Optimal Cryptographic Functions

Lilya Budaghyan

Selmer Center
University of Bergen
Norway

Finse Winter School 2019
May 10, 2019

Boolean Functions

For n and m positive integers

Boolean functions: $F : \mathbb{F}_2^n \to \mathbb{F}_2$

Vectorial Boolean (n, m)-functions: $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

Initial motivation for introduction of Boolean functions:

- fundamental mathematics;
- mathematical logic.

Modern applications of Boolean functions:

- reliability theory, multicriteria analysis, mathematical biology, image processing, theoretical physics, statistics;
- voting games, artificial intelligence, management science, digital electronics, propositional logic;
- coding theory, combinatorics, sequence design, cryptography.

On the Number of Boolean Functions

BF_n is the set of Boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2$.

$$|BF_n| = 2^{2^n}$$

n	4	5	6	7	8
$\lvert BF_n \rvert$	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}
$\approx$	$6 \cdot 10^4$	$4 \cdot 10^9$	10^{19}	10^{38}	10^{77}

BF_n^n is the set of vectorial Boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

$$|BF_n^n| = 2^{n2^n}$$

n	4	5	6	7	8
$\lvert BF_n^n \rvert$	2^{64}	2^{160}	2^{384}	2^{896}	2^{2048}

Cryptographic properties of functions

S-boxes are vectorial Boolean functions used in block ciphers to provide confusion. They should possess certain properties to ensure resistance of the ciphers to cryptographic attacks.

Main cryptographic attacks on block ciphers and corresponding properties of S-boxes:

- Linear attack – Nonlinearity
- Differential attack – Differential uniformity
- Algebraic attack – Existence of low degree multivariate equations
- Higher order differential attack – Algebraic degree
- Interpolation attack – Univariate polynomial degree

Optimal Cryptographic Functions

Optimal Cryptographic functions

- are vectorial Boolean functions optimal for primary cryptographic criteria (APN, AB etc.);
- 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.

Outline

Binary expansion and representation of integers

Binary expansion of an integer k, $0 \leq k < 2^n$:

$$k = \sum_{s=0}^{n-1} 2^s k_s,$$

where k_s, $0 \leq k_s \leq 1$.
2-weight of k:

$$w_2(k) = \sum_{s=0}^{n-1} k_s.$$

$v_k = (k_{n-1}, ..., k_0)$ is the binary representation of k.

Truth Table representation of functions

For $F: \mathbb{F}_2^n \to \mathbb{F}_2^m$ the sequence $(F(v_0), ..., F(v_{2^n-1}))$ is called the truth table of F.

Example 1 Truth table of $F: \mathbb{F}_2^3 \to \mathbb{F}_2$: $(0,1,0,0,0,1,0,1)$.

x_1	x_2	x_3	$F(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

k	0	1	2	3	4	5	6	7
$F(v_k)$	0	1	0	0	0	1	0	1

ANF representation of functions

Algebraic normal form ANF of $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$:

$$F(x_1, ..., x_n) = \sum_{u \in \mathbb{F}_2^n} a_u \prod_{i=1}^{n} x_i^{u_i}, \quad a_u \in \mathbb{F}_2^m, \quad u = (u_1, ..., u_n).$$

The algebraic degree $d^\circ(F)$ of F is the degree of its ANF.
F is affine if $d^\circ(F) \leq 1$.
F is quadratic if $d^\circ(F) \leq 2$.

Example 1

$$F(x_1, x_2, x_3) = x_1x_2x_3 + x_2x_3 + x_3$$

$$d^\circ(F) = 3$$

Field definition

A field $(G, +, \cdot)$ is a set G with binary operations $+, \cdot$ s.t.

(1) $a + b = b + a$ and $a \cdot b = b \cdot a$ for $\forall a, b \in G$,

(2) $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for $\forall a, b, c \in G$,

(3) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for $\forall a, b \in G$,

(4) there exist elements of G, denoted 0 and 1, and called additive and multiplicative identities s.t. $a + 0 = a$ for $\forall a \in G$, and $a \cdot 1 = a$ for $\forall a \in G \setminus \{0\}$,

(5) for $\forall a \in G$ there exist elements of G, denoted $-a$ and, if $a \neq 0$, a^{-1}, called additive and multiplicative inverses, s.t. $a + (-a) = 0$ and $a \cdot a^{-1} = 1$.

