Notes on Bent Functions in Polynomial Forms

Onur Koçak[1], Onur Kurt[1,2], Neşe Öztop[1], Zülfükar Saygı[3]

[1]Department of Cryptography, Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey
[2]Department of Mathematics, Middle East Technical University, Ankara, Turkey
[3] Department of Mathematics, TOBB Economics and Technology University, Ankara, Turkey
e-mail:{onur.kocak, konur, noztop}@metu.edu.tr, zsaygi@etu.edu.tr

Abstract—The existence and construction of bent functions are two of the most widely studied problems in Boolean functions. For monomial functions $f(x) = Tr_1^n(ax^s)$, these problems were examined extensively and it was shown that the bentness of the monomial functions is complete for $n \leq 20$. However, in the binomial function case, i.e. $f(x) = Tr_1^n(ax^{s_1}) + Tr_1^k(bx^{s_2})$, this characterization is not complete and there are still open problems. In this paper, we give a summary of the literature on the bentness of binomial functions and show that there exist no bent functions of the form $Tr_1^n(ax^{r(2^m-1)}) + Tr_1^m(bx^{s(2^m+1)})$ where $n = 2m$, $gcd(r, 2^m + 1) = 1$, $gcd(s, 2^m - 1) = 1$. Also, we give a bent function example of the form $f_{a,b}(x) = Tr_1^n(ax^{2^m-1}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$ for $n = 4$, although, it is stated in [9] that there is no such bent function of this form for any value of a and b.

Keywords—Boolean function, Bent functions, Walsh-Hadamard Transform, Dillon exponents, Kloosterman Sums.

1. Introduction

The class of bent functions is a special set of functions that achieve the highest possible non-linearity among Boolean functions. Such functions are of great importance for cryptography and coding theory. Therefore, the existence of bent functions is a widely studied problem. When considering the polynomial form, monomial bent functions, which are of the form $Tr_1^n(ax^s)$ are studied by [1], [3], [4], [7] and all monomial bent functions are known if $n \leq 20$. After reaching such a point, community started to pay attention on binomial bent functions of the form $Tr_1^n(ax^{s_1})+Tr_1^k(bx^{s_2})$. These functions are examined in [6], [8], [9], [10], [15], [16] and the existence conditions of bent functions are given for some values of the parameters n, k, s_1 and s_2. However, the characterization of binomial bent functions is not complete and open problems remain.

Manuscript received May 22, 2012; revised June 28, 2012.

In this paper, we give a brief summary of current studies on binomial bent functions. Moreover, we give existence and non-existence results for some specific forms of bent function families.

The paper is organized as follows: Section II is devoted to the notation used in the rest of the paper and necessary knowledge. In the third section, in order to give the historical background, we mention the known results on monomial bent functions. Next, in Section IV, we investigate the bentness of binomial functions, give some examples and results on specific values of k, t and m for the functions

$f_{a,b}(x) = Tr_1^n(ax^{2^m-1}) + Tr_1^k(bx^{\frac{2^n-1}{t}})$.

2. Notation and Preliminaries

2.1. Boolean Functions and Polynomial Forms

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function in n variables. The *truth table* of f is defined as the vector $(f(x_0), f(x_1), \ldots, f(x_{2^n-1}))$. The number of non-zero coordinates in the truth table is called the *Hamming weight* $wt(f)$ of f, or weight in short. Equivalently, one can define weight as

$$wt(f) = \sum_{x \in \mathbb{F}_{2^n}} f(x).$$

Any Boolean function f can be uniquely represented in a polynomial form as

$$f(x) = \sum_{r \in R} Tr_1^{o(r)}(a_r x^r) + \epsilon(1 + x^{2^{n-1}}),$$

$\forall x \in \mathbb{F}_{2^n}$, $a_r \in \mathbb{F}_{2^{o(r)}}$ where $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$, the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, is the sum of the conjugates of $x \in \mathbb{F}_{2^n}$, R is the set of *cyclotomic coset leaders* r, $o(r)$ is the size of the coset that contains r and ϵ is the modulo 2 value of $wt(f)$.

