Information Processing Letters 112 (2012) 811–815

Contents lists available at SciVerse ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

On multiple output bent functions

E. Pasalic [a,*], W.G. Zhang [b]

[a] University of Primorska, FAMNIT and IAM, Koper 6000, Slovenia
[b] ISN Laboratory, Xidian University, Xi'an 710071, China

ARTICLE INFO

Article history:
Received 25 April 2012
Received in revised form 26 June 2012
Accepted 2 July 2012
Available online 20 July 2012
Communicated by A. Tarlecki

Keywords:
Cryptography
Boolean functions
Bent functions
Multiple output
Monomial trace functions

ABSTRACT

In this article we investigate the possibilities of obtaining multiple output bent functions from certain power polynomials over finite fields. So far multiple output bent functions $F : GF(2)^n \to GF(2)^m$ (where n is even and $m \leqslant n/2$), for any particular class of Boolean bent functions, has been generated using a suitable collection of m Boolean bent functions so that any nonzero linear combination of these functions is again bent. Here, we take a different approach by deriving these functions directly from the known classes of so-called monomial trace bent functions. We derive a sufficient condition for a bent Boolean function of the form $f(x) = Tr_1^n(\lambda x^d)$ so that the associated mapping $F(x) = Tr_m^n(\lambda x^d)$, where $F : GF(2)^n \to GF(2)^m$, is a multiple output bent function. We consider all the main cases of monomial trace bent functions and specify the restrictions on λ and m that yield multiple output bent functions $F(x) = Tr_m^n(\lambda x^d)$. Interestingly enough, in one particular case when $n = 4r$, $d = (2^r + 1)^2$, a multiple bent function $F(x) = Tr_{2r}^n(ax^d)$ could not be obtained by considering a collection of $2r$ Boolean bent functions of the form $f_i(x) = Tr_1^n(\lambda_i x^d)$ for some suitable coefficients $\lambda_i \in GF(2^n)$.

1. Introduction

Bent functions are extremal combinatorial objects with several areas of application, such as coding theory, maximum length sequences, cryptography, the theory of difference sets to name a few. The term bent Boolean function was introduced by Rothaus [16], where also two classes of bent functions were considered. One of this classes is defined by $f(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$ for all $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$, which was later generalized by Maiorana–McFarland. Another pioneering work on bent functions is due to Dillon [9], who introduced and analyzed another important class of bent functions called partial spread. In 1994, Carlet [4] gave two new classes ($\mathcal{C}$ and $\mathcal{D}$) of bent functions. These combinatorial objects were later extensively studied in many articles, see e.g. [5,2,10], and though there are numerous results on the classification of these functions the work has not been completed yet.

Among other equivalent characterization of bent functions, the one that is most often used is a characterization of Bent functions as a class of Boolean functions having so-called flat Walsh spectra. It means that for any bent function over $GF(2)^n$, its Hamming distance to any affine function in n variables is constant including the distance to the all-zero function (or all-one function). The same characterization of Boolean bent functions is easily generalized by requesting that all nonzero linear combinations of the component functions of $F : GF(2)^n \to GF(2)^m$ are also bent. The construction of such *multiple output bent functions* have been initially considered by Nyberg in [15]. It has been shown in [15] that multiple output bent functions can only exist for $m \leqslant n/2$, and can be constructed using some known classes of bent functions, namely the Maiorana–McFarland class and the Dillon's partial spread class. The same problem has also been treated in [17] and more recently in [11]. What is common to all these approaches is the underlying idea of specifying m bent Boolean functions

* Corresponding author.
E-mail addresses: enes.pasalic6@gmail.com (E. Pasalic), w.g.zhang@qq.com (W.G. Zhang).

0020-0190/$ – see front matter
http://dx.doi.org/10.1016/j.ipl.2012.07.009

in a particular way so that their linear combinations remain bent. On the other hand, it might be true that these component functions may be obtained directly by applying a suitable trace mapping to certain polynomials over finite fields.

In this work we investigate field mappings of the form $f(x) = ax^d$, $a \in GF(2^n)$ for which a standard approach of taking the absolute trace $Tr_1^n : GF(2^n) \to GF(2)$ yields Boolean bent functions. Thus, for a given monomial f over $GF(2^n)$ we consider its associated function $F(x) = Tr_m^n(f(x))$ mapping $GF(2^n)$ onto $GF(2^m)$. In other words, instead of satisfying various conditions on the component functions of F we attempt to obtain multiple bent functions directly. Since all the known classes of trace bent functions are either given in monomial or binomial form (where only one respectively two of the coefficients a_i's of $f(x)$ are nonzero) we confine ourselves to these cases. We derive a sufficient condition on λ and m so that for a bent function $f(x) = Tr_1^n(\lambda x^d)$ its associated function $F(x) = Tr_m^n(\lambda x^d)$ is a multiple output bent function. Several cases of known Boolean trace bent monomials are analyzed with respect to the above condition and the existence of multiple bent functions is confirmed. Interestingly enough, in one particular case when $n = 4r$, $d = (2^r + 1)^2$, a multiple bent function $F(x) = Tr_{2r}^n(ax^d)$ could not be obtained by considering a collection of $2r$ Boolean bent functions of the form $f_i(x) = Tr_1^n(a_i x^d)$ for some suitable coefficients $a_i \in GF(2^n)$.

