Discrete Applied Mathematics 215 (2016) 197–202

Contents lists available at ScienceDirect

Discrete Applied Mathematics

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

On the second-order nonlinearity of the hidden weighted bit function

Qichun Wang*, Chik How Tan

Temasek Laboratories, National University of Singapore, Singapore 117411, Singapore

ARTICLE INFO

Article history:
Received 28 March 2016
Received in revised form 22 June 2016
Accepted 24 June 2016
Available online 22 July 2016

Keywords:
Boolean function
Hidden weighted bit function
Nonlinearity
Second-order nonlinearity

ABSTRACT

The hidden weighted bit function (HWBF) is a well-known benchmark function in the branching program literature. In Wang et al. (2014),authors investigated the cryptographic properties of the HWBF and found that it seems to be a very good candidate for being used in real ciphers. In this paper, we make the following contributions:

(1) We study the behavior of the HWBF against the quadratic approximation attack and give an upper bound on its second-order nonlinearity, which is much lower than the maximum possible second-order nonlinearity of Boolean functions. Therefore, the HWBF may be weak for being used in real ciphers to resist quadratic approximation attacks. But, how to launch the quadratic approximation attack effectively is still in the research stage.

(2) Two bounds on the higher-order nonlinearities were given by C. Carlet in Carlet (2008). In general, one bound is better than the other one. But it was unknown whether it is always better. We give an example to show that it is not always better.

1. Introduction

The hidden weighted bit function (HWBF) is a well-known benchmark function in the branching program literature [15]. It was introduced by Bryant in 1991 [2], and revisited by Knuth in [18], which seems to be the simplest one with exponential binary decision diagram (BDD) size [1].

In [27], Wang et al. investigated the cryptographic properties of the HWBF and found that it has overall very good cryptographic properties: balancedness, optimum algebraic degree, strict avalanche criterion, good algebraic immunity, good nonlinearity and good behavior against fast algebraic attacks. It seems to be a very good candidate for being used in real ciphers. In fact, very few functions have been found so far that can resist all the main known attacks, and except the HWBF, none of them is very efficiently implementable. Based on the HWBF, more functions with good cryptographic properties have been constructed in [30,29].

The second-order nonlinearity can be used to assess the behavior of a Boolean function against the quadratic approximation attack [14,16,17,21]. But it is usually difficult to compute the second-order nonlinearity of a Boolean function [8,10–13,19,20,24,25]. In this paper, we will study the behavior of the HWBF against the quadratic approximation attack and give an upper bound on its second-order nonlinearity, which is much lower than the maximum possible second-order nonlinearity of Boolean functions. Therefore, the HWBF may be weak for being used in real ciphers to resist quadratic approximation attacks. But, how to launch the quadratic approximation attack effectively is still in the research stage.

Moreover, two bounds on the higher-order nonlinearities were given by Carlet in [4]. In general, one bound is better than the other one. But it was unknown whether it is always better. We give an example to show that it is not always better.

* Corresponding author.
E-mail addresses: tslwq@nus.edu.sg (Q. Wang), tsltch@nus.edu.sg (C.H. Tan).

http://dx.doi.org/10.1016/j.dam.2016.06.020
0166-218X/

The paper is organized as follows. In Section 2, the necessary background is established. We give an upper bound on the second-order nonlinearity of the HWBF in Section 3. In Section 4, we give an example to show that one bound given by Carlet is not always better than the other one. We end in Section 5 with conclusions.

2. Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2$. We denote by B_n the set of all n-variable Boolean functions, from $\mathbb{F}_2^n$ into $\mathbb{F}_2$.

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

$$f(x_1, \ldots, x_n) = \sum_{K \subseteq \{1,2,\ldots,n\}} a_K \prod_{k \in K} x_k,$$

which is called 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 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

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

The set 1_f is called the support of f, and its cardinality $|1_f|$ is called the *Hamming weight* of 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 its Hamming weight is 2^{n-1}.

Let $f \in B_n$. The *nonlinearity* of f is its minimum distance from 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 $\frac{n}{2}$ [5,9]. The *r-order nonlinearity*, denoted by $nl_r(f)$, is its distance from the set of all n-variable functions of algebraic degrees at most r. The maximum possible r-order nonlinearity of n-variable Boolean functions is called the *covering radius* of the Reed–Muller code $RM(r, n)$ [7]. For $n \geq 7$, the exact covering radius of $RM(2, n)$ is still unknown [6,21,26].

3. On the second-order nonlinearity of the hidden weighted bit function

The *hidden weighted bit function* (HWBF) $h \in B_n$ is defined as follows [2]:

$$h(x) = \begin{cases} 0 & \text{if } x = 0, \\ x_{wt(x)} & \text{otherwise,} \end{cases}$$

where $x = (x_1, x_2, \ldots, x_n)$ and $wt(x) = x_1 + x_2 + \cdots + x_n$. In the following, we will deduce an upper bound on its second-order nonlinearity.

Theorem 1. *Let h be the HWBF defined on $\mathbb{F}_2^n$. Then*

$$nl_2(h) \leq 2^{n-1} - 2\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}.$$

Proof. We divide the proof into the following two cases.

Case 1: $n = 4m + 1$ or $n = 4m + 2$, where $m \in \mathbb{Z}$.

We construct an n-variable Boolean function

$$g_1(x) = (x_{2m} + x_{2m+1}) \sum_{i=1}^{n} x_i + x_{2m}.$$

Clearly, $\deg(g_1) = 2$. We have

$$\begin{aligned} \sum_{x \in \mathbb{F}_2^n} (-1)^{h(x)+g_1(x)} &= \sum_{\substack{x \in \mathbb{F}_2^n \\ wt(x) \text{ odd}}} (-1)^{x_{wt(x)}+x_{2m+1}} + \sum_{\substack{x \in \mathbb{F}_2^n \\ wt(x) \text{ even}}} (-1)^{x_{wt(x)}+x_{2m}} \\ &= 2^{n-1} - 2\left| \bigcup_{\substack{i=1 \\ i \text{ odd}}}^{n} \{x \in \mathbb{F}_2^n \mid wt(x) = i \text{ and } x_i + x_{2m+1} = 1\} \right| \\ &\quad + 2^{n-1} - 2\left| \bigcup_{\substack{i=1 \\ i \text{ even}}}^{n} \{x \in \mathbb{F}_2^n \mid wt(x) = i \text{ and } x_i + x_{2m} = 1\} \right|. \end{aligned}$$