HAL open science

Symmetric Boolean functions with high nonlinearity

Marion Videau

To cite this version:

Marion Videau. Symmetric Boolean functions with high nonlinearity. WEWoRC 2005 - Western European Workshop on Research in Cryptplogy, Jul 2005, Leuven, Belgium. pp.87-88. hal-00675349

HAL Id: hal-00675349

https://inria.hal.science/hal-00675349v1

Submitted on 29 Feb 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Symmetric Boolean functions with high nonlinearity

Marion Videau

INRIA-Rocquencourt, projet CODES
http://www-rocq.inria.fr/codes/
marion.videau@inria.fr

Abstract. It is known that the symmetric Boolean functions with optimal nonlinearity are the quadratic functions. Here, we extend this work and we characterise the functions with suboptimal nonlinearity by using the link between the periodicity of their simplified value vectors and their algebraic degrees.

Keywords. Boolean functions, symmetric functions, nonlinearity

1 Introduction

Symmetric Boolean functions can be easily represented by reduced versions of their value vectors and of their algebraic normal forms. Besides this conciseness, they are also good functions in terms of gate complexity [Weg87]. These properties make them be interesting candidates to be used in many applications. Unfortunately, it has been proved that their nonlinearities and algebraic degrees which are important cryptographic parameters, cannot be simultaneously maximised. However symmetric functions with suboptimal nonlinearity might be of interest for designing cryptographic primitives.

Definition 1.1 *A Boolean function f is* symmetric *if its output is invariant under any permutation of its input bits :*

$$f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}), \quad \textit{for all permutations } \sigma \textit{ of } \{1,\ldots,n\} \ .$$

It means that there exists a function $v_f : \{0, \ldots, n\} \to \mathbf{F}_2$ such that $\forall x \in \mathbf{F}_2^n, f(x) = v_f(wt(x))$. We will refer to the sequence $v(f) = (v_f(0), \ldots, v_f(n))$ as the simplified value vector *of f.*

Proposition 1.1 *A Boolean function f of n variables is symmetric if and only if its algebraic normal form can be written as*

$$f(x_1, \ldots, x_n) = \bigoplus_{i=0}^{n} \lambda_f(i) \bigoplus_{\substack{u \in \mathbf{F}_2^n \\ wt(u)=i}} \prod_{j=1}^{n} x_j^{u_j}, \ \lambda_f(i) \in \mathbf{F}_2^n.$$

We call the $(n+1)$-bit vector $\lambda(f) = (\lambda_f(0), \lambda_f(1), \ldots, \lambda_f(n))$ the simplified ANF vector *of f.*

It is proved in [CV05] that low degree symmetric functions have a periodic simplified value vector.

Theorem 1.2 *Let f be a symmetric Boolean function of n variables with simplified ANF vector $\lambda(f) = (\lambda_0, \ldots, \lambda_n)$ and simplified value vector $v(f) = (v_0, \ldots, v_n)$.*

Then, $v(f)$ is periodic with period 2^t if and only if $\deg(f) \leq 2^t - 1$. Moreover, $(v_0, \ldots, v_{2^t-1})$ is the simplified value vector of the symmetric Boolean function of (2^t-1) variables with $(\lambda_0, \ldots, \lambda_{2^t-1})$ as simplified ANF vector.

We recall the notation for the Walsh coefficients and the nonlinearity of a Boolean function f. If we denote a linear function by $\varphi_a : x \mapsto a \cdot x$, then

$$\mathcal{F}(f + \varphi_a) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+a\cdot x}, \ \mathcal{L}(f) = \max_{a \in \mathbf{F}_2^n} \mid \mathcal{F}(f + \varphi_a) \mid, \ \text{ and } \mathcal{NL}(f) = 2^{n-1} - \frac{\mathcal{L}(f)}{2} \ .$$

2 Highly nonlinear symmetric Boolean functions

The maximum nonlinearity for symmetric functions of n variables has been proved to be reached only by quadratic functions. More precisely, when n is even, these functions are bent and the nonlinearity is $2^{n-1} - 2^{\frac{n}{2}-1}$[Sav94] and when n is odd, the maximal nonlinearity is $2^{n-1} - 2^{\frac{n-1}{2}}$ [MS02]. In this section we investigate cases of suboptimal nonlinearity and we point out that the nonlinearity is related to the periodicity of the simplified value vector.

