SCIENCE CHINA
Information Sciences

• LETTER •

March 2020, Vol. 63 139108:1–139108:3
https://doi.org/10.1007/s11432-018-9614-3

Characterizing differential support of vectorial Boolean functions using the Walsh transform

Jie PENG[1], Jianhua GAO[2] & Haibin KAN[3,4]*

[1]*Mathematics and Science College, Shanghai Normal University, Shanghai* 200234*, China;*
[2]*College of Information, Mechanical and Electrical Engineering, Shanghai Normal University, Shanghai* 200234*, China;*
[3]*Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai* 200433*, China;*
[4]*Fudan-Zhongan Joint Laboratory of Blockchain and Information Security, Shanghai Engineering Research Center of Blockchain, Shanghai* 200433*, China*

Received 16 July 2018/Accepted 29 September 2018/Published online 11 February 2020

Citation Peng J, Gao J H, Kan H B. Characterizing differential support of vectorial Boolean functions using the Walsh transform. Sci China Inf Sci, 2020, 63(3): 139108, https://doi.org/10.1007/s11432-018-9614-3

Dear editor,

Differential cryptanalysis, which was proposed by Biham and Shamir in [1], is a type of statistical attack to block ciphers. The resistance of ciphers to this type of attack is quantified by the cryptographic property named the differential uniformity of its substitution box, which is a vectorial Boolean function. To have a good resistance to the differential attack, the differential uniformity of the function should be as low as possible. In this sense, the best functions are those differentially 2-uniform functions, which are also called APN (almost perfect nonlinear) functions. There are very few known APN functions, and they may have potential drawbacks. In recent years, increasing attention has been given to differentially 4/6-uniform permutations (see [2–5] and references therein). Another key property of vectorial functions is the nonlinearity, which is characterized by the Walsh transforms of the functions. To resist a linear attack [6], the function should have a high nonlinearity.

An important problem that then arises is whether there are relationships between the two major cryptographic properties, say the differential uniformity and the nonlinearity, of vectorial functions. This question seems to be quite difficult to answer. All known APN functions seem to have rather good nonlinearity, but this parameter does not have a positive lower bound before Carlet's work. Chabaud and Vaudenay [7] found an inequality for the fourth moment of the Walsh transform, which is an equality when the function is APN. This result was generalized recently by Carlet in [8], where he succeeded in characterizing general vectorial functions with differential uniformity at most δ, for any positive even integer δ, using the Walsh transform. Moreover, he obtained a very good lower bound for the nonlinearity of APN power functions.

In this study, using the Walsh transform, we characterize the differential support of any vectorial function, which is defined to be the set of all the positive integers in the differential spectrum of the function, neglecting the multiplicities. This can help people to better understand the differential properties of vectorial functions. Moreover, the equalities in the characterization are much simpler than in Carlet's result, when the function has a small cardinality of differential support. In particular, we characterize differentially two-valued (n,m)-functions by the fourth moment of the Walsh transform. Based on that, we deduce an upper bound for the nonlinearity of differentially two-valued (n,m)-functions, which is always better than the covering radius bound,

* Corresponding author (email: hbkan@fudan.edu.cn)

and is also better than the Sidelnikov-Chabaud-Vaudenay bound, at least for most cases.

Characterizing differential support. For any (n,m)-function $F:\mathbb{F}_{2^n}\mapsto\mathbb{F}_{2^m}$, any $a\in\mathbb{F}_{2^n}^*$ and $b\in\mathbb{F}_{2^m}$, we denote

$$\delta(a,b)=|\{x\in\mathbb{F}_{2^n}\mid D_aF(x)=b\}|,\tag{1}$$

where $D_aF(x)=F(x+a)+F(x)$, and for any set S, its cardinality is denoted by $|S|$.

The differential uniformity $\delta(F)$ of F is defined as

$$\delta(F)=\max_{a\in\mathbb{F}_{2^n}^*,\ b\in\mathbb{F}_{2^m}}\delta(a,b),$$

and F is said to be differentially $\delta(F)$-uniform. The differential spectrum of F is the multiset consisting of all the integers $\delta(a,b)$ with their multiplicities. It is easy to see that $\delta(F)$ is always an even positive integer, which is at least 2^{n-m} if $n>m$, and is at least 2 otherwise. The differentially 2-uniform functions are also called almost perfectly nonlinear (APN). The nonlinearity of a vectorial (n,m)-function F is defined as

$$\mathrm{NL}(F)=2^{n-1}-\frac{1}{2}\max_{u\in\mathbb{F}_{2^n},v\in\mathbb{F}_{2^m}^*}W_F(u,v),$$

where for any $u\in\mathbb{F}_{2^n}$ and $v\in\mathbb{F}_{2^m}^*$, $W_F(u,v)$ is the Walsh transform of F, say

$$W_F(u,v)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^m(vF(x))+Tr_1^n(ux)}.$$

The following theorem was obtained by Carlet as a characterization of the differential uniformity of vectorial functions using the Walsh transform.

