Several infinite families of bent functions and their duals

Sihem Mesnager

University of Paris VIII (department of Mathematics)
and University of Paris XIII (LAGA), CNRS

International Workshop on Boolean Functions and Their Applications
September 2014, Rosendal, Norway

Outline

1. Background on Boolean functions
2. Background on bent functions and quick survey on recent constructions of bent functions
3. Results on bent functions :
   - secondary constructions of bent functions and their duals
   - serval infinite families of bent functions and their duals
4. Conclusion

Background on Boolean functions : representation

☞ We identify the vectorspace $\mathbb{F}_2^n$ with the Galois field $\mathbb{F}_{2^n}$

Definition (The polynomial form (unique))

Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its ***polynomial form :***

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

- Γ_n is the set of representatives of each cyclotomic class of 2 modulo $2^n - 1$,
- $o(j)$ is the size of the cyclotomic coset containing j,
- $\epsilon = wt(f)$ modulo 2 (recall $wt(f) := \#supp(f) := \#\{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$).

Recall :

Definition (Absolute trace of $x \in \mathbb{F}_{2^k}$ over $\mathbb{F}_2$)

$Tr_1^k(x) := \sum_{i=0}^{k-1} x^{2^i} = x + x^2 + x^{2^2} + \cdots + x^{2^{k-1}} \in \mathbb{F}_2$

Algebraic degree of the polynomial form

Definition

Let n be a positive integer. Every Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion called its ***polynomial form*** *:*

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

☞ **The algebraic degree** of f denoted by $\deg(f)$, is the maximum Hamming weight of the binary expansion of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$.

- Affine functions : $Tr_1^n(ax) + \lambda$, $a \in \mathbb{F}_{2^n}$, $\lambda \in \mathbb{F}_2$.

The bivariate representation of Boolean functions

The bivariate representation (unique) : $n = 2m$

$$\mathbb{F}_{2^n} \approx \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$$

$$f(x,y) = \sum_{0 \le i,j \le 2^m-1} a_{i,j} x^i y^j; \; a_{i,j} \in \mathbb{F}_{2^m}$$

.

- Then the algebraic degree of f equals $\max_{(i,j) \mid a_{i,j} \neq 0}(w_2(i) + w_2(j))$.
- And f being Boolean, its bivariate representation can be written in the form $f(x,y) = Tr_1^m(P(x,y))$ where $P(x,y)$ is some polynomial over $\mathbb{F}_{2^m}$.

A cryptographic parameter for Boolean functions : nonlinearity

☞ The nonlinearity of f is the minimum Hamming distance to affine functions :

Definition (The Hamming distance between two Boolean functions)

$$d_H(f,g) = wt(f \oplus g) = \#\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}$$

Definition (Nonlinearity)

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ a Boolean function. The nonlinearity denoted by $\mathrm{nl}(f)$ of f is

$$\mathrm{nl}(f) := \min_{l \in A_n} d_H(f,l)$$

where A_n : is the set of affine functions over $\mathbb{F}_{2^n}$.

General upper bound on the nonlinearity of Boolean functions and bent functions

THEOREM (A GENERAL UPPER BOUND)

For every n-variable Boolean function f, the nonlinearity is always upper bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$

➔It can reach this value if and only if n is even.

DEFINITION (BENT FUNCTION [ROTHAUS 1976])

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ *(n even) is said to be a bent function if* $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$.

Bent functions have been studied for 40 years (initiators : [Dillon 1974] ; [Rothaus, 1976]).

Bent functions and their duals

PROPOSITION (A MAIN CHARACTERIZATION OF "BENTNESS")

(f is bent) $\iff$ $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}, \quad \forall \omega \in \mathbb{F}_{2^n}$. *where* $\widehat{\chi_f}$ *is the discrete Fourier (Walsh) Transform of* f *:* $\widehat{\chi_f}(a) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(ax)}, \quad a \in \mathbb{F}_{2^n}$

- The maximum degree of a bent function on $\mathbb{F}_{2^n}$ is $\frac{n}{2}$.

DEFINITION (DUAL OF A BENT FUNCTION)

If $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ *is bent then*

$$\widehat{\chi_f}(\omega) = 2^{\frac{n}{2}}(-1)^{\widetilde{f}(\omega)}, \quad \forall \omega \in \mathbb{F}_{2^n}$$

defines the dual function $\tilde{f}$ *of* f.

- The dual of a bent function is again bent and $\widetilde{\widetilde{f}} = f$.