Note that bent functions defined on $\mathbb{F}_{2^n}$ exist only for even values of n. Moreover, it is well known that their Hamming weights are even. Therefore, $\epsilon = 0$ and their polynomial form is

$$f(x) = \sum_{r \in R} Tr_1^{o(r)}(a_r x^r) \quad \forall x \in \mathbb{F}_{2^n}.$$

2.2. Bent Functions

The *Walsh-Hadamard transform* of f is the discrete Fourier transform of $(-1)^f$. It is defined for the value $\omega \in \mathbb{F}_{2^n}$ as follows:

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

Definition 1: A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be bent if $W_f(\omega) = \pm 2^{\frac{n}{2}}$ for all $\omega \in \mathbb{F}_{2^n}$.

The classical binary Kloosterman sums on $\mathbb{F}_{2^m}$ are defined as follows:

Definition 2: Let $a \in \mathbb{F}_{2^m}$. The binary Kloosterman sum associated with a is

$$K_m(a) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m\left(ax + \frac{1}{x}\right)}.$$

Proposition 1: [12] Let m be a positive integer. The set $\{K_m(a),\ a \in \mathbb{F}_{2^m}\}$ is the set of all the integers multiple of 4 in the range $\left[-2^{\frac{m+2}{2}} + 1, 2^{\frac{m+2}{2}} + 1\right]$.

3. Monomial Bent Functions

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function such that $f(x) = Tr_1^n(ax^s)$ for a given positive integer s and for some $a \in \mathbb{F}_{2^n}$. Functions of this form are called monomial functions. The exponent s is said to be a bent exponent if there exists $a \in \mathbb{F}_{2^n}^*$ such that $Tr_1^n(ax^s)$ is bent. In order f to be bent, the following two conditions should be satisfied [3]:

- $gcd(s, 2^n - 1) \neq 1$.
- either $gcd(s, 2^{n/2} + 1) = 1$ or $gcd(s, 2^{n/2} - 1) = 1$.

All known bent exponents s for power functions, with $o(s) = n$, are given in Table 1.

TABLE 1
All known bent exponents, s, $o(s) = n$

s	Condition	Reference
$2^i + 1$	$\frac{n}{gcd(n,i)}$ even, $1 \leq i \leq \frac{n}{2}$	[13]
$r \cdot (2^{n/2} - 1)$	$gcd(r, 2^{n/2} + 1) = 1$	[1], [3], [7], [12]
$2^{2i} - 2^i + 1$	$gcd(n, i) = 1$	[14]
$(2^{n/4} + 1)^2$	$n = 4r$, r odd	[3], [5]
$2^{n/3} + 2^{n/6} + 1$	$n = 0 \ mod \ 6$	[4]

Also, Canteaut *et al.* [4] showed by computer experiments that there is no other exponent s for $n \leq 20$.

Moreover, for the exponents s where $o(s) < n$, Mesnager [11], based on an exhaustive search up to $n \leq 14$, claimed that the only bent Boolean functions are of the form $Tr_1^{n/2}(ax^{2^{n/2}+1})$ for some $a \in \mathbb{F}_{2^n}$.

A specific form of monomial functions, $f_a^{(r)}$, namely monomial Dillon functions, can be represented as

$$f_a^{(r)}(x) = Tr_1^n(ax^{r(2^m-1)}),$$

$\forall x \in \mathbb{F}_{2^n},\ a \in \mathbb{F}_{2^n}^*, n = 2m$. Bentness of these functions has been first studied by Dillon [1] for the case $r = 1$. Then, Leander [3] next Charpin and Gong [7] investigated the bentness of monomial Dillon functions in the case $gcd(r, 2^m + 1) = 1$. The following theorem shows the relation between the bentness of monomial Dillon functions and Kloosterman sums.