Finite Fields Properties

- Any finite field $(G, +, \cdot)$ consists of p^n elements for some prime p, called the characteristic of the field, and some positive integer n.
  Then denote $\mathbb{F}_{p^n} = (G, +, \cdot)$ and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$.
- Any prime field $\mathbb{F}_p$ can be identified with the set $\{0, 1, .., p-1\}$ where addition and multiplication is taken modulo p.
- $\alpha \in \mathbb{F}_{p^n}^*$ is a primitive element of $\mathbb{F}_{p^n}^*$ if for any $a \in \mathbb{F}_{p^n}^*$ there is $0 \leq k \leq 2^n - 2$ s.t. $a = \alpha^k$.
- $(p-1)a = -a$, and for $p = 2$ then $a = -a$.

Univariate representation of functions

The univariate representation of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ 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.

Example 1

$$F(x) = x^7 + \alpha x^6 + \alpha^2 x^5 + \alpha^4 x^3$$

where α is a primitive element of $\mathbb{F}_{2^3}$.

Algebraic degree of univariate function

Algebraic degree in univariate representation of F

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

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

Special Functions

- F is linear if
$$F(x) = \sum_{i=0}^{n-1} b_i x^{2^i}.$$
- F is affine if it is a linear function plus a constant.
- F is quadratic if for some affine A
$$F(x) = \sum_{i,j=0, i \neq j}^{n-1} b_{ij} x^{2^i+2^j} + A(x).$$
- F is power function or monomial if $F(x) = x^d$.
- F is permutation if it is a one-to-one map.
- The inverse F^{-1} of a permutation F is s.t. $F^{-1}(F(x)) = F(F^{-1}(x)) = x$.

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.

Outline

Differential Uniformity and Derivatives of 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].
- The derivative of F in direction $a \in \mathbb{F}_{2^n}^*$ is $D_a F(x) = F(x+a) + F(x)$.
- $\delta_F(a, b)$ denotes the number of solutions of $F(x+a) + F(x) = b$.

Almost Perfect Nonlinear Functions

- 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.

Necessary and Sufficient Conditions for APN

- $|\{F(x+a)+F(x) : x \in \mathbb{F}_{2^n}\}| = 2^{n-1}$ for any $a \in \mathbb{F}_{2^n}^*$.
- D_aF is a two-to-one mapping for any $a \neq 0$.
- For every $(a,b) \neq 0$ the system

$$\begin{cases} x+y & = & a \\ F(x)+F(y) & = & b \end{cases}$$

  admits 0 or 2 solutions.

- The function $\gamma_F : \mathbb{F}_{2^n}^2 \to \mathbb{F}_2$ defined by

$$\gamma_F(a,b) = \begin{cases} 1 & \text{if } a \neq 0 \text{ and } \delta_F(a,b) \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

  has the weight $2^{2n-1} - 2^{n-1}$.

Quadratic and Power APN Functions

- $F(x) = x^d$ on $\mathbb{F}_{2^n}$, then F is APN iff D_1F is a two-to-one mapping. Indeed, for any $a \neq 0$

$$D_aF(x) = (x+a)^d + x^d = a^d D_1F(x/a).$$

- If F is quadratic then F is APN iff $F(x+a) + F(x) = F(a)$ has 2 solutions for any $a \neq 0$.

Outline

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].

Walsh Transform of an (n, m)-Function F

$$\lambda_F(u, v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_m(v\ F(x)) + tr_n(ax)}, \quad u \in \mathbb{F}_{2^n},\ v \in \mathbb{F}_{2^m}^*.$$

- Walsh coefficients of F are the values of its Walsh transform.
- Walsh spectrum of F is the multi-set of all Walsh coefficients of F.
- The extended Walsh spectrum of F is the multi-set of absolute values of all Walsh coefficients of F.

Walsh Transform and APN Functions

- For any (n, n)-function F

$$\sum_{a,b\in\mathbb{F}_{2^n}} \delta_F(a,b)^2 = \frac{1}{2^{2n}} \sum_{a,b\in\mathbb{F}_{2^n}} \lambda_F(a,b)^4$$

- F is APN iff

$$\sum_{u,v\in\mathbb{F}_{2^n},v\neq 0} \lambda_F^4(u,v) = 2^{3n+1}(2^n-1).$$

The Nonlinearity of F via Walsh Transform

$$N_F = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^m}^*} |\lambda_F(u, v)|$$

- Covering radius bound for an (n, m)-function F:

$$N_F \leq 2^{n-1} - 2^{n/2-1}.$$

- $N_F = 2^{n-1} - 2^{n/2-1}$ iff $\lambda_F(u, v) = \pm 2^{n/2}$ for any $u \in \mathbb{F}_{2^n}$, $v \in \mathbb{F}_{2^m}^*$. Then F is called bent.