DEFINITION (SELF DUAL AND ANTI-SELF-DUAL)

A bent function f *is said to be self-dual if* $\widetilde{f} = f$.
A bent function f *is said to be anti-self-dual if* $\widetilde{f} = 1 + f$

General Primary constructions of bent functions

- **Maiorana-Mc Farland's class $\mathcal{M}$** : the best known construction of bent functions defined in bivariate form (explicit construction). $f_{\pi,g}(x,y) = x \cdot \pi(y) + g(y)$, with $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be a permutation and $g : \mathbb{F}_2^m \to \mathbb{F}_2$ any mapping.
- **Dillon's Partial Spreads class $\mathcal{PS}^-$** : well known construction of bent functions whose bentness is achieved under a condition based on a decomposition of its supports (not explicit construction) : $supp(f) = \bigcup_{i=1}^{2^{m-1}} E_i^\star$ where $\{E_i, 1 \leq i \leq 2^{m-1}\}$ are m-dimensional subspaces with $E_i \cap E_j = \{0\}$.
- **Dillon's Partial Spreads class $\mathcal{PS}_{ap}$** : a subclass of $\mathcal{PS}^-$'s class. Functions in $\mathcal{PS}_{ap}$ are defined explicitly in bivariate form : $f(x,y) = g(xy^{2^m-2})$ with g is a balanced Boolean function on $\mathbb{F}_{2^m}$ which vanishes at 0.
- **Dillon's class H** : a nice original construction of bent functions in bivariate representation (but less known because Dillon could only exhibit functions which already belonged to the well known Maiorana-Mc Farland class). The bentness is achieved under some non-obvious conditions. It was extended by [Carlet-Mesnager 2011] : **class $\mathcal{H}$**.

Relevant results on the construction of bent functions (1/3) :

• 1968-2008 Monomial bent functions [Gold 1968], [Dillon 1974], [Dillon-Dobbertin 2004], [Leander 2006], [Leander-Kholosha 2006], [Charpin-Kyureghyan 2008], [Canteaut-Charpin-Kyureghyan 2008].

• 2006 : The introduction of 3 families of binomial bent functions with Niho exponents [Dobbertin-Leander-Canteaut-Carlet-Felke-Gaborit 2006].

progress afterward :

- one of them has been extended [Leander-Kholosha 2006].
- the correspondence between the bent functions (bivariate forms) of the class $\mathcal{H}$ and the Niho bent functions (univariate forms) provided answers to questions left open in the literature since 2006 [Carlet-Mesnager 2011].
- progress on the duals of those families [Carlet-Mesnager 2011], [Carlet-Helleseth-Kholosha-Mesnager 2011], [Budaghyan-Carlet-Helleseth-Kholosha-Mesnager 2012].
- one family has been extended [Helleseth-Kholosha-Mesnager 2012].
- etc.

Recent relevant results on the construction of bent functions (2/3) :
• 2009 : Introduction of the two first families of binomial bent function (which are bent up to a change a primitive root in $\mathbb{F}_{2^n}$) via Dillon-like exponents of maximal degree by considering functions over subfields [Mesnager 2009]
progress afterward :

- new several families of bent functions have been exhibited [Mesnager-Flori 2012], [Tang-Lou-Qi-Xu-Guo 2013], [Li-Helleseth-Tang-Kholosha 2013], [Tang-Qi 2014], etc.
- results on bent vectorial bent functions have been obtained [Muratovic-Pasalic -Ribic 2014].
- etc.

Recent relevant results on the construction of bent functions (3/3) :

• 2011 : the introduction of the class $\mathcal{H}$ of bent function (in bivariate forms ; contains a class H introduced by Dillon in 1974) and direct connection with the o(val)-polynomial comes from Finite Projective Geometry [Carlet-Mesnager 2011]

progress afterward :

- many progress in Niho bent functions have been obtained.
- construction of 16 (potentially) new families of bent functions in $\mathcal{H}$ (and thus new bent functions of type Niho) thanks to the 8 classes of o-polynomials discovered by the geometers in 40 years [Carlet-Mesnager 2011].
- New Niho bent functions from quadratic o-monomials [Budaghyan-Kholosha-Carlet-Helleseth 2014]

☞ From now on, $\tilde{f}$ denotes the dual of a bent function f.

A secondary construction of bent functions :

THEOREM ([CARLET 2006])

Let n be any positive integer. Let f_1, f_2 and f_3 be three bent functions. Denote by ψ the function $f_1 + f_2 + f_3$ and by g the function $f_1f_2 + f_1f_3 + f_2f_3$. Then

1. *If ψ is bent and if $\tilde{\psi} = \tilde{f}_1 + \tilde{f}_2 + \tilde{f}_3$, then g is bent and $\tilde{g} = \tilde{f}_1\tilde{f}_2 + \tilde{f}_1\tilde{f}_3 + \tilde{f}_2\tilde{f}_3$.*
2. *If g is bent, or if more generally $\widehat{\chi_g}(w)$ is divisible by $2^{\frac{n}{2}}$ for every $w \in \mathbb{F}_{2^n}$, then ψ is bent.*

Furthermore, for every $\omega \in \mathbb{F}_{2^n}$

$$\widehat{\chi_g}(\omega) = \frac{\widehat{\chi_{f_1}}(\omega) + \widehat{\chi_{f_2}}(\omega) + \widehat{\chi_{f_3}}(\omega) - \widehat{\chi_{\psi}}(\omega)}{2}.$$

One can complete the second assertion of the previous theorem :

THEOREM (*)