Theorem 1 ([8, Theorem III.3])**.** Let n,m and δ be positive integers, with δ even, and let F be an (n,m)-function. Let $\phi_\delta(X)=\sum_{j\geqslant 0}A_jX^j$ be a polynomial over the real number field such that $\phi_\delta(X)=0$ for $X=2,4,\ldots,\delta$ and $\phi_\delta(X)>0$ for every even $X\in\{\delta+2,\ldots,2^n\}$. Then, it holds that

$$2^n(2^n-1)A_0+\sum_{j\geqslant 1}2^{-j(m+n)}A_j((W_F^2)^{\otimes(j+1)}(0,0)\\ -2^{(2j+1)n+jm})\geqslant 0,\tag{2}$$

where $(W_F^2)^{\otimes(j+1)}$ is the convolutional product of W_F^2 iterated $j+1$ times. Moreover, this inequality is an equality if and only if $\delta(F)\leqslant\delta$.

We find that, in fact, the Walsh transforms can describe more on the differential spectrum. We now give our definition of the differential support for any (n,m)-function.

Definition 1. The differential support $\mathrm{DS}(F)$ of any (n,m)-function F is defined to be the set

$$\{2\leqslant i\leqslant 2^n\mid \exists\,(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^m}\text{ s.t. }\delta(a,b)=i\}.$$

In other words, as a set, the differential support is the differential spectrum without multiplicities and the zero. With this new notation, Theorem 1 means that $\mathrm{DS}(F)\subseteq\{2,4,\ldots,\delta\}$ if and only if relation (2) holds with equality for some polynomial $\phi_\delta(X)$ such that $\phi_\delta(X)=0$ for $X=2,4,\ldots,\delta$, and $\phi_\delta(X)>0$ for every even $X\in\{\delta+2,\ldots,2^n\}$. This result characterizes the differential uniformity of F, say $\delta(F)\leqslant\delta$. In the following theorem, we give a more detailed description of $\mathrm{DS}(F)$, which generalizes Carlet's result.

Theorem 2. Let F be an (n,m)-function, $S=\{2,4,6,\ldots,2^n\}$. Let $I\subseteq S$ and $\Psi_I(x)=\Pi_{i\in I}(x-i)=\sum_{j=0}^{|I|}B_jx^j$. If $\mathrm{DS}(F)\subseteq I$, then it holds that

$$2^n(2^n-1)B_0+\sum_{j=1}^{|I|}2^{-j(n+m)}B_j((W_F^2)^{\otimes(j+1)(0,0)}\\ -2^{(2j+1)n+jm})=0.\tag{3}$$

Moreover, $\mathrm{DS}(F)=\{2,4,\ldots,\delta-2,\delta\}$ for some δ if and only if Eq. (3) holds for $I=\{2,4,\ldots,\delta-2,\delta\}$, but not for any proper subset of I.

With this theorem, we can more efficiently characterize some functions with small-sized differential support, such as the differentially two-valued functions, whose $\delta(a,b)$ takes two values only, say $\delta(a,b)\in\{0,2^s\}$ for some positive integer s, or $\mathrm{DS}(F)=\{2^s\}$. For instance, power (n,n)-functions with quadratic exponents or Kasami exponents are differentially two-valued. Differentially two-valued functions can also be seen as a generalization of APN functions; a basic study of them can be found in [9].

For APN functions F over $\mathbb{F}_{2^n}$, it is well known and proved by Chabaud et al. [7] that

$$\sum_{u,v\in\mathbb{F}_{2^n}}W_F^4(u,v)=3\cdot 2^{4n}-2^{3n+1}.$$

Thanks to Theorem 2, we can generalize this result to differentially two-valued (n,m)-functions.

Theorem 3. Let F be a differentially two-valued 2^s-uniform (n,m)-function for some positive integer s; then, one has

$$\sum_{u\in\mathbb{F}_{2^n},v\in\mathbb{F}_{2^m}}W_F^4(u,v)=2^{3n+m}+2^s(2^{3n+m}-2^{2n+m}).$$

Remark 1. Note that in Theorem 3, we only need the convolutional product of W_F^2 iterated 2 times to characterize differentially two-valued

2^s-uniform (n,m)-functions, while Theorem 1 requires the convolutional product of W_F^2 iterated $2^{s-1}+1$ times.

