On the Carlet-Charpin-Zinoviev Paper

Lilya Budaghyan

Selmer Center
University of Bergen
Norway

BFA 2019
International Workshop on Boolean Functions and Their Applications
Florence, Italy
June 17, 2019

Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems

Dedicated to APN and AB functions

CLAUDE CARLET, PASCALE CHARPIN, VICTOR ZINOVIEV

Designs, Codes and Cryptography, 15, 125–156 (1998)

APN and AB Functions

Almost perfect nonlinear (APN) and almost bent (AB) functions

- are vectorial Boolean functions optimal for primary cryptographic criteria (differential and linear cryptanalyses);
- are UNIVERSAL - they define optimal objects in several branches of mathematics and information theory (coding theory, sequence design, projective geometry, combinatorics, commutative algebra);
- are "HARD-TO-GET" - there are only a few known constructions (12 AB, 17 APN);
- are "HARD-TO-PREDICT" - most conjectures are proven to be false.

Main results of CCZ-paper

- Upper bound on algebraic degrees of AB functions
- Property of stability for APN and AB functions
- Quadratic APN for odd dimensions implies AB
- Characterisation of APN and AB functions via Boolean function γ
- Characterisation of APN and AB functions via codes

Main problems inspired by CCZ-paper

- Upper bound on algebraic degrees of APN functions [B., Carlet, Helleseth, Li 2016]
- New equivalence relations invariant for APN and AB properties
- For every AB function F, existence of linear L such that $F + L$ is a permutation [B., Carlet, Pott 2005]
- Existence of quadratic AB functions different from Gold power maps [B., Carlet, Leander 2006]
- Finding γ functions for known APN and AB functions [B., Carlet, Helleseth 2011]
- Existence of APN permutations for even dimensions [Dillon et al 2009]

Univariate representation and algebraic degree

The univariate representation of an (n, m)-function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ for $m|n$:

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, \quad c_i \in \mathbb{F}_{2^n}.$$

The univariate degree of F is the degree of its univariate representation.

Algebraic degree of F

$$d^\circ(F) = \max_{0 \le i < 2^n, c_i \neq 0} w_2(i),$$

where $w_2(i)$ is the binary weight of i.

Trace and Component functions

Trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ for $m|n$:

$$tr_n^m(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}.$$

Absolute trace function:

$$tr_n(x) = tr_n^1(x) = \sum_{i=0}^{n-1} x^{2^i}.$$

For $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and $v \in \mathbb{F}_{2^m}^*$

$$tr_m(vF(x))$$

is a component function of F.

Differential Uniformity and APN Functions

- Differential cryptanalysis of block ciphers was introduced by Biham and Shamir in 1991.
- $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is differentially δ-uniform if

$$F(x+a) + F(x) = b, \qquad \forall a \in \mathbb{F}_{2^n}^*, \quad \forall b \in \mathbb{F}_{2^n},$$

  has at most δ solutions.
- Differential uniformity measures the resistance to differential attack [Nyberg 1993].
- F is almost perfect nonlinear (APN) if $\delta = 2$.
- APN functions are optimal for differential cryptanalysis.

First examples of APN functions [Nyberg 1993]:

- Gold function x^{2^i+1} on $\mathbb{F}_{2^n}$ with $\gcd(i, n) = 1$;
- Inverse function x^{2^n-2} on $\mathbb{F}_{2^n}$ with n odd.

Nonlinearity of Functions

- Linear cryptanalysis was discovered by Matsui in 1993.
- Distance between two Boolean functions:

$$d(f,g) = |\{x \in \mathbb{F}_{2^n} : f(x) \neq g(x)\}|.$$

- Nonlinearity of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$:

$$N_F = \min_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_2, v \in \mathbb{F}_{2^m}^*} d(tr_m(v\,F(x), tr_n(ax) + b)$$

- Nonlinearity measures the resistance to linear attack [Chabaud and Vaudenay 1994].

Bent and Almost Bent Functions

- $N_F \leq 2^{n-1} - 2^{n/2-1}$ for an (n, m)-function F.
  Functions achieving the bound are called bent.
  They exist iff n is even and $m \leq n/2$.

- If $m = n$ then $N_F \leq 2^{n-1} - 2^{\frac{n-1}{2}}$.
  Functions achieving the bound are called almost bent (AB).
  They exist only for n odd.