Let n be an even integer. Let f_1, f_2 and f_3 be three pairwise distinct bent functions over $\mathbb{F}_{2^n}$ such that $\psi = f_3 + f_2 + f_1$ is bent. Let g be a Boolean function defined by $f_1 f_2 + f_1 f_3 + f_2 f_3$. Then g is bent if and only if $\tilde{f}_1 + \tilde{f}_2 + \tilde{f}_3 + \tilde{\psi} = 0$. Furthermore, if g is bent then its dual function $\tilde{g}$ is given by

$$\tilde{g}(x) = \tilde{f}_1(x)\tilde{f}_2(x) + \tilde{f}_2(x)\tilde{f}_3(x) + \tilde{f}_3(x)\tilde{f}_1(x), \forall x \in \mathbb{F}_{2^n}.$$

One can complete the second assertion of the previous theorem :

THEOREM (*)

Let n be an even integer. Let f_1, f_2 and f_3 be three pairwise distinct bent functions over $\mathbb{F}_{2^n}$ such that $\psi = f_3 + f_2 + f_1$ is bent. Let g be a Boolean function defined by $f_1f_2 + f_1f_3 + f_2f_3$. Then g is bent if and only if $\tilde{f}_1 + \tilde{f}_2 + \tilde{f}_3 + \tilde{\psi} = 0$. Furthermore, if g is bent then its dual function $\tilde{g}$ is given by

$$\tilde{g}(x) = \tilde{f}_1(x)\tilde{f}_2(x) + \tilde{f}_2(x)\tilde{f}_3(x) + \tilde{f}_3(x)\tilde{f}_1(x), \forall x \in \mathbb{F}_{2^n}.$$

DEFINITION

The first derivative of a Boolean function f in the direction of $a \in \mathbb{F}_{2^n}$ is defined as $D_a f(x) = f(x) + f(x+a)$.The second order derivative of f with respect to $(a,b) \in \mathbb{F}_{2^n}^2$ is defined as $D_b D_a f(x) = f(x) + f(x+b) + f(x+a) + f(x+a+b)$.

by considering functions of the form $f_i : x \mapsto f_i(x) := h(x) + Tr_1^n(\lambda_i x)$ we obtain the following consequence of Theorem (*) :

COROLLARY

Let h be a bent function defined on $\mathbb{F}_{2^n}$ whose dual function $\tilde{h}$ has a null second order derivative with respect to $(a,b) \in \mathbb{F}_{2^n}^2$ with $a \neq b$. Then the function g' defined by

$$\forall x \in \mathbb{F}_{2^n},\ g'(x) := h(x) + Tr_1^n(ax)Tr_1^n(bx)$$

is bent and its dual $\tilde{g}'$ is given by
$\tilde{g}'(x) = \tilde{h}(x)\tilde{h}(x+a) + \tilde{h}(x)\tilde{h}(x+b) + \tilde{h}(x+a)\tilde{h}(x+b)$.

One can generalize the previous corollary :

Corollary

Let h_1 and h_2 be two bent functions over $\mathbb{F}_{2^n}$. Assume that $D_a\tilde{h}_1 = D_a\tilde{h}_2$ with respect to some $a \in \mathbb{F}_{2^n}^\star$ where $\tilde{h}_1$ and $\tilde{h}_2$ stand for the dual functions of h_1 and h_2, respectively. Let g be the Boolean function defined on $\mathbb{F}_{2^n}$ by

$$g(x) = h_1(x) + Tr_1^n(ax)(h_1(x) + h_2(x) + 1), \forall x \in \mathbb{F}_{2^n}.$$

Then g is bent and its dual function $\tilde{g}$ is given by

$$\tilde{g}(x) = \tilde{h}_1(x) + \tilde{h}_1(x)\tilde{h}_2(x) + \tilde{h}_1(x+a)\tilde{h}_2(x+a), \forall x \in \mathbb{F}_{2^n}.$$

On Secondary Constructions of Bent Functions and their Duals

Now, there are two particular classes of bent Boolean functions when considering their dual : the so-called self-dual and anti-self-dual bent functions.

Corollary

Let n be an even integer. Let f_1, f_2, f_3 be three self-dual bent functions over $\mathbb{F}_{2^n}$ such that $f_3 + f_2 + f_1$ is self-dual bent. Let g be defined as

$$g(x) = f_1(x)f_2(x) + f_1(x)f_3(x) + f_2(x)f_3(x), \forall x \in \mathbb{F}_{2^n}.$$

Then g is self-dual bent.

Open problem

Let n be an even integer. Find three anti-self-dual bent functions f_1, f_2, f_3 over $\mathbb{F}_{2^n}$ such that $f_3 + f_2 + f_1$ is anti-self-dual bent.