Example 1. Considering differentially 4-uniform (n,m)-functions F with $\mathrm{DS}(F)=\{2,4\}$ (note that one must have $m \geqslant n-1$), according to Carlet's result (Theorem 1), if $\mathrm{DS}(F)=\{2,4\}$, then (let $\phi_4(X)=(X-2)(X-4)$) one has

$$(W_F^2)^{\otimes 3}(0,0)+3\cdot 2^{n+m+1}(W_F^2)^{\otimes 2}(0,0) - 2^{3n+2m+3}-2^{4n+2m}(2^n-2)=0 \tag{4}$$

and also $(W_F^2)^{\otimes 2}(0,0)\neq 3\cdot 2^{4n}-2^{3n+1}$ (because F is not APN). However, using Theorems 2 and 3 in this study, one concludes that $\mathrm{DS}(F)=\{2,4\}$ if and only if Eq. (4) holds and

$$(W_F^2)^{\otimes 2}(0,0)\neq 3\cdot 2^{4n}-2^{3n+1},\\ 5\cdot 2^{3n+m}-2^{2n+m+2}.$$

Hence, our result gives more characterizations of the differential support of vectorial functions.

A famous upper bound for the nonlinearity of any (n,m)-function F is the covering radius bound

$$\mathrm{NL}(F)\leqslant 2^{n-1}-2^{\frac{n}{2}-1}, \tag{5}$$

which is achieved by bent functions that satisfy $W_F(u,v)=\pm 2^{\frac{n}{2}}, \forall\ u\in\mathbb{F}_{2^n}, v\in\mathbb{F}_{2^m}^*$. Another well-known bound is the so-called Sidelnikov-Chabaud-Vaudenay (SCV) bound for $m\geqslant n-1$:

$$\mathrm{NL}(F)\leqslant 2^{n-1} - \frac{1}{2}\sqrt{3\cdot 2^n-2-2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

When $m=n-1$, the two bounds are the same. For $m>n-1$, the SCV bound is better than the covering radius bound, but it can only be achieved when $m=n$ is odd [7]. As a byproduct of Theorem 3, we can obtain an upper bound for the nonlinearity of differentially two-valued functions as follows.

Corollary 1. Let F be a differentially two-valued 2^s-uniform (n,m)-function. Then, one has

$$\mathrm{NL}(F)\leqslant 2^{n-1}-\frac{1}{2}\sqrt[4]{\frac{2^{2n+m}-1+2^{n+m+s}(2^n-1)}{2^m-1}}.$$

Note that

$$\frac{1}{2}\sqrt[4]{\frac{2^{2n+m}-1+2^{n+m+s}(2^n-1)}{2^m-1}}\sim 2^{\frac{n}{2}+\frac{s}{4}-1},\\ n\to\infty,$$

no matter what m is. Hence, our bound in Corollary 1 is always better than the covering radius bound (see (5)) for differentially two-valued vectorial functions.

When $m\geqslant n-1$, it can be easily seen that our bound in Corollary 1 is better than the SCV bound if m is not very large, for instance $m=n-1,n,\ldots$. Generally speaking, when $s\geqslant 3$, then our bound is always better than the SCV bound. Indeed, it can be deduced easily by

$$\frac{2^{2n+m}-1+2^{n+m+s}(2^n-1)}{2^m-1}>2^{2n}+2^{2n+s}\\ =2^{2n}(2^s+1)$$

and

$$\left(3\cdot 2^n-2-2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}\right)^2<(3\cdot 2^n)^2\\ =9\cdot 2^{2n}.$$

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61672355, 61672166, U19A2066), National Key Research & Development Plan(Grant No. 2019YFB2101703), Shanghai Excellent Academic Leader (Grant No. 16XD1400200), and Shanghai Innovation Plan of Science & Technology (Grant No. 16JC1402700).

References

1 Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. J Cryptol, 1991, 4: 3–72

2 Qu L J, Tan Y, Tan C H, et al. Constructing differentially 4-uniform permutations over $F_{2^{2k}}$ via the switching method. IEEE Trans Inform Theor, 2013, 59: 4675–4686

3 Tang D, Carlet C, Tang X. Differentially 4-uniform bijections by permuting the inverse function. Des Codes Cryptogr, 2015, 77: 117–141

4 Tu Z, Zeng X, Zhang Z. More permutation polynomials with differential uniformity six. Sci China Inf Sci, 2018, 61: 038104

5 Zha Z B, Hu L, Sun S W, et al. Further results on differentially 4-uniform permutations over $\mathbb{F}_{2^{2m}}$. Sci China Math, 2015, 58: 1577–1588

6 Matsui L. Linear cryptanalysis method for DES cipher. In: Advances in Cryptology–EUROCRYPT'93. Berlin: Springer, 1994. 386–397

7 Chabaud F, Vaudenay S. Links between differential and linear cryptanalysis. In: Proceedings of EUROCRYPT'94, 1995. 950: 356–365

8 Carlet C. Characterizations of the differential uniformity of vectorial functions by the Walsh transform. IEEE Trans Inform Theor, 2018, 64: 6443–6453

9 Blondeau C, Canteaut A, Charpin P. Differential properties of power functions. In: Proceedings of the 2010 IEEE International Symposium on Information Theory, Austin, 2010. 10: 2478–2482