- AB functions are optimal for linear cryptanalysis.

- F is maximally nonlinear if $n = m$ is even and
  $N_F = 2^{n-1} - 2^{\frac{n}{2}}$ (conjectured optimal).

AB Functions

- If F is AB then it is APN.
- If n is odd and F is quadratic APN then F is AB [CCZ].
- Algebraic degrees of AB functions are upper bounded by $\frac{n+1}{2}$ [CCZ].

First example of AB functions:

- Gold functions x^{2^i+1} on $\mathbb{F}_{2^n}$ with $\gcd(i, n) = 1$, *n odd*;
- Gold APN functions with n even are not AB;
- Inverse functions are not AB.

Importance of Equivalence Relations for Functions

Equivalence relations preserving main cryptographic properties (APN and AB) divide the set of all functions into classes.

- They can be powerful construction methods providing for each function a huge class of functions with the same properties.
- Instead of checking invariant properties for all functions, it is enough to check only one in each class.

Cyclotomic, Linear, Affine, EA- and EAI- Equivalences

- F and F' are affine (resp. linear) equivalent if

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

  for some affine (resp. linear) permutations A_1 and A_2.

- F and F' are *extended affine equivalent* (EA-equivalent) if

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

  for some affine permutations A_1 and A_2 and some affine A.

- F and F' are EAI-equivalent if F' is obtained from F by a sequence of applications of EA-equivalence and inverses of permutations.

- Functions x^d and $x^{d'}$ over $\mathbb{F}_{2^n}$ are cyclotomic equivalent if $d' = 2^i \cdot d \mod (2^n - 1)$ or, $d' = 2^i / d \mod (2^n - 1)$ (if $\gcd(d, 2^n - 1) = 1$).

Invariants and Relation Between Equivalences

- Linear equivalence $\subset$ affine equivalence $\subset$ EA-equivalence $\subset$ EAI-equivalence.
- Cyclotomic equivalence $\subset$ EAI-equivalence.
- APNness, ABness and resistance to algebraic attack are preserved by EAI-equivalence.
- Algebraic degree is preserved by EA-equivalence but not by EAI-equivalence.
- Permutation property is preserved by cyclotomic and affine equivalences (not by EA- or EAI-equivalences).

Known AB power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions on n odd
Gold (1968)	$2^i + 1$	$\gcd(i, n) = 1$, $1 \leq i < n/2$
Kasami (1971)	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$, $2 \leq i < n/2$
Welch (conj.1968)	$2^m + 3$	$n = 2m + 1$
Niho (conjectured in 1972)	$2^m + 2^{\frac{m}{2}} - 1$, m even $2^m + 2^{\frac{3m+1}{2}} - 1$, m odd	$n = 2m + 1$

Welch and Niho cases were proven by Canteaut, Charpin, Dobbertin (2000) and Hollmann, Xiang (2001), respectively.

Known APN power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions
Gold	$2^i + 1$	$\gcd(i, n) = 1$, $1 \leq i < n/2$
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$, $2 \leq i < n/2$
Welch	$2^m + 3$	$n = 2m + 1$
Niho	$2^m + 2^{\frac{m}{2}} - 1$, m even $2^m + 2^{\frac{3m+1}{2}} - 1$, m odd	$n = 2m + 1$
Inverse	$2^{n-1} - 1$	$n = 2m + 1$
Dobbertin	$2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$	$n = 5m$

- This list is up to cyclotomic equivalence and is conjectured complete (Dobbertin 1999).
- For n even the Inverse function is differentially 4-uniform and maximally nonlinear and is used as S-box in AES with $n = 8$.

Open problems in the beginning of 2000

- All known APN functions were power functions up to EA-equivalence.
- Power APN functions are permutations for n odd and 3-to-1 for n even.

Open problems:

1. Existence of APN polynomials (EA-)inequivalent to power functions.
2. Existence of APN permutations over $\mathbb{F}_{2^n}$ for n even.

First example for Problem 1 [B., 2003]:

$$F^*(x) = x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^5$$

over $\mathbb{F}_{16}$.

Another equivalence?

