A few observations on APN and AB functions

Claude Carlet
University of Paris 8 (MAATICAH), France

Outline

- PN (bent), APN and AB functions : definitions, properties and equivalence notions (EA-equivalence, CCZ-equivalence)
- The first known APN and AB functions (power functions in finite fields) and the related CCZ-equivalent functions
- Recently found APN and AB functions, new up to CCZ-equivalence, and their properties
- Open problems and observations

PN (bent), APN and AB functions : definitions, properties and equivalence notions

PN and APN functions :

For $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, let :

$$\delta_F(a,b) = |\{x \in \mathbb{F}_2^n : F(x+a)+F(x) = b\}|; \quad a \in \mathbb{F}_2^n \backslash \{0\}; \quad b \in \mathbb{F}_2^m.$$

Let $\delta = \max_{a \in \mathbb{F}_2^n \backslash \{0\}, b \in \mathbb{F}_2^m} \delta_F(a,b)$. We have : $\delta \geq 2^{n-m}$.

If $\delta = 2^{n-m}$, then F is called *Bent* (B) or *Perfect Nonlinear* (PN) :
- All the derivatives $D_a F(x) = F(x) + F(x+a)$, $a \neq 0$ are balanced.
- Equivalently : all component functions $v \cdot F$, $v \neq 0$ are bent.

Best resistance to differential attack.

K. Nyberg : Bent functions exist only when n is even and $m \leq n/2$.

If $m = n$, then δ is lower bounded by 2.

If $\delta = 2$, then F is called *almost perfect nonlinear* (APN).

AB functions :

The nonlinearity of an S-box F is the minimum Hamming distance between :
- all *component functions* $v \cdot F(x)$, $v \in \mathbb{F}_2^m \setminus \{0\}$
- and all *affine functions* $u \cdot x + \epsilon$, $u \in \mathbb{F}_2^n$, $\epsilon \in \mathbb{F}_2$.

The nonlinearity is related to the spectrum of the *Walsh transform*

$$W_F(u,v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x}, \qquad u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m.$$

The set $W_F = \{|W_F(u,v)| : u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m \setminus \{0\}\}$ is called the *extended Walsh spectrum* of F.

The nonlinearity equals :

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m \setminus 0} |W_F(u,v)|.$$

If $m = n$ and if we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ then we can take : $x \cdot y = tr(x\,y)$. We have then :

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

Bounds on the nonlinearity :

The *covering radius bound* states :

$$\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1} \quad \text{with equality iff } F \text{ is bent.}$$

(best resistance to linear attack).

The *Sidelnikov-Chabaud-Vaudenay bound* states that if $m = n$ then :

$$\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}.$$

In case of equality (n necessarily odd) F is called *almost bent* (AB).

From now on, we assume that $m = n$.

Properties

For any AB function F, the ext. Walsh spectrum W_F equals $\{0, 2^{\frac{n+1}{2}}\}$.

Every AB function is APN (Chabaud-Vaudenay).

The converse is not true in general, even in the n odd case (counter-examples : inverse function, Dobbertin function).

The converse is true for n odd if we assume some additionnal condition on F (Canteaut, Charpin and Dobbertin) : the Walsh spectrum is divisible by $2^{\frac{n+1}{2}}$.

This implies that, if n is odd, then for every *quadratic* or more generally *plateaued* function, APN $\Rightarrow$ AB.

Plateaued :

$$\forall u, \forall v \neq 0, W_F(u, v) \in \{0, \pm\lambda_v\}.$$

Different kinds of equivalence for APN and AB functions :

- *Extended affine equivalence* (EA-equivalence) :

$$F' = A_1 \circ F \circ A_2 + A$$

for some affine permutations A_1, A_2 and an affine function A.

- *CCZ equivalence* : the graphs

$$\{(x, F(x)) \mid x \in \mathbb{F}_2^n\} \text{ and } \{(x, G(x)) \mid x \in \mathbb{F}_2^n\}$$

are affine equivalent.

Any permutation is CCZ-equivalent to its inverse.

CCZ-equivalence between two functions F and G is more general than EA-equivalence between F and G or F and G^{-1} or F^{-1} and G^{-1}.

CCZ-equivalence respects APNness and ABness.
It does not respect the algebraic degree, while EA equivalence does.

