Publication I

Kaisa Nyberg and Miia Hermelin. 2007. Multidimensional Walsh transform and a characterization of Bent functions. In: P. Vijay Kumar, Tor Helleseth, and Øyvind Ytrehus (editors). Proceedings of the 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks (ITW 2007). Bergen, Norway. 1-6 July 2007. Pages 83-86.

Multidimensional Walsh Transform and a Characterization of Bent Functions

Kaisa Nyberg
Helsinki University of Technology and Nokia Research Center
kaisa.nyberg@tkk.fi
Miia Hermelin
Helsinki University of Technology
miia.hermelin@tkk.fi

***Abstract*—In this paper, a multidimensional Walsh transform is used to obtain a characterization of vector-valued bent function in terms of the value distributions of the translates of the function by linear functions.**

I. Introduction

S-boxes are fundamental building blocks in contemporary cryptography and typically the only source of nonlinearity in ciphers. Several cryptanalytic methods exploiting linearity properties have been developed, most prominently differential and linear cryptanalysis and their variations. Therefore research on nonlinearity criteria of S-boxes is an important area of contemporary cryptology.

When analyzed mathematically, S-boxes are considered as vector-valued functions the components of which are Boolean functions. The nonlinearity criteria of S-boxes have been investigated by means of the nonlinearity properties of their Boolean components. For example, a vector-valued function is called bent if all its components (non-zero linear combinations of its coordinate functions) are bent. Similarly, a vector-valued function is perfect nonlinear is all its components are perfect nonlinear [1]. When studying correlation with linear functions, autocorrelation properties, propagation characteristics and value distributions of Boolean functions, the Walsh transform is a fundamental tool. In particular it is very effective in handling interaction between different nonlinearity criteria, see for example [2], [3], [4].

In this paper, for the first time to our knowledge, we investigate nonlinearity criteria for vector-valued Boolean functions without making use of properties of components. We introduce, for this purpose, a tool which we call multi-Walsh transform. This tool is very effective in computation and analysis of value distributions of vector-valued Boolean functions. One area of application of multi-Walsh transform is in linear cryptanalysis when multiple linear approximations are used simultaneously. In this paper, we focus on vector-valued bent functions and show that for a bent function, the maximum variance of the value distribution of the sum of the function and a linear function is the least possible, where the maximum is taken over all linear functions.

For simplicity, we restrict to the binary case. It is straightforward to generalize the results given in this paper to the p-ary case, for any odd prime p.

The rest of the paper is organized as follows. First we introduce notation and recall known facts of bent functions in Section II. In Section III we give a brief overview of the basic methods in component-wise analysis of vector-valued Boolean functions. In Section IV we present the multidimensional Walsh transform and prove the equivalent of Parseval's theorem for it. Then the definition of multi-bent function is given in Section V and its equivalence with the definitions of bent and perfect nonlinear functions are given in the next two sections. In Section VIII we conclude.

II. Boolean Functions

Let n be a positive integer. We denote by V_n the vector space formed by binary vectors $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ of n coordinates $\xi_i \in \{0,1\}$, $i = 1, \ldots, n$. A function $f : V_n \to V_1$ is called a Boolean function. Given two vectors $\xi = (\xi_1, \xi_2, \ldots, \xi_n) \in V_n$ and $u = (u_1, u_2, \ldots, u_n) \in V_n$ we denote $u \cdot \xi = u_1 \cdot \xi_1 + u_2 \cdot \xi_2 + \ldots + u_n \cdot \xi_n \in V_1$. The Walsh transform $\mathcal{F}(f)$ maps f to an integer and is defined as

$$\mathcal{F}(f) = \sum_{\xi \in V_n} (-1)^{f(\xi)}, \tag{1}$$

where the sum is taken in the set of integers. A Boolean function is balanced if $\mathcal{F}(f) = 0$. Given $f : V_n \to V_1$ and $w \in V_n$ we denote by $f + w$ the Boolean function $(f + w)(\xi) = f(\xi) + w \cdot \xi$. Parseval's theorem states that

$$\sum_{w \in V_n} \mathcal{F}^2(f + w) = 2^{2n}. \tag{2}$$

A Boolean function $f : V_n \to V_1$ is called bent if $|\mathcal{F}(f+w)| = 2^{\frac{n}{2}}$, for all $w \in V_n$. Hence bent functions exist only if n is even. A Boolean function is called perfect nonlinear, if for all $\alpha \in V_n$, $\alpha \neq 0$, the function $D_\alpha f : \xi \mapsto f(\xi + \alpha) + f(\xi)$ is balanced. It is known since the invention of bent functions by Oscar Rothaus [5] that a Boolean function is bent if and only it is perfect nonlinear.