Property of stability [CCZ]
Let F be APN (resp. AB) on $\mathbb{F}_{2^n}$ and L_1, L_2 be affine functions from $\mathbb{F}_{2^n}^2$ to $\mathbb{F}_{2^n}$. If (L_1, L_2) is a permutation on $\mathbb{F}_{2^n}^2$ and $F_1(x) = L_1(x, F(x))$ is a permutation on $\mathbb{F}_{2^n}$ then, $F_2 \circ F_1^{-1}$ is APN (resp. AB), where $F_2(x) = L_2(x, F(x))$.
EAI-equivalence is a particular case of property of stability.

At YACC 2004 Canteaut, Carlet, Dobbertin were aware of the example F^* (independently found by Knutsen) and searching for its infinite family.

The property of stability was "rediscovered" by Breveglieri, Cherubini, Macchetti (Asiacrypt 2004).

CCZ-Equivalence

The *graph of a function* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is the set

$$G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}.$$

F and F' are CCZ-equivalent if $\mathcal{L}(G_F) = G_{F'}$ for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ [B., Carlet, Pott 2005].

CCZ-equivalence

- preserves differential uniformity, nonlinearity, and resistance to algebraic attack.
- is more general than EAI-equivalence [BCP 2005].
- was used to solve the problems:
  - There exist AB functions EA-inequivalent to any permutation [B., Carlet, Pott 2005].
  - For n even there exist APN permutations for $n = 6$ [Dillon et al. 2009].

First Classes of APN Maps EAI-ineq. to Monomials

APN and AB functions CCZ-equivalent to Gold functions and EAI-inequivalent to power functions on $\mathbb{F}_{2^n}$ [BCP 2005].

Functions	Conditions
$x^{2^i+1} + (x^{2^i} + x + \mathrm{tr}_n(1) + 1)\mathrm{tr}_n(x^{2^i+1} + x\,\mathrm{tr}_n(1))$	$n \geq 4$ $\gcd(i, n) = 1$
$[x + \mathrm{tr}_n^3(x^{2(2^i+1)} + x^{4(2^i+1)}) + \mathrm{tr}_n(x)\mathrm{tr}_n^3(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1}$	$6\|n$ $\gcd(i, n) = 1$
$x^{2^i+1} + \mathrm{tr}_n^m(x^{2^i+1}) + x^{2^i}\mathrm{tr}_n^m(x) + x\,\mathrm{tr}_n^m(x)^{2^i}$ $+[\mathrm{tr}_n^m(x)^{2^i+1} + \mathrm{tr}_n^m(x^{2^i+1}) + \mathrm{tr}_n^m(x)]^{\frac{1}{2^i+1}}(x^{2^i} + \mathrm{tr}_n^m(x)^{2^i} + 1)$ $+[\mathrm{tr}_n^m(x)^{2^i+1} + \mathrm{tr}_n^m(x^{2^i+1}) + \mathrm{tr}_n^m(x)]^{\frac{2^i}{2^i+1}}(x + \mathrm{tr}_n^m(x))$	$m \neq n$ n odd $m\|n$ $\gcd(i, n) = 1$

The first function F is AB such that $F + L$ is not a permutation for any linear L.

- An AB function is not necessarily EA-equivalent to a permutation.

Relation Between Equivalences

- Two power functions are CCZ-equivalent iff they are cyclotomic equivalent [Dempwolff; Yoshiara 2018].
- For Gold APN monomials and quadratic APN polynomials CCZ$>$EAI [B., Carlet, Pott 2005; B., Carlet, Leander 2009].
- CCZ$=$EAI for non-quadratic power APN with $n \leq 7$ [B., Calderini, Villa 2019].
- CCZ$>$EAI for non-power non-quadratic APN functions [B., Calderini, Villa 2019].

CCZ- and EA- Equivalences

Cases when CCZ-equivalence coincides with EA-equivalence:

- Boolean functions [B., Carlet 2009].
- All bent functions [B., Carlet 2009].
- Two quadratic APN functions [Yoshiara 2012].
- A quadratic APN function is CCZ-equivalent to a power function iff it is EA-equivalent to one of the Gold functions [Yoshiara 2018].

Cases when CCZ-equivalence differs from EA-equivalence:

- For functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \geq 2$ [B., Carlet 2009; Pott, Zhou 2013].

CCZ-construction of Bent Functions

Although for bent functions CCZ -and EA-equivalences coincide, constructing new bent functions using CCZ-equivalence is possible [B., Carlet 2011].