The rest of this article is organized as follows. In Section 2 some basic definitions are introduced. A sufficient condition that a bent function $f(x) = Tr_1^n(\lambda x^d)$ gives rise to a multiple output bent function $F(x) = Tr_m^n(\lambda x^d)$ is discussed in Section 3. In Section 4, the known classes of monomial trace bent functions are analyzed with respect to the possibility of obtaining multiple output bent functions from these classes. Finally, some concluding remarks are given in Section 5.

2. Preliminaries

Let $\mathbb{F}_{2^n}$ denote the finite Galois field $GF(2^n)$ consisting of 2^n elements. The group of units of $\mathbb{F}_{2^n}$, denoted by $\mathbb{F}_{2^n}^*$, is a cyclic group consisting of $2^n - 1$ elements. An element $\alpha \in \mathbb{F}_{2^n}$ is said to be a primitive element if it is a generator of the multiplicative group $\mathbb{F}_{2^n}^*$. Once the basis of the field is fixed, say $(\gamma_0, \ldots, \gamma_{n-1})$ so that $\alpha = \alpha_0\gamma_0 + \cdots + \alpha_{n-1}\gamma_{n-1}$, where $\gamma_i \in \mathbb{F}_{2^n}$ and $\alpha_i \in \mathbb{F}_2$, there is a natural isomorphism between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$ given by

$$\alpha_0\gamma_0 + \cdots + \alpha_{n-1}\gamma_{n-1} \in \mathbb{F}_{2^n} \mapsto (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{F}_2^n.$$

Any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a Boolean function on n variables. The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$.

The trace function $Tr_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, a mapping to a subfield $\mathbb{F}_{2^m}$ when $m|n$, is defined as

$$Tr_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{(n/m-1)m}}, \quad \text{for all } x \in \mathbb{F}_{2^n}. \tag{1}$$

The absolute trace $Tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$, also denoted by Tr, then maps to the prime field. The trace representation [12] of any function $f \in \mathcal{B}_n$ is

$$f(x) = \sum_{k \in \Gamma(n)} Tr_1^{n_k}\left(A_k x^k\right) + A_{2^n-1}x^{2^n-1}, \quad \text{for all } x \in \mathbb{F}_{2^n}, \tag{2}$$

where $\Gamma(n)$ is the set of all coset leaders modulo $2^n - 1$ and $A_k \in \mathbb{F}_{2^{n_k}}$, $A_{2^n-1} \in \mathbb{F}_2$, for all $k \in \Gamma(n)$. A Boolean function is said to be a *monomial trace function* or said to have a *monomial trace representation* if its trace representation consists of only one trace term.

The Walsh–Hadamard transform of a Boolean function $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined by

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\lambda x)}. \tag{3}$$

The multiset

$$\left\{W_f(\lambda) \colon \lambda \in \mathbb{F}_{2^n}\right\} \tag{4}$$

is said to be the Walsh–Hadamard spectrum of the Boolean function f. For any even positive integer $n = 2m$, there exist Boolean functions with a "flat" Walsh–Hadamard spectra. A function $f \in \mathcal{B}_n$ is called bent if and only if $|W_f(\lambda)| = 2^m$ for all $\lambda \in \mathbb{F}_{2^n}$. It is known that the bent functions provide maximum resistance to linear approximations and therefore play a major role in construction of cryptographic Boolean functions.

The nonlinearity of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and hereby the resistance to linear cryptanalysis of Matsui [14] is measured through extended Walsh transform defined as,

$$W_F(\sigma, \gamma) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\gamma F(x))+Tr_1^n(\sigma x)}, \quad \sigma \in \mathbb{F}_{2^n},\ \gamma \in \mathbb{F}_{2^m}^*. \tag{5}$$

Here, $\gamma \in \mathbb{F}_{2^m}^*$ selects nonzero linear combinations of the component functions of F, since $F(x) = (f_1(x), \ldots, f_m(x))$ where $f_i : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Using this representation via component functions, a multiple output bent function over $\mathbb{F}_{2^m}$ is defined for $m \leqslant n/2$ so that $a_1 f_1(x) + \cdots + a_m f_m(x)$ is a bent function for any choice of $a_i \in \mathbb{F}_2$, where not all of the a_i's are zero.

3. Multiple output bent functions from trace bent functions

Some interesting classes of Boolean bent functions were derived using trace representation, i.e., $f(x) = Tr(F(x))$ for a suitably chosen polynomial $F(x)$ in the polynomial ring $\mathbb{F}_{2^n}[x]$. Since the extended Walsh transform is hard to compute for arbitrary F mostly monomial and binomial trace functions have been studied, see e.g. [7,13,1,6,10,18]. These classes of Boolean bent functions are defined as $Tr(ax^{d_1} + bx^{d_2})$ for suitably chosen coefficients $a, b \in \mathbb{F}_{2^n}$ and integer-valued exponents d_1, d_2. In the case $b = 0$ such a function is called monomial trace function, otherwise if $a, b \neq 0$ it is called a binomial trace function.