A NOTE ON SEMI-BENT BOOLEAN FUNCTIONS

CLAUDE CARLET AND SIHEM MESNAGER

Abstract. We show how to construct semi-bent Boolean functions from $\mathcal{PS}_{ap}$-like bent functions.

Keywords. Boolean function, Bent functions, Maximum nonlinearity, Semi-bent function, Walsh-Hadamard transformation, Partial Spread class.

1. Introduction

A number of research works in symmetric cryptography are devoted to problems of resistance of various ciphering algorithms to the fast correlation attacks (on stream ciphers) and the linear cryptanalysis (on block ciphers) and to the analysis of various classes of approximating functions and constructions of functions with the best resistance to such approximations. Some general classes of Boolean functions play a central role with this respect: the class of bent functions [13], i.e., of Boolean functions of an even number of variables that have the maximum possible Hamming distance from the set of all affine functions (see for instance [4]), its subclasses of homogeneous bent functions [12], hyper-bent functions [14], and generalizations of the notion: semi-bent functions [5], Z-bent functions [8], negabent functions [11], etc.

In this paper we investigate constructions of the so called *semi-bent functions*. The term of semi-bent function has been introduced by Chee, Lee and Kim at Asiacrypt' 94. These functions have been previously investigated under the name of 3-valued almost optimal Boolean functions in [2]. Also, they are particular cases of the so-called plateaued functions [15]. Semi-bent functions are studied in cryptography because, besides having low Hadamard transform which provides protection against fast correlation attacks [10] and linear cryptanalysis [9], they can possess desirable properties in addition to the propagation criterion and low additive autocorrelation, such as resiliency and high algebraic degree.

The paper is organized as follows. In section 2, we fix our main notation and recall the necessary background. Next, in section 3, we consider how to construct semi-bent Boolean functions from bent functions.

2. Notation and preliminaries

For any set E, we will denote $E \setminus \{0\}$ by $E^\star$ and the cardinality of E by $\#E$.

Date: September 14, 2010.

Department of Mathematics, University of Paris VIII and University of Paris XIII. CNRS UMR 7539 LAGA (Laboratoire Analyse, Géometrie et Applications).
Email: claude.carlet@inria.fr,mesnager@math.jussieu.fr.

• *Boolean functions and polynomial forms*:
Let n be a positive integer. A Boolean function f on $\mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-valued function over the Galois field $\mathbb{F}_{2^n}$ of order 2^n (or over the vector space $\mathbb{F}_2^n$ but in this paper we shall always endow this vector space with the structure of field, thanks to the choice of a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$). The *weight* of f, denoted by $\mathrm{wt}(f)$, is the *Hamming weight* of the image vector of f, that is, the cardinality of its support $Supp(f) := \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.
For any positive integer k, and for any r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, is the mapping defined as: $\forall x \in \mathbb{F}_{2^k}, \quad Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}}$.
In particular, the *absolute trace* over $\mathbb{F}_2$ is the function $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

Recall that, for every integer r dividing k, the trace function Tr_r^k satisfies the transitivity property, that is, $Tr_1^k = Tr_1^r \circ Tr_r^k$.
Every non-zero Boolean function f defined over $\mathbb{F}_{2^n}$ has a (unique) trace expansion of the form:

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1})$$

called its polynomial form, where Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo $2^n - 1$, $o(j)$ is the size of the cyclotomic coset of 2 modulo $2^n - 1$ containing j, $a_j \in \mathbb{F}_{2^{o(j)}}$ and, $\epsilon = \mathrm{wt}(f)$ modulo 2.

• *Niho power functions:*
Let $n = 2m$ be an even integer. Recall that a positive integer d (always understood modulo $2^n - 1$) is said to be a *Niho exponent*, and x^d is a *Niho power function*, if the restriction of x^d to $\mathbb{F}_{2^m}$ is linear or in other words $d \equiv 2^j \pmod{2^m - 1}$ for some $j < n$. As we consider $Tr_1^n(x^d)$, without loss of generality, we can assume that d is in the normalized form, with $j = 0$, and then we have a unique representation $d = (2^m - 1)s + 1$ with $2 \leq s \leq 2^m$.

• *Walsh transform, bent, semi-bent and hyper-bent functions*:
Let f be a Boolean function on $\mathbb{F}_{2^n}$. Its *"sign" function* is the integer-valued function $\chi(f) := (-1)^f$. The Walsh Hadamard transform of f is the discrete Fourier transform of χ_f, whose value at $\omega \in \mathbb{F}_{2^n}$ is defined as follows:

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr_1^n(\omega x)}.$$

Bent functions [13] can be defined as follows:

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

Semi-bent functions [5, 6] can be defined as follows, for n even and for n odd:

Definition 2. Let n be an even integer. A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be semi-bent if if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+2}{2}}\}$, for all $\omega \in \mathbb{F}_{2^n}$.