A few infinite families of bent Boolean and vectorial functions are constructed by applying CCZ-equivalence to non-bent vectorial functions with bent components.

Example $F'(x) = x^{2^i+1} + (x^{2^i} + x + 1)\mathrm{tr}_n(x^{2^i+1})$ and $F(x) = x^{2^i+1}$ are CCZ-equivalent on $\mathbb{F}_{2^n}$.
$f(x) = \mathrm{tr}_n(bF'(x))$ is cubic bent when $n/gcd(n,i)$ even, $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^i}$ s.t. neither b nor $b+1$ are (2^i+1)-th powers.

Big APN problem

Do APN permutations exist for n even?

Negative results:

- no for quadratics [Nyberg 1993],
- no for $F \in \mathbb{F}_{2^4}[x]$ if $n/2$ is even [Hou 2004],
- no for $F \in \mathbb{F}_{2^{n/2}}[x]$ [Hou 2004].

CCZ-construction of APN permutation for n even

The only known APN permutation for n even [Dillon et al 2009]:

- Applying CCZ-equivalence to quadratic APN on $\mathbb{F}_{2^n}$ with $n = 6$ and c primitive

$$F(x) = x^3 + x^{10} + cx^{24}$$

obtain a nonquadratic APN permutation

$$c^{25}x^{57}+c^{30}x^{56}+c^{32}x^{50}+c^{37}x^{49}+c^{23}x^{48}+c^{39}x^{43}+c^{44}x^{42}+c^{4}x^{41}+c^{18}x^{40}+c^{46}x^{36}+c^{51}x^{35}+c^{52}x^{34}+c^{18}x^{33}+c^{56}x^{32}+c^{53}x^{29}+c^{30}x^{28}+cx^{25}+c^{58}x^{24}+c^{60}x^{22}+c^{37}x^{21}+c^{51}x^{20}+cx^{18}+c^{2}x^{17}+c^{4}x^{15}+c^{44}x^{14}+c^{32}x^{13}+c^{18}x^{12}+cx^{11}+c^{9}x^{10}+c^{17}x^{8}+c^{51}x^{7}+c^{17}x^{6}+c^{18}x^{5}+x^{4}+c^{16}x^{3}+c^{13}x$$

Problem Find APN permutations for $n \geq 8$ even.

The first APN and AB classes CCZ-ineq. to Monomials

Let s, k, p be positive integers such that $n = pk$, $p = 3, 4$, $\gcd(k, p) = \gcd(s, pk) = 1$ and α primitive in $\mathbb{F}_{2^n}^*$. Then

$$x^{2^s+1} + \alpha^{2^k-1} x^{2^{-k}+2^{k+s}}$$

is quadratic APN on $\mathbb{F}_{2^n}$ and, if n is odd then it is an AB permutation [B., Carlet, Felke, Leander 2006; B., Carlet, Leander 2008].

- This binomials solved an open problem from CCZ-paper on existence of quadratic AB functions inequivalent to Gold functions.
- These binomials and Gold maps are the the only known quadratic AB permutations.
- Among all 480 known quadratic AB functions with $n = 7$, only Gold maps are CCZ-equivalent to permutations [Yu 2018].

Known APN families CCZ-ineq. to power functions

N°	Functions	Conditions
C1-C2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk, \gcd(k,3)=\gcd(s,3k)=1, p\in\{3,4\}, i=sk \bmod p, m=p-i, n\geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$
C3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+cx^{2^iq+1}+c^qx^{2^i+q}$	$q=2^m, n=2m, gcd(i,m)=1,$ $c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q, X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$
C4	$x^3+a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a\neq 0$
C5	$x^3+a^{-1}\mathrm{Tr}_n^3(a^3x^9+a^6x^{18})$	$3\|n, a\neq 0$
C6	$x^3+a^{-1}\mathrm{Tr}_n^3(a^6x^{18}+a^{12}x^{36})$	$3\|n, a\neq 0$
C7-C9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k, \gcd(k,3)=\gcd(s,3k)=1, v,w\in\mathbb{F}_{2^k}, vw\neq 1, 3\|(k+s), u$ primitive in $\mathbb{F}_{2^n}^*$
C10	$(x+x^{2^m})^{2^k+1}+u'(ux+u^{2^m}x^{2^m})^{(2^k+1)2^i}+u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	$n=2m, m\geqslant 2$ even, $\gcd(k,m)=1$ and $i\geqslant 2$ even, u primitive in $\mathbb{F}_{2^n}^*, u'\in\mathbb{F}_{2^m}$ not a cube
C11	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$	$n=3m, m$ odd, $L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions in Lemma 8 of [7]

- All are quadratic.
- All have the same optimal nonlinearity and for *n* odd they are AB.
- In general, these families are pairwise CCZ-inequivalent.