On Secondary Constructions of Bent Functions and their Duals

Remark

A vectorial function $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^r}$ *(or a* (n,r)*-function) is bent if and only if all its components (Boolean) functions* $f_a : x\in\mathbb{F}_{2^n}\mapsto Tr_1^r(aF(x)), a\in\mathbb{F}_{2^r}^\star$ *are bent.*
It is well known [Nyberg 1993] that bent (n,r)*-functions exist when* n *is even and* $r\leq\frac{n}{2}$*.*
If we can find three pairwise distinct components f_{a_1}*,* f_{a_2} *and* f_{a_3} *such that* $\tilde{f}_{a_1}+\tilde{f}_{a_2}+\tilde{f}_{a_3}+\tilde{f}_{a_1+a_2+a_3}=0$*. Then,*
$g(x)=f_{a_1}(x)f_{a_2}(x)+f_{a_1}(x)f_{a_3}(x)+f_{a_2}(x)f_{a_3}(x)$
is bent and that its dual function is $\tilde{f}_{a_1}\tilde{f}_{a_2}+\tilde{f}_{a_1}\tilde{f}_{a_3}+\tilde{f}_{a_2}\tilde{f}_{a_3}$*.*

Application : example of functions from Maiorana-McFarland ’s class

- The class of bent functions given by $f(x,y) = Tr_1^m(\phi(y)x) + g(y), \quad (x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ (where m is some positive integer, ϕ is a function from $\mathbb{F}_{2^m}$ to itself and g stands for a Boolean function over $\mathbb{F}_{2^m}$) is the so-called Maiorana-McFarland ’s class.

Furthermore, its dual function $\tilde{f}$ is given by $\tilde{f}(x,y) = Tr_1^m(y\phi^{-1}(x)) + g(\phi^{-1}(x))$.

- Now, in order to apply Theorem (*), one has to find three permutations ϕ_1, ϕ_2, ϕ_3 of $\mathbb{F}_{2^m}$ and three Boolean functions g_1, g_2 and g_3 on $\mathbb{F}_{2^m}$ such that

(C1) $\psi = \phi_1 + \phi_2 + \phi_3$ is a permutation whose inverse function is $\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$.

(C2) $g_1 \circ \phi_1^{-1} + g_2 \circ \phi_2^{-1} + g_3 \circ \phi_3^{-1} + h \circ \psi^{-1} = 0$ where $h = g_1 + g_2 + g_3$.

Construction 1 : New Infinite Families of Bent Functions via Kasami Function and their Duals :

THEOREM

Let $n = 2m$. *Let* $\lambda \in \mathbb{F}_{2^m}^\star$. *Let* $(a, b) \in \mathbb{F}_{2^n}^\star \times \mathbb{F}_{2^n}^\star$ *such that* $a \neq b$ *and* $Tr_1^n(\lambda^{-1} b^{2^m} a) = 0$. *Then the Boolean function* f *defined on* $\mathbb{F}_{2^n}$ *as* $f(x) = Tr_1^m(\lambda x^{2^m+1}) + Tr_1^n(ax)Tr_1^n(bx)$ *is a bent function of algebraic degree* 2 *and its dual function* $\tilde{f}$ *is given by*

$$\begin{aligned}\tilde{f}(x) = Tr_1^m(\lambda^{-1} x^{2^m+1}) &+ \left(Tr_1^m(\lambda^{-1} a^{2^m+1}) + Tr_1^n(\lambda^{-1} a^{2^m} x)\right) \\ &\times \left(Tr_1^m(\lambda^{-1} b^{2^m+1}) + Tr_1^n(\lambda^{-1} b^{2^m} x)\right) + 1.\end{aligned}$$

Construction 2 : New bent functions from Niho exponents ant their duals

Theorem

Let (λ, μ) *be a pair of distinct elements of* $\mathbb{F}_{2^m}^\star$. *Define a Boolean function* h *over* $\mathbb{F}_{2^n}$ *by*
$h(x) = Tr_1^m(x^{2^m+1}) + Tr_1^n\Big(\sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)\frac{i}{2^r}+1}\Big) + Tr_1^n(\lambda x)Tr_1^n(\mu x).$
Then h *is bent and its dual function* $\tilde{h}$ *is given by*

$$\begin{aligned}\tilde{h}(x) = {} & Tr_1^m\Big(\big(u(1+x+x^{2^m}) + u^{2^{n-r}} + x^{2^m}\big)(1+x+x^{2^m})^{\frac{1}{2^r-1}}\Big)\\ & \times Tr_1^m\Big((\lambda+\mu)(1+x+x^{2^m})^{\frac{1}{2^r-1}}\Big)\\ & + Tr_1^m\Big(\big(u(1+x+x^{2^m}) + u^{2^{n-r}} + x^{2^m} + \lambda\big)(1+x+x^{2^m})^{\frac{1}{2^r-1}}\Big)\\ & \times Tr_1^m\Big(\big(u(1+x+x^{2^m}) + u^{2^{n-r}} + x^{2^m} + \mu\big)(1+x+x^{2^m})^{\frac{1}{2^r-1}}\Big)\end{aligned}$$

where u *is any element in* $\mathbb{F}_{2^n}$ *satisfying* $u + u^{2^m} = 1$.