***Theorem** 1:* [1], [7] Suppose that $a \in \mathbb{F}_{2^m}^*$. The function $f_a^{(r)}$ defined on $\mathbb{F}_{2^n}$ by $f_a^{(r)}(x) = Tr_1^n(ax^{r(2^m-1)})$ where $gcd(r, 2^m + 1) = 1$ is bent if and only if the Kloosterman sum on $\mathbb{F}_{2^m}$ denoted by K_m satisfies $K_m(a) = 0$.

In this paper, we focus on the bent functions with Dillon exponents.

4. Binomial Bent Functions

Monomial bent functions have been intensively investigated over the years and all the bent exponents have been identified for $n \leq 20$. As the search heavily relies on computer experiments, it is very hard to find a new exponent s for $n > 20$ so that $Tr_1^n(ax^s)$ does not belong to any of the previous constructions. Therefore, the community started to search bent functions with multiple trace terms where the first step, naturally, is binomial functions. The first studies in finding binomial bent functions were performed by Dobbertin *et al.* [2] where they showed that $Tr_1^n(a_1x^{s_1} + a_2x^{s_2})$ is bent with s_1 and s_2 being Niho exponents. Note that, a positive integer s (always understood modulo 2^n-1) is said to be a Niho exponent, and x^s is Niho power function, if the restriction of x^s to $\mathbb{F}_{2^m}$ is linear or in other words $s \equiv 2^j (mod\ 2^m - 1)$ for some $j < n$. The following are bent Niho exponents given by Dobbertin *et al.* [2]. The fractions are interpreted modulo $2^m + 1$, for instance $\frac{1}{2} = 2^{m-1} + 1$.

- $s_1 = (2^m - 1)\frac{1}{2} + 1$ and $s_2 = (2^m - 1)3 + 1$;
- $s_1 = (2^m - 1)\frac{1}{2} + 1$ and $s_2 = (2^m - 1)\frac{1}{4} + 1$ (m odd);
- $s_1 = (2^m - 1)\frac{1}{2} + 1$ and $s_2 = (2^m - 1)\frac{1}{6} + 1$ (m even);

Then, in [6], [8], [9], Mesnager investigated the functions $Tr_1^n(ax^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$ and gave the conditions on $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_{2^2}^*$ for bentness. Following Mesnager's approach, Wang *et al.* [15] considered the functions of the form $f_{a,b}(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^4(bx^{\frac{2^n-1}{5}})$ where $n = 2m$, $m \equiv 2\ (mod\ 4)$, $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{2^4}$.

In this section, we investigate bentness of $f_{a,b}(x) = Tr_1^n(ax^{2^m-1}) + Tr_1^k(bx^{\frac{2^n-1}{t}})$ when $t|2^m+1$ and when $t|2^m - 1$. We cover the previous work of Mesnager [9] and Wang *et al.* [10], [15], give some examples for both cases and state a result on the existence of bent functions of the form $f_{a,b}(x) = Tr_1^n(ax^{(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$ for $n = 4$.

4.1. $Tr_1^n(ax^{(2^m-1)}) + Tr_1^k(bx^{\frac{2^n-1}{t}})$, *where* $o(\frac{2^n-1}{t}) = k$ *and* $t|2^m + 1$

Mesnager [9] showed that the bentness of

$$f_{a,b}(x) = Tr_1^n(ax^{(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$$

$a \in \mathbb{F}_{2^n}^*,\ b \in \mathbb{F}_4^*,\ n = 2m$, can be characterized via Kloosterman sums for $m > 3$, m odd. If $K_m(a) = 4$, then $f_{a,1}$,$f_{a,\beta}$ and f_{a,β^2} are bent while if $K_m(a) \neq 4$ then $f_{a,1}$,$f_{a,\beta}$ and f_{a,β^2} are not bent. Wang *et al.* [10] followed similar approach given in [9] and showed that

$$g_{a,b}(x) = Tr_1^n(ax^{(2^m-1)}) + Tr_1^4(bx^{\frac{2^n-1}{5}})$$

is bent for some values of a and b, where $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^4}$, $n = 2m$ and $m \equiv 2 \ mod \ 4$. The following function can be given as an example of a bent function of this form:

$$Tr_1^{12}(x^{63}) + Tr_1^4(\beta x^{819})$$

where $\beta = \alpha^{273}$ is a root of the primitive polynomial x^4+x+1 and α is a root of the primitive polynomial $x^{12} + x^6 + x^4 + x + 1$.