Definition 3. Let n be an odd integer. A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be semi-bent if if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+1}{2}}\}$, for all $\omega \in \mathbb{F}_{2^n}$.

Hyper-bent functions [14] have properties still stronger than bent functions. More precisely, they can be defined as follows:

Definition 4. A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be hyper-bent if the function $x \mapsto f(x^i)$ is bent, for every integer i co-prime with $2^n - 1$.

• *The Dillon Partial Spread classes*:
The Partial Spread class $\mathcal{PS}$, introduced in [7] by Dillon, is the set of all the sums (modulo 2) of the indicators of $2^{\frac{n}{2}-1}$ or $2^{\frac{n}{2}-1}+1$ disjoint $\frac{n}{2}$-dimensional subspaces of $\mathbb{F}_{2^n}$ (disjoint meaning that any two of these spaces intersect in 0 only, and therefore that their sum is direct and equals $\mathbb{F}_{2^n}$). Dillon denotes by $\mathcal{PS}^-$ (resp. $\mathcal{PS}^+$) the class of those bent functions for which the number of $\frac{n}{2}$-dimensional subspaces is $2^{\frac{n}{2}-1}$ (resp. $2^{\frac{n}{2}-1}+1$).

Dillon exhibits a subclass of $\mathcal{PS}^-$, denoted by $\mathcal{PS}_{ap}$, whose elements are defined in an explicit form:

Definition 5. Let $n = 2m$. The Partial Spread class $\mathcal{PS}_{ap}$ consists of all functions f defined over $\mathbb{F}_{2^n}$ as follows: let g be a balanced Boolean function over $\mathbb{F}_{2^m}$ (ie. $wt(g) = 2^{m-1}$) such that $g(0) = 0$ (in fact this last condition is not necessary for f to be bent). Define a Boolean function f from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_2$ as $f(x, y) = g(\frac{x}{y})$ (i.e $g(xy^{2^m-2})$) with $\frac{x}{y} = 0$ if $y = 0$.

All the bent functions from the PS_{ap} class defined by Dillon [7] are hyper-bent. They are the functions or the complements of the functions defined over $\mathbb{F}_{2^n}$ and whose supports have the form $\bigcup_{u\in S} u\mathbb{F}_{2^m}^\star$ where U is the set $\{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$ and S is a subset of U of size 2^{m-1}.

In the whole paper $n = 2m$ is an (even) integer.

3. Construction of semi-bent functions

Recall [7] that a collection $\{E_i,\, i = 1, \ldots, 2^m + 1\}$ of vector spaces of dimension m such that:

(1) $E_i \cap E_j = \{0\}$ for every i and j,
(2) $\bigcup_{i=1}^{2^m+1} E_i = \mathbb{F}_{2^n}$.

is called a *spread*.

Conjecture 1. We conjecture that, for every spread $\{E_i,\, i = 1, \ldots, 2^m + 1\}$, there exists a bent Boolean function h defined over $\mathbb{F}_{2^n}$ such that, for every i, the restriction of h to E_i is linear.

In the next theorem, we show that the sum of a PS_{ap} function and of a bent function whose restriction to any multiplicative coset of $\mathbb{F}_{2^n}^*$ is linear is semi-bent. More generally:

Theorem 1. *Let $\{E_i,\, i = 1, \ldots, 2^m + 1\}$ be a spread in $\mathbb{F}_{2^n}$ and h a Boolean function whose restriction to every E_i is linear. Let S be any subset of size 2^{m-1} of $\{1, \ldots, 2^m + 1\}$. Let g be the Boolean function defined over $\mathbb{F}_{2^n}$ whose support is $\bigcup_{s\in S} E_s^\star$ if $\#S = 2^{m-1}$ or $\bigcup_{s\in S} E_s$ if $\#S = 2^{m-1} + 1$ (note that g is necessarily in the Partial Spread class PS). If h is bent, then $g + h$ is semi-bent.*

Obviously the result remains valid when replacing g by $g + 1$.