Several new infinite families of bent functions and their duals

Construction 3 : New bent functions from the class of Maiorana-McFarland and their Duals

THEOREM

Let d be a positive integer not a power of 2 and coprime with $2^m - 1$. For $i \in \{1,2,3\}$, let $f_i(x,y) = Tr_1^m(a_i y^d x)$ for some $a_i \in \mathbb{F}_{2^m}$. Assume the a_i's are pairwise distinct such that $b := a_1 + a_2 + a_3 \neq 0$ and $a_1^{-e} + a_2^{-e} + a_3^{-e} = b^{-e}$ where e stands for the inverse of d modulo $(2^m - 1)$. Let f be the Boolean function defined in bivariate form over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ as

$$\begin{aligned} f(x,y) = {} & Tr_1^m(a_1 y^d x) Tr_1^m(a_2 y^d x) + Tr_1^m(a_1 y^d x) Tr_1^m(a_3 y^d x) \\ & + Tr_1^m(a_2 y^d x) Tr_1^m(a_3 y^d x). \end{aligned}$$

Then f is bent and its dual function is given by
$\tilde{f}(x,y) =$
$Tr_1^m(a_1^{-e} x^e y) Tr_1^m(a_2^{-e} x^e y) + Tr_1^m(a_1^{-e} x^e y) Tr_1^m(a_3^{-e} x^e y) + Tr_1^m(a_2^{-e} x^e y) Tr_1^m(a_3^{-e} x^e y)$.

The algebraic degree of f is equal to $max\Big(w_2((2d)$

$\mod 2^m - 1) + 1, \quad max_{1 \le i \le \frac{m}{2}} \big(w_2(((2^i + 1)d) \mod 2^m - 1) + 2\big)\Big).$

Several new infinite families of bent functions and their duals

An example Let $m = 4$ and $d = 7$ $(e = 13)$
Let ζ be a primitive element of $\mathbb{F}_{16}$ such that $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$.

- Then, the f function on $\mathbb{F}_{16} \times \mathbb{F}_{16}$

$$f(x,y) = Tr_1^4(y^7x)Tr_1^4((\zeta^2 + \zeta^3)y^7x) + Tr_1^4((\zeta + \zeta^3 + 1)y^7x)Tr_1^4((\zeta + \zeta^2 + 1)y^7x)$$

is bent

- The dual function of f is :

$$\tilde{f}(x,y) = Tr_1^4(yx^{13})Tr_1^4((1 + \zeta^3 + \zeta^2)yx^{13}) + Tr_1^4((\zeta + \zeta^2 + 1)yx^{13})Tr_1^4((\zeta + \zeta^3)yx^{13}).$$

- The algebraic degree of f is $\max(w_2(7) + 1, w_2(6) + 2, w_2(5) + 2) = 4$, that is, f is of optimal degree for a bent function in dimension 8. The dual function $\tilde{f}$ is of algebraic degree $\max(w_2(11) + 1, w_2(9) + 2, w_2(5) + 2) = 4$, also optimal for a bent function in dimension 8.

A consequence of Construction 3 : A particular case where $d = e = 2^m - 2$:

COROLLARY

For $i \in \{1,2,3\}$, let $f_i(x,y) = Tr_1^m(a_i y^{2^m-2} x)$ for some $a_i \in \mathbb{F}_{2^m}$ (where $0^{-1} = 0$). Assume the a_i's are pairwise distinct such that $a_1 + a_2 + a_3 \neq 0$. Let f be the Boolean function defined in bivariate form as

$$\begin{aligned} f(x,y) = {} & Tr_1^m(a_1 y^{2^m-2} x) Tr_1^m(a_2 y^{2^m-2} x) \\ & + Tr_1^m(a_1 y^{2^m-2} x) Tr_1^m(a_3 y^{2^m-2} x) \\ & + Tr_1^m(a_2 y^{2^m-2} x) Tr_1^m(a_3 y^{2^m-2} x). \end{aligned}$$

Then f belongs to the class PS_{ap} and is of degree m.

Construction 4 : New bent functions from the class of Maiorana-McFarland and their Duals

THEOREM

Let $n = 2m$ be an even positive integer which is a multiple of 4 but not of 10 (in this case $2^n - 1$ and 11 are coprime). Let d be the inverse of 11 modulo $2^n - 1$. Let c be such that $c^4 + c + 1 = 0$ and $a \in \mathbb{F}_{2^n}^\star$. Then

$$\begin{aligned} f(x,y) &= Tr_1^m(a^{-11}x^{11}y)Tr_1^m(a^{-11}c^{-11}x^{11}y) \\ &\quad + Tr_1^m(a^{-11}x^{11}y)Tr_1^m(c^{11}a^{-11}x^{11}y) \\ &\quad + Tr_1^m(a^{-11}c^{-11}x^{11}y)Tr_1^m(c^{11}a^{-11}x^{11}y) \end{aligned}$$

is bent and its dual function is given by

$$\begin{aligned} \tilde{f}(x,y) &= Tr_1^m(ay^dx)Tr_1^m(acy^dx) + Tr_1^m(ay^dx)Tr_1^m\left(ac^{-1}y^dx\right) \\ &\quad + Tr_1^m(acy^dx)Tr_1^m\left(ac^{-1}y^dx\right). \end{aligned}$$