Both these approaches are quite similar and depend on the fact that 3 or 5 do not only divide $2^n - 1$ but also $2^m + 1$. Mesnager [16] proved this idea for general case

$$h_{a,b}(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^k(bx^{s(2^m-1)})$$

where $n = 2m$ is an even integer, R is a subset of representatives of the cyclotomic classes modulo $(2^m + 1)$, $a_r \in \mathbb{F}_{2^m}^*$, $b \in \mathbb{F}_{2^k}$ and $s = \frac{2^m+1}{t}$. Note, $o(s(2^m - 1)) = k$, i.e. the size of the cyclotomic coset of s modulo $(2^m + 1)$ is k. The proof for the general case depends on Dickson polynomials.

4.2. $Tr_1^n(ax^{(2^m-1)}) + Tr_1^k(bx^{\frac{2^n-1}{t}})$*, where* $o(\frac{2^n-1}{t}) = k$ *and* $t | 2^m - 1$

In [9], Mesnager studied the functions of the form

$$f_{a,b}(x) = Tr_1^n(ax^{(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$$

and found some results when m is odd. Because of the fact that 3 divides $2^m - 1$ when m is even, this case seems much harder than the case for m odd. Therefore, the bentness of $f_{a,b}$ for even values of m has not been characterized yet. On the other hand, it is claimed in [9] by conducting exhaustive search that for $n = 8, 12$, there exist bent Boolean functions of the form $f_{a,b}(x) = Tr_1^n(ax^{(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$, but there is no bent function of this form for $n = 4$. However, our computer experiments resulted in the existence of a bent function for $n = 4$ and it is shown in *Remark 1*.

TABLE 2

x	$Tr_1^4(x^3)$	$Tr_1^2(x^5)$	$f(x)$	$W_f(x)$
0	0	0	0	4
1	0	0	0	-4
α	1	1	0	4
$\alpha + 1 = \alpha^4$	1	1	0	-4
α^2	1	1	0	4
$\alpha^2 + 1 = \alpha^8$	1	1	0	-4
$\alpha^2 + \alpha = \alpha^5$	0	1	1	-4
$\alpha^2 + \alpha + 1 = \alpha^{10}$	0	1	1	4
α^3	1	0	1	4
$\alpha^3 + 1 = \alpha^{14}$	1	1	0	4
$\alpha^3 + \alpha = \alpha^9$	1	0	1	4
$\alpha^3 + \alpha + 1 = \alpha^7$	1	1	0	4
$\alpha^3 + \alpha^2 = \alpha^6$	1	0	1	4
$\alpha^3 + \alpha^2 + 1 = \alpha^{13}$	1	1	0	4
$\alpha^3 + \alpha^2 + \alpha = \alpha^{11}$	1	1	0	-4
$\alpha^3 + \alpha^2 + \alpha + 1 = \alpha^{12}$	1	0	1	-4

Remark 1: $f_{a,b}(x) = Tr_1^4(ax^3) + Tr_1^2(bx^5)$ is bent for $a = 1$ and $b = 1$ where $\mathbb{F}_{2^4} = \mathbb{F}_2(\alpha)$ and α is a root of the primitive polynomial $x^4 + x + 1$ over $\mathbb{F}_{2^4}$.

Algebraic normal form of $f(x)$ is

$$f(x) = Tr_1^4(x^3) + Tr_1^2(x^5) = x_1 + x_2x_3 + x_1x_4$$

where $x = (x_1, x_2, x_3, x_4)$. The truth table and Walsh spectrum of $f(x)$ can be seen from Table 2.