Proof. Let us compute the Walsh transform of $g+h$,

$$\forall c \in \mathbb{F}_{2^n}, \quad \widehat{\chi_{g+h}}(c) = 1 + \sum_{i=1}^{2^m+1} \sum_{e \in E_i^\star} \chi(g(e) + h(e) + Tr_1^n(ce)).$$

since $\bigcup_{i=1}^{2^m+1} E_i^\star = \mathbb{F}_{2^n}^\star$ and $E_i^\star \cap E_j^\star = \emptyset$. The Boolean function g is constant on each set $E_i^\star$. Let us denote by g_i the value of g on $E_i^\star$. Furthermore, we denote by h_i the restriction of h to E_i. Thus

$$\begin{aligned}\forall c \in \mathbb{F}_{2^n}, \quad \widehat{\chi_{g+h}}(c) &= 1 + \sum_{i=1}^{2^m+1} \chi(g_i) \sum_{e \in E_i^\star} \chi(h_i(e) + Tr_1^n(ce)) \\ &= 1 - \sum_{i=1}^{2^m+1} \chi(g_i) + \sum_{i=1}^{2^m+1} \chi(g_i) \sum_{e \in E_i} \chi(h_i(e) + Tr_1^n(ce))\end{aligned}$$

Now, $\sum_{i=1}^{2^m+1} \chi(g_i) = 2^m + 1 - 2\#S = 1$. Introduce the set $I(c) = \{i \in [1, \ldots, 2^m + 1] \mid \forall e \in E_i,\, h_i(e) = Tr_1^n(ce)\}$. Thus, since h_i is linear on E_i, one has

$$\sum_{e \in E_i} \chi(h_i(e) + Tr_1^n(ce)) = 2^m \text{ if } i \in I(c) \text{ and } 0 \text{ otherwise}$$

Therefore

$$\forall c \in \mathbb{F}_{2^n}, \quad \widehat{\chi_{g+h}}(c) = 2^m \sum_{i \in I(c)} \chi(g_i).$$

Now, let us compute the Walsh transform of h :

$$\forall c \in \mathbb{F}_{2^n}, \quad \widehat{\chi_h}(c) = \sum_{x \in \mathbb{F}_{2^n}} \chi(h(x) + Tr_1^n(cx)) = 1 + \sum_{i=1}^{2^m+1} \sum_{e \in E_i^\star} \chi(h_i(e) + Tr_1^n(ce)).$$

that is,

$$\widehat{\chi_h}(c) = 1 - (2^m+1) + \sum_{i=1}^{2^m+1} \sum_{e \in E_i} \chi(h_i(e) + Tr_1^n(ce)) = -2^m + 2^m \#I(c) = 2^m(\#I(c) - 1).$$

If h is bent, then we necessarily have that $\#I(c) \in \{0, 2\}$ (because one has $\widehat{\chi_h}(c) \in \{\pm 2^m\}$). The sum $\sum_{i \in I(c)} \chi(g_i)$ takes thus its values in $\{0, \pm 2\}$ proving that $g+h$ is semi-bent. □

Remark 1. Under the hypothesis of Theorem 1, if h is not bent but semi-bent then $g+h$ is bent. Indeed, we have then $\#I(c) \in \{1, 3\}$ (because one has $\widehat{\chi_h}(c) \in \{0, \pm 2^{m+1}\}$ and $2^m(\#I(c) - 1) \geq -2^m$). The sum $\sum_{i \in I(c)} \chi(g_i)$ is then congruent with 2^m modulo 2^{m+1} proving that $g+h$ is bent, according to Lemma 1 in [3]. But there can not exist a semi-bent function whose restriction to every E_i is linear. Indeed, this function having non-negative Walsh transform as we saw above, we would then have $\sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_h}(\omega) = 2^n$ and Parseval's relation $\sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_h}^2(\omega) = 2^{2n} = \left(\sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_h}(\omega)\right)^2$ would imply, since each $\widehat{\chi_h}(\omega)$ is non-negative, that for every $\omega \neq \omega'$, we have $\widehat{\chi_h}(\omega)\widehat{\chi_h}(\omega') = 0$ and therefore h would be affine, a contradiction.

We apply now Theorem 1 to the spread $\{u\mathbb{F}_{2^m}\,;\, u \in U\}$ where U is the multiplicative group $\{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$.

Corollary 2. *Let h be a Boolean function whose expression is a sum of Niho power monomials :*

$$\forall x \in \mathbb{F}_{2^n}, \quad h(x) = \sum_{i=1}^{L} Tr_1^n(a_i x^{d_i}) + Tr_1^m(a_0 x^{2^m+1})$$

where $d_i = (2^m-1)s_i + 1$, $2 \leq s_i \leq 2^m$ with $s_i \neq 2^{m-1}+1$ (in fact, $o(d_i) = m$ if $s_i = 2^{m-1}+1$ and n orherwise), $a_0 \in \mathbb{F}_{2^m}$, $a_i \in \mathbb{F}_{2^n}$ for $i \in \{1, \cdots, L\}$. Assume that h is bent. Let g be any PS_{ap} function. Then, $g+h$ is semi-bent.