- Bent (n, m)-functions exist iff n is even and $m \leq n/2$.

Almost Bent Functions

Sidelnicov-Chabaud-Vaudenay bound for $m \geq n-1$:

$$N_F \leq 2^{n-1} - \frac{1}{2}\sqrt{3 \cdot 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

It is tight iff $m = n$ and (n, n)-functions achieving this bound have $N_F = 2^{n-1} - 2^{\frac{n-1}{2}}$ and are called almost bent (AB).

- AB functions are optimal for linear cryptanalysis.
- F is AB iff $\lambda_F(u, v) \in \{0, \pm 2^{\frac{n+1}{2}}\}$.
- AB functions exist only for n odd.
- F is maximally nonlinear if $n = m$ is even and $N_F = 2^{n-1} - 2^{\frac{n}{2}}$ (conjectured optimal).

Almost Bent Functions II

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

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.

Necessary and Sufficient Conditions for AB

- For every $a, b \in \mathbb{F}_{2^n}$ the system of equations

$$\begin{cases} x + y + z & = & a \\ F(x) + F(y) + F(z) & = & b \end{cases}$$

has $3 \cdot 2^n - 2$ solutions if $b = F(a)$, and $2^n - 2$ otherwise.

- The function $\gamma_F : \mathbb{F}_{2^n}^2 \to \mathbb{F}_2$

$$\gamma_F(a, b) = \begin{cases} 1 & \text{if } a \neq 0 \text{ and } \delta_F(a, b) \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

is bent.

- F is APN and all its Walsh coefficients are divisible by $2^{\frac{n+1}{2}}$.

Almost Bent Power Functions

- In general, checking Walsh spectrum for power functions is sufficient for $a \in \mathbb{F}_2$ and $b \in \mathbb{F}_{2^n}^*$.
  - $F(x) = x^d$ is AB on $\mathbb{F}_{2^n}$ iff $\lambda_F(a, b) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ for $a \in \mathbb{F}_2$, $b \in \mathbb{F}_{2^n}^*$, since $\lambda_F(a, b) = \lambda_F(1, a^{-d}b)$ for $a \in \mathbb{F}_{2^n}^*$.
- In case of power permutation, sufficient for $b = 1$ and all a.
  - If $F = x^d$ is a permutation, F is AB iff $\lambda_F(a, 1) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ for $a \in \mathbb{F}_{2^n}$, since $\lambda_F(a, b) = \lambda_F(ab^{-\frac{1}{d}}, 1)$.

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.

Outline

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).

EAI-equivalence

If F and $F + A$ are permutation for some F and an affine A then $(F + A)^{-1}$ is not necessarily EA-equivalent to F or F^{-1}(2005).

Example: If $F(x) = x^{\frac{1}{2^i+1}}$, $A(x) = tr_{n/3}(x + x^{2^{2i}})$ over $\mathbb{F}_{2^n}$, then

$$(F + A)^{-1}(x) = x^{2^i+1} + (tr_{n/3}(x^{2^i+1}))^6 + (tr_{n/3}(x^{2^i+1}))^5 + (tr_{n/3}(x^{2^i+1}))^3$$

$$+ (tr_{n/3}(x^{2^i+1}))^4 + x^{2^i} tr_n(x) tr_{n/3}(x^{2^i+1} + x^{2^{2s}(2^i+1)})$$

$$+ x\ tr_n(x) tr_{n/3}(x^{2^i+1} + x^{2^s(2^i+1)}) + x^{2^i} tr_{n/3}(x^{2(2^i+1)} + x^{2^{2s+1}(2^i+1)})$$

$$+ x\ tr_{n/3}(x^{2(2^i+1)} + x^{2^{s+1}(2^i+1)}) + tr_n(x) tr_{n/3}(x^{2^i+1} + x^{4(2^i+1)})$$

with $s = i$ [mod 3], $\gcd(2i, n) = 1$ and $n \geq 9$

$d^\circ(F^{-1}) = 2$, $d^\circ(F) = \frac{n+1}{2}$, $d^\circ((F + A)^{-1}) = 4$.

