions [13,14,34] and secondary constructions [11].

Parseval's relation [22] implies that the nonlinearity of an n-variable function is less than or equal to $2^{n-1} - 2^{\frac{n}{2}-1}$. For n even, there exist functions whose nonlinearity is equal to this upper bound. The corresponding functions are called bent [27]. However, although many concrete constructions of bent functions [3,11] have been discovered, the general structure of bent functions is still unclear. In particular a complete classification of bent functions seems hopeless today.

* Corresponding author. Tel.: +86 15152451689.
E-mail addresses: zhfl203@163.com (F.-r. Zhang), claude.carlet@univ-paris8.fr (C. Carlet), yphu@mail.xidian.edu.cn (Y.-p. Hu), tjcao@cumt.edu.cn (T.-j. Cao).

http://dx.doi.org/10.1016/j.ins.2014.06.024
0020-0255/© 2014 Elsevier Inc. All rights reserved.

In odd number of input variables n, the evaluation of the maximum nonlinearity of Boolean functions remains an open problem. For n odd, the best known upper bound on the nonlinearities of n-variable Boolean functions is $2\left\lfloor 2^{n-2} - 2^{\frac{n}{2}-2}\right\rfloor$ [18], where $\lfloor n/2 \rfloor$ denotes the largest integer smaller than or equal to $n/2$. It has been shown in [23] that it equals $2^{n-1} - 2^{\frac{n-1}{2}}$ (which is also called *bent-concatenation bound* since it can be achieved by the concatenation of two bent functions in $n-1$ variables) when $n = 1, 3, 5, 7$, and in [25,26], by Patterson and Wiedemann, that it is strictly larger than $2^{n-1} - 2^{\frac{n-1}{2}}$ if $n \geqslant 15$ (see also [20]). More recently it has been proved in [19] that the best nonlinearity of Boolean functions in odd numbers of variables is strictly greater than the bent-concatenation bound for any $n > 7$. Additionally, balanced functions with nonlinearity strictly greater than the bent-concatenation bound are also presented in [15] for $n \geqslant 35$. These results motivate us to find more Boolean functions whose nonlinearities are strictly greater than the bent-concatenation bound.

In this paper, we modify a generalization of the indirect sum, which was introduced and used in [11] to construct bent functions, for constructing Boolean functions with high nonlinearity. We study the relationships between the nonlinearities of the constructed functions and those of the initial functions. Utilizing Theorem 3.2, it is possible to obtain $(n+15)$-variable functions with nonlinearity $2^{n+15-1} - 2^{(n+15-1)/2} + 20 \times 2^{n/2}$ from PW functions (Patterson and Wiedemann in [25] proposed 15-variable Boolean functions with nonlinearity $2^{14} - 2^{7} + 20$, which are called PW functions). Further, we can obtain new 12-variable 2-resilient functions with nonlinearity 2000 and algebraic degree 8, and which achieve optimal algebraic immunity. These constructed functions are different with the functions constructed by the direct sum and the indirect sum constructions. We can also obtain a quadruple of disjoint spectra functions in $n+m$ variables which are $(n + 2\lfloor \frac{m-2}{2} \rfloor)$th-order plateaued functions and have no nonzero linear structure. These constructed disjoint spectra plateaued functions can also be used as the initial functions of Theorem 4.1.

The rest of the paper is organized as follows. Section 2 introduces cryptographic criteria relevant for Boolean functions. In Section 3, we provide a generalization of the indirect sum construction for constructing highly nonlinear functions. In Section 4, a quadruple of disjoint spectra plateaued functions is proposed. At last, some conclusions are given in Section 5.

2. Preliminaries

In the remainder of this paper, we denote the addition over the finite field $\mathbb{F}_2$ by $\oplus$. Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$, and B_n be the set of all n-variable Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. A basic representation of a Boolean function $f(x_1, \ldots, x_n)$ is by the output column of its truth-table, i.e., a binary string of length 2^n,

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

The *Hamming weight* wt (f) of a Boolean function $f \in B_n$ is the weight of the above binary string. We say a Boolean function f is *balanced* if its Hamming weight equals 2^{n-1}. The *Hamming distance* $d(f, g)$ between two Boolean functions f and g is the Hamming weight of their difference $f \oplus g$.

Any Boolean function has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form*(ANF):

$$f(x_1, \ldots, x_n) = \bigoplus_{I \subseteq \{1,2,\ldots,n\}} a_I \prod_{l \in I} x_l$$

where $a_I \in \mathbb{F}_2$, and the terms $\prod_{l \in I} x_l$ are called monomials. The *algebraic degree* $\deg(f)$ of a Boolean function f equals the maximum degree of those monomials whose coefficients are nonzero in its ANF. A Boolean function is affine if it has algebraic degree at most 1. The set of all n-variable affine functions is denoted by A_n. An n-variable affine function with constant term 0 is a linear function, and can be represented as $\omega \cdot x = \omega_1 x_1 \oplus \ldots \oplus \omega_n x_n$ where $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{F}_2^n, x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$.

The *nonlinearity* of $f \in B_n$ is its distance to the set of all n-variable affine functions, i.e.,

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

Boolean functions used in cryptographic systems must have high nonlinearity to withstand linear and fast correlation attacks [2].

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

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

In terms of Walsh spectrum, the nonlinearity of f is given by

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

Parseval's equation [22] states that $\sum_{\omega \in \mathbb{F}_2^n} (W_f(\omega))^2 = 2^{2n}$ and implies that

$$N_f \leqslant 2^{n-1} - 2^{n/2-1}.$$

Download English Version:

https://daneshyari.com/en/article/6857692

Download Persian Version:

https://daneshyari.com/article/6857692

Daneshyari.com