Representatives of APN polynomial families $n \leq 12$

Dimension	Functions	Equivalent to
6	$x^{24} + ax^{17} + a^8x^{10} + ax^9 + x^3$	$C3$
	$ax^3 + x^{17} + a^4x^{24}$	$C7 - C9$
7	$x^3 + Tr_7(x^9)$	$C4$
8	$x^3 + x^{17} + p^{48}x^{18} + p^3x^{33} + px^{34} + x^{48}$	$C3$
	$x^3 + Tr_8(x^9)$	$C4$
	$x^3 + a^{-1}Tr_8(a^3x^9)$	$C4$
	$a(x + x^{16})(ax + a^{16}x^{16}) + a^{17}(ax + a^{16}x^{16})^{12}$	$C10$
9	$x^3 + Tr_9(x^9)$	$C4$
	$x^3 + Tr_9^3(x^9 + x^{18})$	$C5$
	$x^3 + Tr_9^3(x^{18} + x^{36})$	$C6$
	$x^3 + a^{246}x^{10} + a^{47}x^{17} + a^{181}x^{66} + a^{428}x^{129}$	$C11$
10	$x^6 + x^{33} + p^{31}x^{192}$	$C3$
	$x^3 + x^{72} + p^{31}x^{258}$	$C3$
	$x^3 + Tr_{10}(x^9)$	$C4$
	$x^3 + a^{-1}Tr_{10}(a^3x^9)$	$C4$
11	$x^3 + Tr_{11}(x^9)$	$C4$

Infinite families are identified for

- only 3 out of 13 quadratic APN functions of $\mathbb{F}_{2^6}$;
- only 4 out of more than 480 quadratic APN of $\mathbb{F}_{2^7}$;
- only 6 out of more than 8000 quadratic APN of $\mathbb{F}_{2^8}$.

APN Polynomial CCZ-Ineq. to Monomials and Quadratics

Only one known example of APN polynomial CCZ-inequivalent to quadratics and to power functions for n=6:

$$x^3 + c^{17}(x^{17} + x^{18} + x^{20} + x^{24})+$$

$$c^{14}\left(\mathrm{tr}_6(c^{52}x^3 + c^6x^5 + c^{19}x^7 + c^{28}x^{11} + c^2x^{13})+\right.$$

$$\left.\mathrm{tr}_3(c^{18}x^9) + x^{21} + x^{42}\right)$$

where c is some primitive element of $\mathbb{F}_{2^6}$ [Leander et al, Edel et al. 2008].

- No infinite families known.
- No AB examples known.

Classification of APN Functions

Leander et al 2008:

CCZ-classification finished for:

- APN functions with $n \leq 5$ (there are only power functions).

EA-classification is finished for:

- APN functions with $n \leq 5$ (there are only power functions and the ones constructed by CCZ-equivalence in 2005).

Commutative semifields

$\mathbb{S} = (S, +, \star)$ is a commutative semifield if all axioms of finite fields hold except associativity for multiplication.

- $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is planar (p odd) if

$$F(x + a) - F(x), \qquad \forall a \in \mathbb{F}_{p^n}^*,$$

  are permutations.
- There is one-to-one correspondence between quadratic planar functions and commutative semifields [Coulter, Henderson 2008].

The only previously known infinite classes of commutative semifields defined for all odd primes p were Dickson (1906) and Albert (1952) semifields.

Some of the classes of APN polynomials were used as patterns for constructions of new such classes of semifields
[B., Helleseth 2007; Zha et al 2009; Bierbrauer 2010].

Yet another equivalence?

- Isotopisms of commutative semifields induces isotopic equivalence of quadratic planar functions more general than CCZ-equivalence [B., Helleseth 2007].