Construction 5 : New infinite family of bent functions

Theorem

Let $m = 2r$. Let d be a positive integer coprime with $2^m - 1$. For $i \in \{1, 2, 3\}$, let $f_i(x, y) = Tr_1^m(a_i y^d x)$ for some $a_i \in \mathbb{F}_{2^m}$. Assume the a_i's are pairwise distinct such that $b := a_1 + a_2 + a_3 \neq 0$ and $a_1^{-e} + a_2^{-e} + a_3^{-e} = b^{-e}$. Let g_1, g_2 and g_3 be three Boolean functions on $\mathcal{D}_m := \{g : \mathbb{F}_{2^m} \to \mathbb{F}_2 \mid g(ax) = g(x), \forall (a, x) \in \mathbb{F}_{2^r} \times \mathbb{F}_{2^m}\}$. Let h be the Boolean function defined in bivariate form as

$$\begin{aligned} h(x,y) = {} & (Tr_1^m(a_1y^dx) + g_1(y))(Tr_1^m(a_2y^dx) + g_2(y)) \\ & + (Tr_1^m(a_1y^dx) + g_1(y))(Tr_1^m(a_3y^dx) + g_3(y)) \\ & + (Tr_1^m(a_2y^dx) + g_2(y))(Tr_1^m(a_3y^dx) + g_3(y)). \end{aligned}$$

Then h is bent and its dual function is

$$\begin{aligned} \tilde{h}(x,y) = {} & (Tr_1^m(a_1^{-e}x^ey) + g_1(x^e))(Tr_1^m(a_2^{-e}x^ey) + g_2(x^e)) \\ & + (Tr_1^m(a_1^{-e}x^ey) + g_1(x^e))(Tr_1^m(a_3^{-e}x^ey) + g_3(x^e)) \\ & + (Tr_1^m(a_2^{-e}x^ey) + g_2(x^e))(Tr_1^m(a_3^{-e}x^ey) + g_3(x^e)) \end{aligned}$$

Several new infinite families of bent functions and their duals

Construction 6 : New infinite family of bent functions from the Maiorana-McFarland completed class (that is, the smallest possible complete class containing the class of Maiorana-McFarland which is globally invariant under the action of the general affine group and under the addition of affine functions). By considering self dual bent functions in [Carlet-Danielsen-Parker-Sole 2010] :

Theorem

Let k be a positive integer such that $k \geq 2$. Let a_1, a_2, a_3 be three pairwise distinct nonzero solutions in $\mathbb{F}_{2^{4k}}$ of the equation $\lambda^{2^{3k}} + \lambda = 1$ such that $a_1 + a_2 + a_3 \neq 0$. Let g be the Boolean function over $\mathbb{F}_{2^{4k}}$ defined as

$$\begin{aligned} g(x) = {} & Tr_1^{4k}(a_1 x^{2^k+1}) Tr_1^{4k}(a_2 x^{2^k+1}) \\ & + Tr_1^{4k}(a_1 x^{2^k+1}) Tr_1^{4k}(a_3 x^{2^k+1}) \\ & + Tr_1^{4k}(a_2 x^{2^k+1}) Tr_1^{4k}(a_3 x^{2^k+1}), \forall x \in \mathbb{F}_{2^{4k}}. \end{aligned}$$

Then g is self-dual bent of algebraic degree 4.

Several new infinite families of bent functions and their duals

Construction 7 : New infinite family of cubic bent functions :

Theorem

Let $k \geq 2$ be a positive integer. Let $\lambda_2 \in \mathbb{F}_{2^{4k}}$ such that $\lambda_2 + \lambda_2^{2^{3k}} = 1$. Let $a \in \mathbb{F}_{2^{4k}}^{\star}$ be a solution of $a^{2^{2k}} + \lambda_2^{2^{-k}} a^{2^{-k}} + \lambda_2 a^{2^k} = 0$ and $\beta \in \mathbb{F}_{2^{4k}}$ such that $Tr_1^{4k}(\beta a) = Tr_1^{2k}(a^{2^{2k}+1}) + Tr_1^{4k}(\lambda_2 a^{2^k+1})$. Let g be the Boolean function over $\mathbb{F}_{2^{4k}}$ defined by

$$\begin{aligned} g(x) &= Tr_1^{2k}(x^{2^{2k}+1}) + Tr_1^{4k}(ax)Tr_1^{2k}(x^{2^{2k}+1}) \\ &+Tr_1^{4k}(ax)Tr_1^{4k}(\lambda_2(x+\beta)^{2^k+1}) + Tr_1^{4k}(ax), \forall x \in \mathbb{F}_{2^{4k}}. \end{aligned}$$

Then the cubic function g is bent and its dual function $\tilde{g}$ is given by

$$\begin{aligned} \tilde{g}(x) &= Tr_1^{2k}(x^{2^{2k}+1}) \\ &+\Big(Tr_1^{2k}(x^{2^{2k}+1}) + Tr_1^{4k}(\lambda_2 x^{2^k+1}) + Tr_1^{4k}(\beta x)\Big) \\ &\quad \times \Big(Tr_1^{4k}(a^{2^k} x) + Tr_1^{2k}(a^{2^{2k}+1})\Big), \forall x \in \mathbb{F}_{2^{4k}}. \end{aligned}$$

To apply Theorem (*) to a 3-tuple of functions of the form $f(x,y)=Tr_1^m(\phi(y)x)+g(y), \quad (x,y)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ with $g=0$, one has to choose appropriately the maps ϕ involved in their expressions.