The first known APN and AB functions (power functions in finite fields) and the related CCZ-equivalent functions

Exponents d such that $F(x) = x^d$ is APN on $\mathbb{F}_{2^n}$ up to EA-equivalence and inverse

- Gold functions : $d = 2^i + 1$, with $\gcd(i, n) = 1$
- Kasami functions : $d = 2^{2i} - 2^i + 1$, with $\gcd(i, n) = 1$ *(Janwa, Wilson, 1993)*
- Welch function : $d = 2^t + 3$, $n = 2t + 1$ *(Dobbertin, 1999)*
- Niho functions : $d = 2^t + 2^{\frac{t}{2}} - 1$, if $n = 2t + 1$, t even ; *(Dobbertin, 1999)*
  $d = 2^t + 2^{\frac{3t+1}{2}} - 1$, if $n = 2t + 1$, t odd
- Inverse function : $d = 2^{2t} - 1$, with $n = 2t + 1$ *(Beth, Ding, Nyberg, 1993)*
- Dobbertin function : $d = 2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$, if $n = 5t$ *(Dobbertin, 2000)*

Conjecture (Dobbertin) :
This list of APN power functions is complete.

Proved (Dobbertin) :
APN power functions are permutations of $\mathbb{F}_{2^n}^*$ if n is odd, and are three-to-one if n is even.

Exponents d that x^d is AB on $\mathbb{F}_{2^n}$ up to EA-equivalence and inverse

- Gold functions : $d = 2^i + 1$, with $\gcd(i, n) = 1$ *(Gold, 1968)*
- Kasami functions : $d = 2^{2i} - 2^i + 1$, with $\gcd(i, n) = 1$ *(Kasami, 1971)*
- Welch function : $d = 2^t + 3$, $n = 2t + 1$ *(Canteaut, Charpin, Dobbertin, 2000)*
- Niho function : $n = 2t + 1$; $d = 2^t + 2^{\frac{t}{2}} - 1$ if t even *(Hollman, Xiang, 2001)*
  $d = 2^t + 2^{\frac{3t+1}{2}} - 1$ if t odd

Existence of APN non-power functions (up to equivalence) ?

- Functions $\sum_{i=0}^{n-1} c_i x^{2^i+1}$; $c_i \in \mathbb{F}_{2^n}$, are not APN, except Gold (Berger, Canteaut, Charpin, Laigle-Chapuy)

- *Budaghyan, C.C. and Pott* obtained "new" APN and AB functions from Gold functions by using CCZ-equivalence :

1. $F(x) = x^{2^i+1} + (x^{2^i} + x)\, tr(x^{2^i+1} + x)$,
where $n > 3$ *is odd,* $gcd(n, i) = 1$, *is AB.*
It is EA-inequivalent to any power function and to any permutation.

2. $F(x) = x^{2^i+1} + (x^{2^i} + x + 1)\, tr(x^{2^i+1})$, *where* $n \geq 4$ *is even,* $gcd(n, i) = 1$ *is APN.*
It is EA-inequivalent to any power function.

3. For n even and divisible by 3, the function

$$[x + tr_{n/3}(x^{2(2^i+1)} + x^{4(2^i+1)}) + tr(x)\, tr_{n/3}(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1},$$

where $gcd(n,i) = 1$, $tr_{n/3}(x) = \sum_{i=0}^{n/3-1} x^{2^{3i}}$ is APN and is EA-inequivalent to any known APN function.

4. For n odd and divisible by m, $n \neq m$ and $\gcd(n,i) = 1$, the function

$$x^{2^i+1} + tr_{n/m}(x^{2^i+1}) + x^{2^i} tr_{n/m}(x) + x\ tr_{n/m}(x)^{2^i} +$$

$$[tr_{n/m}(x)^{2^i+1} + tr_{n/m}(x^{2^i+1}) + tr_{n/m}(x)]^{\frac{1}{2^i+1}}(x^{2^i} + tr_{n/m}(x)^{2^i} + 1) +$$

$$[tr_{n/m}(x)^{2^i+1} + tr_{n/m}(x^{2^i+1}) + tr_{n/m}(x)]^{\frac{2^i}{2^i+1}}(x + tr_{n/m}(x))$$

from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ is an AB function of algebraic degree $m+2$ which is EA-inequivalent to any power function.

Next step : existence of APN functions *new* (non-power) *up to CCZ-equivalence*?

Recently found APN and AB functions, new up to CCZ-equivalence, and their properties

1. *L. Budaghyan, C.C. and G. Leander* have found two classes of binomial APN quadratic functions generalizing a sporadic example found by Edel, Kyureghyan and Pott.