- If quadratic planar functions F and F' are isotopic equivalent then F' is EA-equivalent to

$$F(x+L(x))-F(x)-F(L(x))$$

  for some linear permutation L [B., Calderini, Carlet, Coulter, Villa 2018].

- Isotopic equivalence for APN functions?

Isotopic construction

Isotopic construction of APN functions:

$$F(x + L(x)) - F(x) - F(L(x))$$

where linear L and F an APN function.

It is not equivalence but a powerful construction method:

- a new infinite family of quadratic APN functions;
- for $n = 6$, starting with any quadratic APN it is possible to construct all the other quadratic APNs.

Isotopic construction for planar functions?

Equivalence more general than CCZ-equivalence?

The indicator of the graph G_F of $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$:

$$1_{G_F}(x,y) = \begin{cases} 1 & \text{if} \quad y = F(x) \\ 0 & \text{otherwise} \end{cases} .$$

- F and F' are CCZ-equivalent iff $1_{G_{F'}} = 1_{G_F} \circ L$ for some affine permutation L.

- F and F' are CCZ-equivalent iff 1_{G_F} and $1_{G_{F'}}$ are CCZ-equivalent [B., Carlet 2010].

Currently CCZ-equivalence is the most general known equivalence relation preserving APN property.

Characterization of APN and AB functions

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_{2^n}$, define $\gamma_F : \mathbb{F}_{2^n}^2 \to \mathbb{F}_2$ as

$$\gamma_F(a,b) = \begin{cases} 1 & \text{if } a \neq 0 \text{ and } F(x+a) + F(x) = b \text{ has solutions,} \\ 0 & \text{otherwise.} \end{cases}$$

CCZ; B., Carlet, Helleseth 2011:

- F is APN iff γ_F has weight $2^{2n-1} - 2^{n-1}$.
- F is AB iff γ_F is bent.
- γ_F is determined for C1-C6 and all APN monomials except Dobbertin's.
- For nonquadratic AB cases found γ_F provide potentially new bent functions.
- If F and F' are CCZ-equivalent then $\gamma_{F'} = \gamma_F \circ \mathcal{L}$ for some affine permutation $\mathcal{L}$.
    - All affine invariants for γ_F are CCZ-invariants for F.

Bounds on algebraic degree of APN and AB functions

If F is AB over $\mathbb{F}_{2^n}$ then

$$d^\circ(F) \leq \frac{n+1}{2}$$

[CCZ].
The bound is reachable (for example, the inverses of Gold functions [Nyberg 1993]).

Bound on algebraic degree of APN?

- For n odd the inverse APN function has algebraic degree $n-1$.
- For n even Dobbertin function has algebraic degree $n/5+3$.
- Kasami functions have algebraic degree $i+1$ for $i \leq n/2-1$, $\gcd(n,i)=1$.

APN functions of algebraic degree n

B., Carlet, Helleseth, Li 2016:

Conjecture 1 There exists no APN function over $\mathbb{F}_{2^n}$ of algebraic degree n for $n \geq 3$.

- This conjecture is true for $n \in \{3, 4, 5\}$.
- $x^{2^n-1} + F(x)$ is not APN for most of the known APN functions F over $\mathbb{F}_{2^n}$.

It implies for most of the known APN functions the following conjecture is true.

Conjecture 2 If $n \geq 3$ and F' is a function over $\mathbb{F}_{2^n}$ obtained from an APN function F by changing its value in one point then F' is not APN.

Changing multiple points in APN functions

Changing two points [Kaleyski 2019]:

$$F'(x) = x^{2^n-1} + (x+1)^{2^n-1} + F(x)$$

If F is AB and $n \geq 5$ then F' is not AB.
For $n = 4$ minimum distance between APN functions is 2.

Problem What is minimum number of points two APN (resp. AB) functions can differ.

Distance between known APN functions tends to grow with n [B., Carlet, Helleseth, Kaleyski 2019]. $d(F,G) \geq 1+$

$$\left\lceil \frac{1}{3} \min_{b,\beta \in \mathbb{F}_{2^n}} |\{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n})(F(x) + F(a+x) + F(a+\beta) = b)\}| \right\rceil .$$

- For $n = 5$ a low bound for distance between *all* APN functions is 4 (tight or not is not known).
- For $n = 6$ a low bound for distance between *all known* APN functions is 6; for $n = 7$ is 19; for $n = 8$ is 24.