Proof. Without loss of generality, we assume that the support of g is $\bigcup_{u \in S} u\mathbb{F}_{2^m}$ where S is a subset of U of size 2^{m-1}. Since all the exponents in h are Niho power exponents, the restriction of h to any vector space $u\mathbb{F}_{2^m}$ is linear. Hence Corollary 2 is a direct consequence of Theorem 1. □

The bivariate version of the spread $\{u\mathbb{F}_{2^m}\,;\, u \in U\}$ is the spread $\{E_a\,;\, a \in \mathbb{F}_{2^m}\} \cup \{E'\}$ where $E_a = \{(au, u), u \in \mathbb{F}_{2^m}\}$ and $E' := \{(u,0), u \in \mathbb{F}_{2^m}\} = \mathbb{F}_{2^m} \times \{0\}$: $\mathbb{F}_{2^n}$ being identified with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ thanks to the choice of a basis $(1, w)$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$. It can be directly checked that the E_a's and E' are indeed vector spaces of dimension m, and we have $E_a \cap E_b = \{0\}$ for every pair (a,b) such that $a \neq b$ and $E' \cap E_a = \{0\}$ for every $a \in \mathbb{F}_{2^m}$. Note that any function g in the PS_{ap} class can be viewed as the indicator of 2^{m-1} or $2^{m-1}+1$ of these vector spaces.

Corollary 3. *Let g be a function in the PS_{ap} class. Let i be any integer co-prime with m and $h(x,y) = Tr_1^m(xy^{2^i-1})$. Then the function $g+h$ is semi-bent.*

Indeed, h belongs to the Maiorana-McFarland class of bent functions since the function y^{2^i-1} is a permutation of $\mathbb{F}_{2^m}$, the restriction of h to E_a is linear for every a and its restriction to E' is null.

Remark 2. According to [1, Theorem 6], the permutations y^{2^i-1} are the only permutations π such that $x\pi(x)$ is linear.

Open problem:
Do there exist spreads which are not linearly equivalent to the spaces $u\mathbb{F}_{2^m}$ (used in Corollary 2)?

References

[1] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy. On almost perfect nonlinear functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 4160-4170, 2006.

[2] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine. On cryptographic properties of the cosets of R(1,m), IEEE Transactions on Information Theory, Vol. 47,pp 1494-1513, 2001.

[3] C. Carlet. Generalized Partial Spreads, *IEEE Transactions on Information Theory*, vol. 41, no. 5, pp. 1482-1487, 1995.

[4] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering" published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.). pp. 257-397, 2010.

[5] S. Chee and S. Lee and K. Kim. Semi-bent Functions Advances in Cryptology-ASIACRYPT94. Proc. 4th Int. Conf. on the Theory and Applications of Cryptology, Wollongong, Australia, 1994, Pieprzyk, J. and Safavi-Naini, R., Eds., Lect. Notes Comp. Sci. Vol. 917, pp 107-118, 1994.

[6] J. H. Cheon and S. Chee. Elliptic curves and resilient functions Lecture Notes in Computer Science, Vol. 2015 pp 386–397, 2000.

[7] J. Dillon. Elementary Hadamard difference sets PhD dissertation, University of Maryland, 1974.

[8] H. Dobbertin, and G. Leander. Cryptographers Toolkit for Construction of 8-Bit Bent Functions Cryptology ePrint Archive, Report no. 2005/089. Available at http://eprint.iacr.org/2005/089 2005.

[9] M. Matsui. Linear cryptanalysis method for DES cipher. *Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science* 765, pp. 386-397, 1994.

[10] W. Meier and O. Staffelbach. Fast correlation attacks on stream ciphers. *Advances in Cryptology, EUROCRYPT'88, Lecture Notes in Computer Science* 330, pp. 301-314, 1988.

[11] M.G. Parker and A. Pott. On Boolean Functions Which Are Bent and Negabent, Int. Workshop on Sequences, Subsequences, and Consequences (SSC 2007), Los Angeles, USA, 2007. Revised Invited Papers, Golomb, S.W., Gong, G., Helleseth, T., and Song, H.-Y., Eds., Lect. Notes Comp. Sci. 4893 (2007), 9-23.

[12] C. Qu, J. Seberry, and J. Pieprzyk. Homogeneous Bent Functions, Discrete Appl. Math. 102 no. 1-2 , 133-139, 2000.

[13] O.S. Rothaus. On "bent" functions, J. Combin.Theory Ser A 20, pp. 300-305, 1976.

[14] A. M. Youssef and G. Gong. Hyper-Bent Functions, Advances in Crypology Eurocrypt'01, LNCS, Springer, pp. 406-419, 2001.

[15] Y. Zheng and X. M. Zhang. Relationships between bent functions and complementary plateaued functions, Lecture Notes in Computer Science, Vol. 1787, pp. 60-75, 1999.