III. Vector-Valued Boolean Functions

Let $f : V_n \to V_m$ be a vector-valued Boolean function. We denote its coordinate functions by f_i, $i = 1, 2, \ldots, m$. Given $u \in V_m$, $u \neq 0$, the Boolean function $u \cdot f$ defined as $u \cdot f(\xi) = u_1 f_1(\xi) + \ldots u_m f_m(\xi)$ is called a (non-zero) component of f.

We begin by recalling a fundamental fact about the value distribution of f. Let $f : V_n \to V_m$ be a vector-valued Boolean function and $\eta \in V_m$. We make the following notation

$$a_\eta(f) = \#\{\xi \in V_n \,|\, f(\xi) = \eta\}.$$

Lemma 1: Let $f : V_n \to V_m$ be a vector-valued Boolean function. Then

$$a_\eta(f) = 2^{-m} \sum_{u \in V_m} \sum_{\xi \in V_n} (-1)^{u \cdot f(\xi) + u \cdot \eta}. \qquad (3)$$

Proof:

$$\begin{aligned} &\sum_{u \in V_m} \sum_{\xi \in V_n} (-1)^{u \cdot f(\xi) + u \cdot \eta} \\ &= \sum_{\xi ; f(\xi) = \eta} \sum_{u \in V_m} (-1)^{u \cdot (f(\xi) + \eta)} \\ &+ \sum_{\xi ; f(\xi) \neq \eta} \sum_{u \in V_m} (-1)^{u \cdot (f(\xi) + \eta)} \\ &= 2^m a_\eta(f). \end{aligned}$$

■

We say that a vector-valued Boolean function $f : V_n \to V_m$ is balanced if $a_\eta(f) = 2^{n-m}$, for all $\eta \in V_m$. By Lemma 1 we have the following known fact.

Corollary 1: A vector-valued Boolean function $f : V_n \to V_m$ is balanced if and only if the Boolean functions $u \cdot f$ are balanced, for all $u \neq 0$.

We recall the following definitions from [1].

Definition 1: A vector-valued Boolean function $f : V_n \to V_m$ is bent if its components $u \cdot f$ are bent, for all $u \neq 0$.

Definition 2: A vector-valued Boolean function $f : V_n \to V_m$ is perfect nonlinear if the function

$$D_\alpha : \xi \mapsto f(\xi + \alpha) + f(\xi)$$

is balanced, for all $\alpha \in V_n$, $\alpha \neq 0$.

By Corollary 1 a vector-valued Boolean function is perfect nonlinear if and only if its non-zero components are perfect nonlinear. Hence a vector-valued Boolean function is bent if and only if it is perfect nonlinear, and this fact is proved by means of the components of the function.

To conclude this survey of vector-valued bent functions we recall the following result from [1] and give a new short proof of it based on Lemma 1.

Theorem 1: If $f : V_n \to V_m$ is bent then $a_\eta(f) = b_\eta 2^{\frac{n}{2} - m}$ where b_η is odd, for all $\eta \in V_m$.

Proof: Using (3)

$$\begin{aligned} a_\eta(f) &= 2^{-m} \sum_{u \in V_m} \mathcal{F}(u \cdot f + u \cdot \eta) \\ &= 2^{-m}(\mathcal{F}(0) + 2^{\frac{n}{2}} \sum_{u \neq 0} \text{sign}(\mathcal{F}(u \cdot f + u \cdot \eta))) \\ &= 2^{n-m} + 2^{\frac{n}{2} - m} c_\eta, \end{aligned}$$

where c_η is an odd integer. Then $b_\eta = c_\eta + 2^{\frac{n}{2}}$ is an integer as bent Boolean functions exist only for even n, and it is odd.

■

One corollary of Theorem 1 is that bent functions from V_n to V_m exist only when $m \leq \frac{n}{2}$.

IV. Multidimensional Walsh Transform

Various types of Fourier transforms are known to exist. In cryptography and coding, the discrete Fourier transform, see for example [6], is commonly used. The transform to be introduced in this paper is different from the discrete Fourier transform and particularly suitable for analysis of vector-valued Boolean functions.