Common framework (observed by Bierbrauer) for these two classes :

- $n = tk$; $t \in \{3, 4\}$,
- t, s, k pairwise coprime and $t \,|\, k + s$,
- α a primitive element of $\mathbb{F}_{2^n}$ and $w = \alpha^e$, where e is a multiple of $2^k - 1$, coprime with $2^t - 1$:

$$F(x) = x^{2^s+1} + wx^{2^{k+s}+2^{k(t-1)}}.$$

For $n \geq 12$, these functions are EA-inequivalent to power functions and CCZ-inequivalent to Gold and Kasami mappings.
In particular, for $n = 12, 20, 24, 28$ they are CCZ-inequivalent to all power functions.

The class above with $t = 3$ has been generalized by *C. Bracken, E. Byrne, N. Markin and G. McGuire* :

$$F(x) = u^{2^k} x^{2^{-k}+2^{k+s}} + ux^{2^s+1} + vx^{2^{-k}+1} + wu^{2^k+1} x^{2^{k+s}+2^s}$$

is APN on $\mathbb{F}_{2^{3k}}$, when $3 \,|\, k+s$, $(s, 3k) = (3, k) = 1$ and u is primitive in $\mathbb{F}_{2^{3k}}$, $v \neq w^{-1} \in \mathbb{F}_{2^k}$.

2. *L. Budaghyan, C.C., G. Leander* :

Let n be any positive integer. Then the function $x^3 + tr(x^9)$ is APN on $\mathbb{F}_{2^n}$.

This function is CCZ-inequivalent to any Gold function on $\mathbb{F}_{2^n}$ if $n \geq 7$ and $n > 2p$ where p is the smallest positive integer different from 1 and 3 and coprime with n.

C. Bracken, E. Byrne, N. Markin, G. McGuire (Cirencester 2007) : the extended Walsh spectrum of this function is the same as for Gold function.

3. An idea of *J. Dillon* : try functions of the form :

$$F(x) = x(Ax^2 + Bx^q + Cx^{2q}) + x^2(Dx^q + Ex^{2q}) + Gx^{3q},$$

where $q = 2^{n/2}$, n even.

L. Budaghyan, C.C. (pushing further Dillon's idea) :
Let n be even and i be co-prime with $n/2$. Set $q = 2^{n/2}$ and let $c, b \in \mathbb{F}_{2^n}$ be such that $c^{q+1} = 1$, $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $cb^q + b \neq 0$. Then the function

$$F(x) = x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$$

is APN on $\mathbb{F}_{2^n}$.

Such vectors b, c do exist if and only if $\gcd(2^i + 1, q + 1) \neq 1$. For $n/2$ odd, this is equivalent to saying that i is odd.

4. *L. Budaghyan, C.C.* :

Let n be even and i be co-prime with $n/2$. Set $q = 2^{n/2}$ and let $c \in \mathbb{F}_{2^n}$ and $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$. If the polynomial

$$X^{2^i+1} + cX^{2^i} + c^q X + 1$$

is irreducible over $\mathbb{F}_{2^n}$, then the function

$$F(x) = x(x^{2^i} + x^q + cx^{2^i q}) + x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$$

is APN on $\mathbb{F}_{2^n}$.

We checked with a computer for $n = 6$ that some of the functions of cases 3 and 4 are CCZ-inequivalent to power functions on $\mathbb{F}_{2^6}$. It remains open to prove this for every even $n \geq 6$.

5. *C. Bracken, E. Byrne, N. Markin, G. McGuire* :

$$F(x) = bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^k+1} + \sum_{i=1}^{k-1} r_i x^{2^{i+k}+2^i}$$

where k, s are odd and coprime, $b, c \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$, $r_i \in \mathbb{F}_{2^k}$ is APN on $\mathbb{F}_{2^{2k}}$.

The extended Walsh spectrum of this function is the same as for Gold function.

Open problems and observations

1. Find a better bound than the covering radius bound for :

- n odd and $m < n$;
- n even and $n/2 < m < n$.