Corollary

Let ϕ_1, ϕ_2 and ϕ_3 be three permutations of $\mathbb{F}_{2^m}$. Then,
$g(x,y)=$
$Tr_1^m(x\phi_1(y))Tr_1^m(x\phi_2(y))+Tr_1^m(x\phi_1(y))Tr_1^m(x\phi_3(y))+Tr_1^m(x\phi_2(y))Tr_1^m(x\phi_3(y))$
is bent if and only if

1. $\psi=\phi_1+\phi_2+\phi_3$ *is a permutation.*
2. $\psi^{-1}=\phi_1^{-1}+\phi_2^{-1}+\phi_3^{-1}$

Furthermore, its dual function $\tilde{g}$ is given by
$\tilde{g}(x,y)=Tr_1^m(\phi_1^{-1}(x)y)Tr_1^m(\phi_2^{-1}(x)y)+Tr_1^m(\phi_1^{-1}(x)y)Tr_1^m(\phi_3^{-1}(x)y)+$
$Tr_1^m(\phi_2^{-1}(x)y)Tr_1^m(\phi_3^{-1}(x)y)$

Several new infinite families of bent functions and their duals

In [Mesnager IEEE 2014], it has been investigated the case where ϕ is a monomial permutation. Some new bent functions have been exhibited. Here we investigate another family of permutations of $\mathbb{F}_{2^m}$:

$$\phi(x) = L(x) + L(\alpha)f(x) \quad (1)$$

where L is a linear permutation and f is a Boolean function over $\mathbb{F}_{2^m}$.

Definition

Let $\alpha \in \mathbb{F}_{2^n}^\star$ and f be a Boolean function on $\mathbb{F}_{2^n}$. α is called an a-linear structure for f if $f(x + u\alpha) + f(x) = ua$ holds for any $x \in \mathbb{F}_{2^n}$ and $u \in \mathbb{F}_2$ and a fixed $a \in \mathbb{F}_2$.

Set $\mathcal{L}_f^0 = \{\alpha \in \mathbb{F}_{2^m} \mid D_\alpha f = 0\}$ for a fixed $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$.

Proposition

Let $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a $\mathbb{F}_2$-linear permutation of $\mathbb{F}_{2^n}$. Let f a Boolean function over $\mathbb{F}_{2^n}$ and α be a 0-linear structure of f. Then ϕ defined by (1) is a permutation of $\mathbb{F}_{2^m}$ and $\phi^{-1}(x) = L^{-1}(x) + \alpha f(L^{-1}(x))$.

If we take α to be a 1-linear structure of f then $F(x) = L(x) + L(\alpha)f(x)$ is 2-to-1.

Several new infinite families of bent functions and their duals

THEOREM

Let L be a linear permutation on $\mathbb{F}_{2^m}$. Let f be a Boolean function over $\mathbb{F}_{2^m}$ such that $\mathcal{L}_f^0$ is of dimension at least two over $\mathbb{F}_2$. Let $(\alpha_1, \alpha_2, \alpha_3)$ be any 3-tuple of pairwise distinct elements of $\mathcal{L}_f^0$. Then the Boolean function g defined in bivariate representation on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$\begin{aligned} g(x,y) = Tr_1^m(xL(y)) + f(y)\Big(&Tr_1^m(L(\alpha_1)x)Tr_1^m(L(\alpha_2)x) \\ &+ Tr_1^m(L(\alpha_1)x)Tr_1^m(L(\alpha_3)x) + Tr_1^m(L(\alpha_2)x)Tr_1^m(L(\alpha_3)x)\Big) \end{aligned}$$

is bent and its dual function $\tilde{g}$ is given by
$\tilde{g}(x,y) = Tr_1^m(L^{-1}(x)y)$
$+ f(L^{-1}(x))\Big(Tr_1^m(\alpha_1 y)Tr_1^m(\alpha_2 y) + Tr_1^m(\alpha_1 y)Tr_1^m(\alpha_3 y) + Tr_1^m(\alpha_2 y)Tr_1^m(\alpha_3 y)\Big)$

To find a Boolean function f such that $\mathcal{L}_f^0$ is of dimension at least 2 : if $m = rk$ with r even and $k \geq 2$, candidates are functions of the form $f(x) = h(Tr_k^m(x))$ where h is a Boolean function over $\mathbb{F}_{2^k}$. Many other examples can be found.

We introduce a new infinite family of permutations involving any Boolean functions as well as their compositional inverses.