Theorem 2.1 *Let f be a symmetric Boolean function of n variables. If $\mathcal{L}(f) < 2^{\lfloor \frac{n+1}{2} \rfloor} + 2^{t+1}$ for some integer t, $0 \leq t < \lfloor \frac{n+1}{2} \rfloor$, then*

$$v_f(i+2) = v_f(i) \oplus 1, \text{ for all } t \leq i \leq n-2-t \ ,$$

or equivalently $f = q + h$ where q is a symmetric quadratic function and h is a symmetric function of n variables such that $v_h(i) = 0$ for all $t \leq i \leq n-t$.

This can be proved by induction on t using the properties of periodicity of the restrictions of a symmetric Boolean function [CV05].

As a direct corollary, we can deduce a necessary condition on the simplified value vector of the symmetric functions f with $\mathcal{L}(f) < 2^{\lfloor \frac{n+1}{2} \rfloor + 1}$.

Corollary 2.2 *Let f be a symmetric Boolean function of n variables.*

- *For n even, if $v_f(\frac{n}{2} - 1) = v_f(\frac{n}{2} + 1)$, then $\mathcal{L}(f) \geq 2^{\frac{n}{2}+1}$.*
- *For n odd, if $v_f(\frac{n+1}{2}) = v_f(\frac{n-3}{2})$ or if $v_f(\frac{n+3}{2}) = v_f(\frac{n-1}{2})$, then $\mathcal{L}(f) \geq 2^{\frac{n+1}{2}+1}$.*

Theorem 2.1 also points out that the resiliency order of a highly nonlinear symmetric function is limited.

Corollary 2.3 *Let f be a symmetric Boolean function of n variables such that $\mathcal{L}(f) < 2^{\lfloor \frac{n+1}{2} \rfloor} + 2^{t+1}$ for some integer t, $0 \leq t < \lfloor \frac{n+1}{2} \rfloor$. Then, f is at most $(2t+2)$-resilient.*

Now, we can characterise the symmetric functions whose nonlinearity is very close to the optimal nonlinearity.

Proposition 2.1 *The symmetric Boolean functions f of n variables such that $\mathcal{L}(f) = 2^{\lfloor \frac{n+1}{2} \rfloor} + 2$ are the 8 functions of degree n defined by the following simplified ANF vectors:*

$$\lambda_f = (a, b, 1, 0, \ldots, 0, 1) \ \text{ and } \ \lambda_f = (a, b, 0, 1, \ldots, 1, 1), \ a, b \in \mathbf{F}_2.$$

Proposition 2.2 *The symmetric Boolean functions f of n variables such that $\mathcal{L}(f) = 2^{\lfloor \frac{n+1}{2} \rfloor} + 4$ are the 4 functions of degree $(n-1)$ defined by the following simplified ANF vectors:*

$$\lambda_f = (a, b, 0, 1, \ldots, 1, 0), \ a, b \in \mathbf{F}_2 \ .$$

References

[CV05] A. Canteaut and M. Videau, Symmetric Boolean functions, *IEEE Trans. Inform. Theory.* — Regular paper, to appear.

[MS02] S. Maitra and P. Sarkar, Maximum nonlinearity of symmetric Boolean functions on odd number of variables, *IEEE Trans. Inform. Theory*, vol. 48, no. 9, 2002.

[Sav94] P. Savicky, On the bent functions that are symmetric, *European J. of Combin.*, vol. 15, pp. 407–410, 1994.

[Weg87] I. Wegener, *The complexity of Boolean functions.* Wiley, 1987.