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. We derive infinite classes of semi-bent functions in even dimension having multiple trace terms.

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 [22], 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 [5]), its subclasses of homogeneous bent functions [21], hyper-bent functions [23], and generalizations of the notion: semi-bent functions [7], Z-bent functions [10], negabent functions [20], 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 [24]. Semi-bent functions are studied in cryptography because, besides having low Hadamard transform which provides protection against fast correlation attacks [16] and linear cryptanalysis [15], 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 26, 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. The algebraic degree of f is equal to the maximum 2-weight of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$.

- *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 Hadamard transform*:

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:

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

Recall the well-known Parseval's relation

$$\sum_{\omega\in\mathbb{F}_{2^n}} \widehat{\chi_f}^2(\omega) = 2^{2n}.$$

and also this inverse formula

$$\sum_{\omega\in\mathbb{F}_{2^n}} \widehat{\chi_f}(\omega) = 2^n(-1)^{f(0)}.$$

It is easy to see that not all values of the values of the Walsh transform have the same sign. This comes from the fact that

$$\left(\sum_{\omega\in\mathbb{F}_{2^n}} \widehat{\chi_f}(\omega)\right)^2 = \sum_{\omega\in\mathbb{F}_{2^n}} \widehat{\chi_f}^2(\omega)$$

which implies that it is impossible to have $\widehat{\chi_f}(\omega) \geq 0$ for all ω as well $\widehat{\chi_f}(\omega) \leq 0$ for all ω, unless f is affine.

- *Bent, semi-bent and hyper-bent functions*:

Bent functions [22] 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 [7, 8] 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 $\omega \in \mathbb{F}_{2^n}$.

It is well Known (see for instance [5]) that the algebraic degree of a semi-bent Boolean function defined on $\mathbb{F}_{2^n}$ is at most $\frac{n}{2}$.

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 [23] 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 [9] 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 [9] 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 $\bigcup_{u\in S} u\mathbb{F}^\star_{2^m}$ 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 [9] that a collection $\{E_i,\, i = 1, \dots, 2^m + 1\}$ 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 $\{E_i,\, i = 1, \dots, 2^m + 1\}$, 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 characterize when a function whose restriction to every E_i^* is affine is semi-bent:

Theorem 1. *Let $m \geq 2$ and $n = 2m$. Let $\{E_i,\, i = 1, \dots, 2^m + 1\}$ 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 $\{1, \dots, 2^m + 1\}$ and $g = \sum_{i \in S} 1_{E_i} \pmod 2$ where 1_{E_i} is the indicator of E_i. Then $g + h$ is semi-bent if and only if g and h are bent.*

Note that g is then in the Partial Spread class PS and h is in a class generalizing the class that Dillon denotes by H in [9].

We can modify the hypothesis of Theorem 1 by assuming that we have only a partial spread. We need then to add a condition on the E_i's, and we have only a sufficient condition (not a necessary and sufficient one) for $g + h$ being semi-bent:

Theorem 2. *Let g be a bent function in the PS class, equal to the sum modulo 2 of the indicators of $l := 2^{m-1}$ or $2^{m-1} + 1$ pairwise "disjoint" vector paces E_i having dimension m, and h a bent function which is linear on each E_i. Assume additionally that for every $c \in \mathbb{F}_{2^n}$ there exist at most 2 indices i such that $\forall e \in E_i$, $h(e) = Tr_1^n(ce)$. Then $g + h$ is bent.*

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. Two new classes of bent functions. In *Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science* 765, pp. 77-101, 1994.

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

[5] 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.

[6] P. Charpin and G. Gong. Hyperbent functions, Kloosterman sums and Dickson polynomials, *IEEE Trans. Inform. Theory (54) 9*, pp 4230–4238, 2008.

[7] 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.

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

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

[10] 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.

[11] H. Dobbertin and G. Leander and A. Canteaut and C. Carlet and P. Felke and P. Gaborit. Construction of bent functions via Niho Power Functions, *Journal of Combinatorial therory, Serie A 113*, pp 779-798, 2006.

[12] F. Gologlu. Almost Bent and Almost Perfect Nonlinear Functions, Exponential Sums, Geometries ans Sequences, *PhD dissertation, University of Magdeburg*, 2009.

[13] G. Leander. Monomial Bent Functions. *IEEE Trans. Inform. Theory (52) 2*, pp 738–743, 2006.

[14] G. Leander and A. Kholosha. Bent functions with 2^r Niho exponents. *IEEE Trans. Inform. Theory 52 (12)*, pp 5529–5532, 2006

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

[16] 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.

[17] S. Mesnager. A new class of Bent Boolean functions in polynomial form. *Proceedings of international Workshop on Coding and Cryptography, WCC 2009*, pp 5-18,2009.

[18] S. Mesnager. A new family of hyper-bent Boolean functions in polynomial form. *Proceedings of Twelfth International Conference on Cryptography and Coding, Cirencester, United Kingdom. M. G. Parker (Ed.): IMACC 2009*, LNCS 5921, pp 402-417, Springer, Heidelberg (2009).

[19] S. Mesnager. Hyper-bent Boolean functions with multiple trace terms. *Proceedings of International Workshop on the Arithmetic of Finite Fields. M.A. Hasan and T.Helleseth (Eds.): WAIFI 2010*, LNCS 6087, pp. 97–113 Springer, Heidelberg (2010).

[20] 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.

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

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

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

[24] 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.