The following functions are numerical examples for $f_{a,b}$ when 3 divides $2^m - 1$:

- For $n = 8$, $m = 4$, $k = 2$ and $t = 3$

  $$Tr_1^8(\alpha^{51}x^{15}) + Tr_1^2(x^{85})$$

  where α is a root of the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$.
- For $n = 12$, $m = 6$, $k = 2$ and $t = 3$

  $$Tr_1^{12}(\alpha^{195}x^{63}) + Tr_1^2(x^{1365})$$

  where α is a root of the primitive polynomial $x^{12} + x^6 + x^4 + x + 1$.

Consider the case $t = 2^m - 1$. Then,

$$f_{a,b}(x) = Tr_1^n(ax^{2^m-1}) + Tr_1^m(bx^{2^m+1}).$$

It is known that if $f_{a,b}(x)$ is bent, then $W_f(w) = \pm 2^m,\ \forall w$.
Before looking at the Walsh-Hadamard transform, it is worth to note two well-known facts one of which is about the Kloosterman sums.

Proposition 2: [1]

$$\sum_{u\in\mathbb{U}}(-1)^{Tr_1^n(au)} = 1 - K_m(a),$$

where $\mathbb{U}$ is the cyclic group of order 2^m+1 and $a \in \mathbb{F}_{2^m}^*$.

Proposition 3: Any $x \in \mathbb{F}_{2^n}^*$ can be written as $x = uy$ with $y \in \mathbb{F}_{2^m}^*$ and $u \in \mathbb{U}$ where $\mathbb{U}$ is the cyclic group of order 2^m+1.

Computation of the Walsh-Hadamard transform for $w = 0$ shows

$$W_f(0) = \textstyle\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n\left(ax^{2^m-1}\right)+Tr_1^m\left(bx^{2^m+1}\right)}$$

$$\begin{aligned}
&= 1+\sum_{u\in\mathbb{U}}\sum_{y\in\mathbb{F}_{2^m}^*}(-1)^{Tr_1^n\left(a(uy)^{2^m-1}\right)+Tr_1^m\left(b(uy)^{2^m+1}\right)}\\
&= 1+\sum_{u\in\mathbb{U}}(-1)^{Tr_1^n\left(au^{2^m-1}\right)}\sum_{y\in\mathbb{F}_{2^m}^*}(-1)^{Tr_1^m\left(by^2\right)}\\
&= 1+\sum_{u\in\mathbb{U}}(-1)^{Tr_1^n(au)}\sum_{y\in\mathbb{F}_{2^m}^*}(-1)^{Tr_1^m(by)}\\
&= 1+(1-K_m(a))(-1)\\
&= K_m(a)
\end{aligned}$$

In order for $f_{a,b}(x)$ to be bent, $W_f(0) = K_m(a) = \pm 2^m$. However, by Proposition 1, we know that $K_m(a)$ is in the interval $[-2^{\frac{m+2}{2}}+1, 2^{\frac{m+2}{2}}+1]$ $\forall a \in \mathbb{F}_{2^m}^*$. One can easily show that, for any value of $m > 2$, $\pm 2^m$ is out of Kloosterman sums bounds. To illustrate, the boundaries for $K_m(a)$ and the Walsh spectrum values are given in Table 3 for distinct values of m. This observation is stated in Proposition 4.

Proposition 4: Boolean functions of the form

$$f_{a,b}(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^m(bx^{s(2^m+1)})$$

TABLE 3

m	$K_m(a)$	$W_f(0)$
2	[-3, 5]	± 4
3	[-4.65, 6.65]	± 8
4	[-7, 9]	± 16
5	[-10.31, 12.31]	± 32
6	[-15, 17]	± 64

where $gcd(r, 2^m+1) = 1$, $gcd(s, 2^m-1) = 1$ are not bent for any $a,\ b \in \mathbb{F}_{2^m}^*$.