2. Find new PN functions $F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^{n/2}$.

Mainly, two primary constructions are known (K. Nyberg) :

- the Maiorana-McFarland construction (and a variant) :

$$(x, y) \in \mathbb{F}_{2^{n/2}} \longrightarrow x\pi(y) + G(y),\ \pi \text{ bijective};$$

- the Dillon construction :

$$(x, y) \in \mathbb{F}_{2^{n/2}} \longrightarrow G\left(\frac{x}{y}\right),\ G \text{ balanced.}$$

Observation : two secondary constructions of PN S-boxes can be derived from constructions of Boolean bent functions.
The simplest (and probably most effective) is :

Proposition 1 *Let r and s have the same evenness ; $r \leq \frac{s}{3}$.*
Let $\psi : \mathbb{F}_2^s \to \mathbb{F}_{2^r}$ be such that $\psi^{-1}(a)$ is an $(s-r)$-dimensional flat of $\mathbb{F}_2^s$, for every $a \in \mathbb{F}_{2^r}$.
Let $H : \mathbb{F}_2^s \to \mathbb{F}_{2^r}$ be bent on $\psi^{-1}(a)$ for every $a \in \mathbb{F}_{2^r}$.
Then $F_{\psi,H}(x,y) = x\,\psi(y) + H(y)$, $x \in F_{2^r}, y \in F_2^s$, is bent.

But it gives $F_{\psi,H} : \mathbb{F}_2^n \to \mathbb{F}_{2^r}$ with $r \leq \frac{n}{4}$.

3. Find secondary constructions of APN functions.

Observation : the method above can give functions $F_{\psi,H} : \mathbb{F}_2^n \to \mathbb{F}_{2^r}$ with extended Walsh spectrum $\{0, \pm 2^{\frac{n+1}{2}}\}$ but with $r \leq \frac{n}{3}$.

4. Find constructions of APN/AB functions from PN, and *vice versa*.

5. Find classes of APN functions by using CCZ-equivalence with Kasami (resp. Welch, Niho, Dobbertin) functions.

6. Find classes of APN functions CCZ-inequivalent to power functions and to quadratic functions.

7. Find APN permutations with n even, or prove they cannot exist.

Observation : If APN permutations exist for n even, they are :
- neither power functions (Dobbertin),
- nor in $\mathbb{F}_2[x]$ (Hou),
- nor plateaued (Nyberg for partially-bent component functions) :

Proposition 2 *Let n be even. Let F be a plateaued APN function from $\mathbb{F}_2^n$ to itself. Then the number of bent functions among the functions $v \cdot F$ is at least $\frac{2}{3}(2^n - 1)$.*

8. Classify the extended Walsh spectra of APN functions.

Observations :

For n odd, the known APN functions have three possible spectra :

- the spectrum of the AB functions (e.g. the Gold functions) which gives a nonlinearity of $2^{n-1} - 2^{\frac{n-1}{2}}$,
- the spectrum of the inverse function, which takes any value divisible by 4 in the range $[-2^{n/2+1} + 1; 2^{n/2+1} + 1]$ and gives a nonlinearity close to $2^{n-1} - 2^{n/2}$,
- the spectrum of the Dobbertin function which is more complex (it is divisible by $2^{n/5}$ and not divisible by $2^{2n/5+1}$) ; its nonlinearity seems equal to $2^{n-1} - 2^{3n/5-1} - 2^{2n/5-1}$.

For n even, the spectra may be more diverse :

- the Gold functions,
- the Dobbertin function,
- As soon as $n \geq 6$, we find (quadratic) functions with different spectra.

The nonlinearities seem also lower bounded by approximately $2^{n-1} - 2^{3n/5-1} - 2^{2n/5-1}$.

Open question : is this situation general to all APN functions or specific to the APN functions found so far ?

Proposition 3 *Let F be an APN function in $n > 2$ variables. Then*
- the nonlinearity of F cannot be null;
- for every real numbers a and b such that $a \leq b$, let $N_{a,b}$ be the number of ordered pairs $(u, v) \in F_2^n \times (F_2^n \setminus \{0\})$ such that $W^2_{v \cdot F}(u) \in]2^n + a; 2^n + b[$. Then the nonlinearity of F is lower bounded by

$$2^{n-1} - \frac{1}{2}\sqrt{2^n + \frac{1}{2}(b + a + \sqrt{\Delta_{a,b}})},$$

where $\Delta_{a,b} = (N_{a,b} + 1)(b - a)^2 + a\, b\, 2^{n+2}(2^n - 1) + 2^{4n+2} - 2^{3n+2}$.

Consequences :

- if $W^2_{v \cdot F}(u)$ does not take values in the range $]0; 2^{n+1}[$, then F is AB (known).

- more generally, if $W^2_{v \cdot F}(u)$ does not take values in the range $]2^n - \frac{2^{2n}}{b}; 2^n + b[$ for some $b\,(\geq 2^n)$, the nonlinearity of F is lower bounded by $2^{n-1} - \frac{1}{2}\sqrt{2^n + b}$.