THEOREM

Let $m = 2k$ be a even positive integer. Let $a \in \mathbb{F}_{2^k}$ and $b \in \mathbb{F}_{2^m}$ such that $b^{2^k+1} \neq a^2$. Let g be a Boolean function over $\mathbb{F}_{2^k}$. Set $\rho = a + b^{2^k}$ and

$$\phi(x) = ax + bx^{2^k} + g(Tr_k^m(\rho x)),\ x \in \mathbb{F}_{2^m}. \tag{1}$$

Then ϕ is a permutation of $\mathbb{F}_{2^m}$ and its inverse is

$$\phi^{-1}(x) = \alpha^{-1}\left(ax + bx^{2^k} + (a+b)g(Tr_k^m(x))\right) \tag{2}$$

where $\alpha = b^{2^k+1} + a^2 \neq 0$.

Several new infinite families of bent functions and their duals

Theorem

Let $m = 2k$. Let $a \in \mathbb{F}_{2^k}$ and $b \in \mathbb{F}_{2^m}$ such that $b^{2^m+1} \neq a^2$. Set $\alpha = b^{2^k+1} + a^2$ and $\rho = a + b^{2^k}$. Let g_1, g_2 and g_3 be three Boolean functions over $\mathbb{F}_{2^k}$. Then the Boolean function h defined in bivariate representation on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$\begin{aligned} h(x,y) &= Tr_1^m(axy + bxy^{2^k}) + Tr_1^m(xg_1(Tr_k^m(\rho y)))Tr_1^m(xg_2(Tr_k^m(\rho y))) \\ &\quad +Tr_1^m(xg_1(Tr_k^m(\rho y)))Tr_1^m(xg_3(Tr_k^m(\rho y))) \\ &= \quad Tr_1^m(xg_2(Tr_k^m(\rho y)))Tr_1^m(xg_3(Tr_k^m(\rho y))) \end{aligned}$$

is bent and its dual function $\tilde{h}$ is given by

$$\begin{aligned} \tilde{h}(x,y) &= Tr_1^m(\alpha^{-1}(axy + bx^{2^k}y)\Big) \\ &\quad +Tr_1^m\Big(\alpha^{-1}(a+b)yg_1\left(Tr_k^m(x)\right)\Big)Tr_1^m\Big(\alpha^{-1}(a+b)yg_2\left(Tr_k^m(x)\right)\Big) \\ &\quad +Tr_1^m\Big(\alpha^{-1}(a+b)yg_1\left(Tr_k^m(x)\right)\Big)Tr_1^m\Big(\alpha^{-1}(a+b)yg_3\left(Tr_k^m(x)\right)\Big) \\ &\quad +Tr_1^m\Big(\alpha^{-1}(a+b)yg_2\left(Tr_k^m(x)\right)\Big)Tr_1^m\Big(\alpha^{-1}(a+b)yg_3\left(Tr_k^m(x)\right)\Big). \end{aligned}$$

"Secondary" construction of mappings leading to serval families of bent functions

Let m be a positive integer.
A set $\{\phi_1, \phi_2, \phi_3\}$ of three permutations of $\mathbb{F}_{2^m}$ are said to satisfy (A_m) if and only if

1. Their sum $\psi = \phi_1 + \phi_2 + \phi_3$ is a permutation of $\mathbb{F}_{2^m}$.
2. It holds $\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$.

"Secondary" construction of mappings leading to serval families of bent functions

Let m be a positive integer.
A set $\{\phi_1, \phi_2, \phi_3\}$ of three permutations of $\mathbb{F}_{2^m}$ are said to satisfy (A_m) if and only if

1. Their sum $\psi = \phi_1 + \phi_2 + \phi_3$ is a permutation of $\mathbb{F}_{2^m}$.
2. It holds $\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$.

Let m be a positive integer. Let ϕ_1, ϕ_2, ϕ_3 be three permutations satisfying (A_m). Let n be any non-zero multiple of m (different from m). Let ρ be a permutation of $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Define ψ_1, ψ_2, ψ_3 on $\mathbb{F}_{2^n}$ by

$$i \in \{1,2,3\},\ \psi_i(x) = \begin{cases} \phi_i(x) & \text{if } x \in \mathbb{F}_{2^m} \\ \rho(x) & \text{if } x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m} \end{cases}$$

One can generate many families of bent functions using the following result :

PROPOSITION

$\{\psi_1, \psi_2, \psi_3\}$ *satisfies* (A_n) *if and only if* $\{\phi_1, \phi_2, \phi_3\}$ *satisfies* (A_m)

Conclusion

The results presented here :

- published in [Mesnager IEEE 2014]
- new results :
  1. two new infinite families of bent functions with their duals functions ;
  2. an infinite new family of permutations ;
  3. a "secondary" construction of permutations leading to the construction of many families of bent functions.

Quite fascinatingly, despite its simplicity and the conditions that seem restrictive at first, we have derived from the secondary construction [Carlet 2006] several infinite families of bent Boolean functions. A very important point is that we can provide the dual functions of all their elements which is rarely achieved.

Future work and work in progress

- Constructions of new semi-bent and near-bent functions,
- Constructions of new vectorial bent functions
- Check whether the bent functions presented in this talk are affinely inequivalent to known constructions or not.
- Study their other cryptographic properties,
- etc.