5. Conclusion

The classification and characterization of bent functions in polynomial forms is a hard problem. Despite the existence of notably many specified bent functions, there are still open problems and unclassified bent functions. In this note, we studied previous characterization of some binomial functions of the form $f_{(a,b)}(x) = Tr_1^n(ax^{(2^m-1)}) + Tr_1^k(bx^{\frac{2^n-1}{t}})$ where t divides either 2^m+1 or 2^m-1. Mesnager [9] investigated the former case and presented some conditions on bentness of this function family. The latter case has not been characterized yet. In this study, we showed for specific values of t, where $t = 2^m-1$, that there is no bent function of the form $Tr_1^n(ax^{(2^m-1)}) + Tr_1^m(bx^{2^m+1})$. As a future work, it is planned to study the characterization of $f_{(a,b)}$ in the case t divides 2^m-1 which still has open problems.

6. Acknowledgment

This paper is an extended version of the paper appeared in the Proceedings of 5th International Conference on Information Security and Cryptology, 2012. The first and the third authors are supported by TÜBİTAK under Fellowship Program No. 2211.

The fourth author is supported by TÜBİTAK under Grant No. TBAG–109T344.

References

[1] J. F. Dillon, *Elementary Hadamard Difference Sets*, Ph.D Dissertation, University of Maryland 1974.

[2] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, P. Gaborit, *Construction of bent functions via Niho power functions*, J. Combin. Theory, ser. A, vol. 113, pp 779-798, 2006.

[3] G. Leander, *Monomial bent functions*, IEEE Trans. Inf. Theory, vol. 2, no. 52, pp. 738-743, 2006.

[4] A. Canteaut, P. Charpin, and G. Kyureghyan, *A new class of monomial bent functions*, Finite Fields Applicat., vol. 14, no. 1, pp 221-241, 2008.

[5] P. Charpin and G. Kyureghyan, *Cubic monomial bent functions: A subclass of M*, SIAM J. Discr. Math., vol. 22, no. 2, pp. 650-665,2008.

[6] S. Mesnager, *A new class of bent boolean functions in polynomial forms*, in Proc. Int. Workshop on Coding and Cryptography, WCC 2009, pp. 5-18, 2009.

[7] P. Charpin, G. Gong, *Hyperbent functions, Kloosterman Sums and Dickson Polynomials*, IEEE Trans. Inform. Theory 9(54), 4230-4238 (2008).

[8] S. Mesnager, *A new family of hyper-bent boolean functions in polynomial form*, M. G. Parker Ed., in Proc. Twelfth Int. Conf. Cryptography and Coding, Cirencester, United Kingdom. IMACC 2009, Heidelberg, Germany, 2009, vol. 5921, LNCS, pp. 402-417.

[9] S. Mesnager, *A new class of bent and hyper-bent boolean functions in polynomial forms*, Des. Codes Cryptography, 59(1-3):265-279, 2011.

[10] B. Wang, C. Tang, Y. Qi, Y. Yang, M. Xu, *A New Class of Hyper-bent Boolean Functions with Multiple Trace Terms*, Cryptology ePrint Archive, Report 2011/600, 2011. http://eprint.iacr.org/.

[11] S. Mesnager, *Recent Results on Bent and Hyper-bent Functions and Their Link With Some Exponential Sums.* IEEE Information Theory Workshop (ITW 2010), Dublin, August-September 2010.

[12] G. Lachaud, J. Wolfmann, *The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes* IEEE Trans. Inf. Theory, vol. 36, no 3, pp. 686-692, 1990.

[13] R.Gold, *Maximal Recursive Sequences with 3-valued Recursive Cross-Correlation Functions* IEEE Trans. Inf. Theory, vol. 14, no 1, pp. 154-156, 1968.

[14] J.F. Dillon, H. Dobbertin, *New Cyclic Difference Sets with Singer Parameters* Finite Fields and Their Applications, vol.10, no 3, pp. 342-389, 2004.

[15] B. Wang, C. Tang, Y. Qi, and Y. Yang, *A generalization of the class of hyper-bent Boolean functions in binomial forms*, Cryptology ePrint Archive, Report 2011/698, 2011. http://eprint.iacr.org/.

[16] S. Mesnager, J.-P. Flori, *A note on hyper-bent functions via Dillon-like exponents*, Cryptology ePrint Archive, Report 2012/033, 2012. http://eprint.iacr.org/.