For a positive integer n, we denote by V_n the linear space of binary strings of length n. Let n and m be positive integers and let $f : V_n \to V_m$ be a vector valued Boolean function of n variables. The i^{th} component of f is denoted by f_i. Then we define

$$\mathcal{W}(f)(x) = \mathcal{W}(f)(x_1, \ldots, x_m) = \sum_{\xi \in V_n} \prod_{i=1}^{m} x_i^{f_i(\xi)},$$

where the sum is taken in the set $\mathbb{Z}[x_1, \ldots, x_m]/\langle x_1^2 - 1, \ldots, x_m^2 - 1\rangle$ of multivariate polynomials over integers, where the indeterminates x_i satisfy $x_i^2 = 1$, $i = 1, \ldots, m$. We call $\mathcal{W}(f)$ the *multi-Walsh transform* of f. Clearly, for $m = 1$ and $x_1 = -1$, we get the usual Walsh transform for Boolean functions (1).

The multi-Walsh transform of f is a polynomial of m indeterminates and with non-negative integer coefficients. It gives the value distribution of f. Indeed, we can write

$$\mathcal{W}(f)(x) = \sum_{\eta \in V_m} a_\eta \prod_{i=1}^{m} x_i^{\eta_i},$$

where $a_\eta = a_\eta(f)$ for $\eta = (\eta_1, \eta_2, \ldots, \eta_m) \in V_m$. If $f : V_n \to V_m$ is uniformly distributed, then $m \leq n$, and

$$\mathcal{W}(f)(x) = 2^n u_m(x), \text{ where } u_m(x) = 2^{-m} \prod_{i=1}^{m} (1 + x_i).$$

For multi-Walsh transform the uniform distribution plays the same role as zero for the onedimensional Walsh transform with $x_1 = -1$. In particular, for any normalized distribution $d_m(x)$ of values in V_m, we have $u_m(x) d_m(x) = u_m(x)$. In what follows we identify the m-tuple $M = (M_1, \ldots, M_m)$ of vectors $M_i \in V_n$ and the linear function $M : V_n \to V_m$, $M\xi = (M_1 \cdot \xi, \ldots, M_m \cdot \xi)$ and denote the set of such M by V_n^m . Next we state a multidimensional form of Parseval's theorem. We omit the proof as it is a special case of the proof of Theorem 5 with $\alpha = 0$.

Theorem 2: For any vector-valued Boolean function $f : V_n \to V_m$ the following holds:

$$\sum_{M \in V_n^m} \mathcal{W}^2(f + M)(x) = 2^{(m+1)n}(1 + (2^n - 1) u_m(x)).$$

V. Multi-Bent Functions

Analogous to the one-dimensional definition of bent functions we define the *multi-bent* functions as functions for which the squared distributions $\mathcal{W}(f + M)$ are equal, for all $M \in V_n^m$.

Definition 3: A vector-valued Boolean function $f : V_n \to V_m$ is multi-bent if

$$\mathcal{W}^2(f + M)(x) = 2^n(1 + (2^n - 1) u_m(x)), \qquad (4)$$

for all linear functions $M \in V_n^m$.

The following property of multi-bent functions follows directly from the definition when we observe that the constant term of the polynomial $\mathcal{W}^2(f+M)(x)$ is the sum of the squares of the frequencies $a_\eta(f+M)$.

Theorem 3: For $f : V_n \to V_m$ and $M \in V_n^m$ we denote $a_\eta(f+M) = \#\{\xi \in V_n \,|\, f(\xi) + M\xi = \eta\}$. If f is multi-bent then

$$\sum_{\eta \in V_m} a_\eta(f+M)^2 = 2^n(1 + (2^n - 1)2^{-m}) \text{ and}$$
$$\sum_{\eta \in V_m} (a_\eta(f+M) - 2^{n-m})^2 = 2^n - 2^{n-m}.$$

for all $M \in V_n^m$.

To summarize, the least maximum of quadratic deviation of the distributions of $f + M$ from the uniform distribution, where the maximum is taken over $M \in V_n^m$, is achieved by multi-bent functions, and for multi-bent functions the quadratic deviations are equally small for all $M \in V_n^m$.

The main result of this paper is a proof of the fact that a vector-valued Boolean function is bent if and only if it is multi-bent. We state the following theorem.

Theorem 4: Let $f : V_n \to V_m$ be a vector-valued Boolean function. Then the following are equivalent:

(i) f is multi-bent;
(ii) f is perfect nonlinear; and
(iii) f is bent.

The equivalence of (ii) and (iii) is known, see Section III. In the next section, a relation between the multi-Walsh transform of f and the multi-Walsh transform of $D_\alpha(f)$ is proved. Using this relation we obtain the implication from (i) to (ii). Finally, in Section VII we prove that (iii) implies (i).

VI. Multi-Bent Is Perfect Nonlinear

The result stated in the title of this section is a corollary of the following theorem which gives the general relationship between the multidimensional auto-correlation property and the multi-Walsh transform.

Theorem 5: Let $M = (M_1, \ldots, M_m) \in V_n^m$. Then

$$\sum_{M \in V_n^m} \mathcal{W}^2(f+M)(x) \prod_{i=1}^m x_i^{\alpha \cdot M_i} = 2^{nm}\mathcal{W}(D_\alpha f)(x) + 2^{n(m+1)}(2^n - 1)u_m(x), \tag{5}$$

for all $\alpha \in V_n$.

Proof:

$$\begin{aligned}
&\sum_{M \in V_n^m} \mathcal{W}^2(f+M)(x) \prod_{i=1}^m x_i^{\alpha \cdot M_i} \\
&= \sum_{M \in V_n^m} \prod_{i=1}^m x_i^{\alpha \cdot M_i} \sum_{\xi \in V_n} \prod_{i=1}^m x_i^{f_i(\xi) + M_i \cdot \xi} \\
&\times \sum_{\gamma \in V_n} \prod_{i=1}^m x_i^{f_i(\gamma) + M_i \cdot \gamma} \\
&= \sum_{\xi \in V_n} \sum_{\gamma \in V_n} \prod_{i=1}^m x_i^{f_i(\xi) + f_i(\gamma)} \prod_{i=1}^m \sum_{M_i \in V_n} x_i^{M_i \cdot (\alpha + \xi + \gamma)} \\
&= \sum_{\xi \in V_n} \prod_{i=1}^m x_i^{f_i(\xi) + f_i(\xi + \alpha)} 2^{nm} \\
&+ \sum_{\xi \in V_n} \sum_{\gamma; \gamma \neq \xi + \alpha} \prod_{i=1}^m \sum_{M_i \in V_n} x_i^{M_i \cdot (\alpha + \xi + \gamma) + f_i(\xi) + f_i(\gamma)} \\
&= 2^{nm}\mathcal{W}(D_\alpha f)(x) + 2^n(2^n - 1)2^{nm}u_m(x).
\end{aligned}$$

■

If f is multi-bent, then $\mathcal{W}^2(f+M)(x) = 2^n(1 + (2^n - 1)u_m(x)$. By substituting this to the left hand side of Eq. (5) gives $\mathcal{W}(D_\alpha f)(x) = 2^n u_m(x)$, for all $\alpha \neq 0$ as desired.

VII. Bent Is Multi-Bent

The following theorem completes the proof of Theorem 4.

Theorem 6: If a vector-valued Boolean function is bent then it is multi-bent.

Proof: Let $f : V_n \to V_m$ be a function and $M = (M_1, \ldots, M_m)$ an m-tuple of vectors in V_n. We start by using Lemma 1 and writing

$$\begin{aligned}
&\mathcal{W}(f+M)(x) \\
&= \sum_{\eta \in V_m} a_\eta(f+M) \prod_{i=1}^m x_i^{\eta_i} \\
&= \sum_{\eta \in V_m} 2^{-m} \sum_{u \in V_m} \sum_{\xi \in V_n} (-1)^{u \cdot (f(\xi) + M\xi + \eta)} \prod_{i=1}^m x_i^{\eta_i}.
\end{aligned}$$

Then

$$\begin{aligned}
&2^{2m}\mathcal{W}^2(f+M)(x) \\
&= \sum_{\eta, \zeta \in V_m} \sum_{u, v \in V_m} \sum_{\xi, \gamma \in V_n} (-1)^{u \cdot (f(\xi) + M\xi + \eta) + v \cdot (f(\gamma) + M\gamma + \zeta)} \\
&\times \prod_{i=1}^m x_i^{\eta_i + \zeta_i} \\
&= \sum_{u, v \in V_m} \mathcal{F}(u \cdot (f+M))\mathcal{F}(v \cdot (f+M))S,
\end{aligned}$$

where

$$S = \sum_{\eta, \zeta \in V_m} (-1)^{u \cdot \eta + v \cdot \zeta} \prod_{i=1}^m x_i^{\eta_i + \zeta_i}.$$

Substituting η by $\eta + \zeta$ we obtain

$$\begin{aligned}
S &= \sum_{\zeta \in V_m} (-1)^{(u+v) \cdot \zeta} \sum_{\eta \in V_m} (-1)^{u \cdot \eta} \prod_{i=1}^m x_i^{\eta_i} \\
&= \begin{cases} 2^m \sum_{\eta \in V_m} (-1)^{u \cdot \eta} \prod_{i=1}^m x_i^{\eta_i}, & \text{if } u = v, \\ 0, & \text{if } u \neq v. \end{cases}
\end{aligned}$$

Then

$$\begin{aligned}
&\mathcal{W}^2(f+M)(x)\\
&= 2^{-m}\sum_{u\in V_m}\mathcal{F}^2(u\cdot(f+M))\sum_{\eta\in V_m}(-1)^{u\cdot\eta}\prod_{i=1}^{m}x_i^{\eta_i}\\
&= 2^{-m}2^{2n}\sum_{\eta\in V_m}\prod_{i=1}^{m}x_i^{\eta_i}+2^{-m}2^{n}\sum_{u\neq 0}\sum_{\eta\in V_m}(-1)^{u\cdot\eta}\prod_{i=1}^{m}x_i^{\eta_i}\\
&= 2^{2n}u_m(x)+2^{n-m}\sum_{\eta\in V_m}\prod_{i=1}^{m}x_i^{\eta_i}\sum_{u\neq 0}(-1)^{u\cdot\eta}\\
&= 2^{2n}u_m(x)+2^{n-m}(2^m-1+\sum_{\eta\neq 0}\prod_{i=1}^{m}x_i^{\eta_i}\sum_{u\neq 0}(-1)^{u\cdot\eta})\\
&= 2^{2n}u_m(x)+2^{n-m}(2^m-2^m u_m(x))\\
&= 2^n(1+(2^n-1)u_m(x)),
\end{aligned}$$

as desired. ■

We conlude by giving a small example.

Example. Let $n=4$ and $m=2$. We set

$$\begin{aligned}
f_1(\xi_1,\xi_2,\xi_3,\xi_4) &= \xi_1\xi_2+\xi_3\xi_4\\
f_2(\xi_1,\xi_2,\xi_3,\xi_4) &= \xi_2\xi_3+(\xi_1+\xi_3)\xi_4.
\end{aligned}$$

Then $f=(f_1,f_2)$ is bent. The value distributions of the functions $f+M$ are either (7,3,3,3) or (1,5,5,5) (in various orders). Their variance is 76. Absolute values of the differences from the uniform distribution are (3,1,1,1) (where the order varies) and the quadratic sum of the differences is equal to 12.

These distributions follow the pattern that one value is taken $2^{\frac{n}{2}}\pm(2^m-1)$ times and the other 2^m-1 values are taken $2^{\frac{n}{2}}\mp 1$ times each. For $n>2m$, these frequencies are multiplied by $2^{\frac{n}{2}-m}$ as shown in Theorem 1. Do other patterns exist?

A second interesting question is what is the smallest possible maximum variance of the distributions of $f+M$ for $n<2m$ and how to identify such functions.

VIII. Conclusion

We have introduced a multidimensional Walsh transform to be used in the analysis of value distribution. In particular, we proved that the maximum variance of the value distribution of a vector-valued bent function, and all its translates by a linear function, is the smallest possible.

Acknowledgement

The authors thank Risto Hakala for useful suggestions for improving the presentation of this paper. The research work of the second author is supported by the Scientific Advisory Board for Defence.

References

[1] K. Nyberg, "Perfect nonlinear S-boxes," in *Advances in Cryptology – Eurocrypt '91*, ser. LNCS, vol. 547. Springer Verlag, 1991, pp. 378–386.

[2] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, "On almost perfect nonlinear functions over $\mathbf{F}_2^n$," *IEEE Transactions on Information Theory*, vol. 52, no. 9, pp. 4160 – 4170, 2006.

[3] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings," *IEEE Transactions on Information Theory*, vol. 45, pp. 475–485, 1999.

[4] X.-M. Zhang and Y. Zheng, "GAC - the criterion for global avalanche characteristics of cryptographic functions," *Journal of Universal Computer Science*, vol. 1, no. 5, pp. 320–337, 1995.

[5] O. S. Rothaus, "On "bent" functions," *Journal of Combinatorial Theory*, vol. A 20, pp. 300–305, 1976.

[6] J. L. Massey, "The discrete Fourier transform in coding and cryptography," in *Proceedings of ITW 1998*, 1998.