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

Functions	Exponents d	Conditions on n odd
Gold (1968)	2^i+1	$\gcd(i,n)=1, 1\le i<n/2$
Kasami (1971)	$2^{2i}-2^i+1$	$\gcd(i,n)=1, 2\le i<n/2$
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.

Outline

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 $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ [Carlet, Charpin, Zinoviev 1998].

CCZ-equivalence

- preserves differential uniformity, nonlinearity, extended Walsh spectrum and resistance to algebraic attack.
- is more general than EAI-equivalence [2005].
- was used to disprove two conjectures of 1998:
  - 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].

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.

CCZ-Equivalence Formula

Let $\mathcal{L}$ be a affine permutation of $\mathbb{F}_{2^n}^2$ such that $\mathcal{L}(G_F) = G_{F'}$.

$\mathcal{L}(x, y) = (L_1(x, y), L_2(x, y))$ for some affine $L_1, L_2 : \mathbb{F}_{2^n}^2 \to \mathbb{F}_{2^n}$.

Then $\mathcal{L}(x, F(x)) = (F_1(x), F_2(x))$, where

$$F_1(x) = L_1(x, F(x)),$$

$$F_2(x) = L_2(x, F(x)),$$

and

$$\mathcal{L}(G_F) = \{(F_1(x), F_2(x)) : x \in \mathbb{F}_{2^n}\}.$$

$\mathcal{L}(G_F)$ is the graph of a function iff F_1 is a permutation.

Then, $F' = F_2 \circ F_1^{-1}$ and $\mathcal{L}(G_F) = G_{F'}$.

$$L_i(x, y) = A_{i1}(x) + A_{i2}(y)$$

for some affine $A_{ij} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $i, j \in \{0, 1\}$.

CCZ- and EAI-equivalences

- If $\mathcal{L}'(x, y) = \mathcal{L}(x, y) + (a, b)$ for a linear permutation $\mathcal{L}$ and $a, b \in \mathbb{F}_{2^n}$, and $\mathcal{L}(G_F) = G_{F'}$ then $\mathcal{L}'(G_F) = G_{F'(x+a)+b}$.
- If $\mathcal{L}(x, y) = (y, x)$ then $\mathcal{L}(x, F(x)) = (F(x), x)$ gives F^{-1}.
- If $\mathcal{L}(x, y) = (x, A(x) + y)$ then $\mathcal{L}(x, F(x)) = (x, F(x) + A(x))$ gives $F(x) + A(x)$.
- If $\mathcal{L}(x, y) = (x, A(y))$ then $\mathcal{L}(x, F(x)) = (x, A \circ F(x))$ gives $A \circ F(x)$.
- If $\mathcal{L}(x, y) = (A(x), y)$ then $\mathcal{L}(x, F(x)) = (A(x), F(x))$ gives $F \circ A^{-1}(x)$.

Construction of CCZ-eq. but EAI-ineq. F and F'

1. Find a *permutation* $L_1(x, F(x)) = A_1 \circ F(x) + A_2(x)$ where A_1, A_2 are linear.
   - L_1 depends on both variables is a necessary but not sufficient condition.
     - F' is EA-equivalent to F or to F^{-1} (if it exists) iff there exists a linear permutation $\mathcal{L} = (L_1, L_2)$ such that $\mathcal{L}(G_F) = G_{F'}$ and $L_1(x, y) = L(x)$ or $L_1(x, y) = L(y)$.
     - Example: Let $n = 2m + 1$ and $s \equiv m \pmod 2$. Then

$$\mathcal{L}(x, y) = (x + tr_n(x) + \sum_{j=0}^{m-s} y^{2^{2j+s}}, y + tr_n(x))$$

       is a linear permutation on $\mathbb{F}_{2^n}^2$ and $\mathcal{L}(G_F) = G_{F'}$ for $F(x) = x^3$ and F' which is EA-equivalent to F^{-1}.
   - If $A_1 \circ F(x) + A_2(x)$ is a permutation then for any L linear permutation, $L \circ A_1 \circ F(x) + L \circ A_2(x)$ does not produce new functions up to EA-equivalence.

Construction of CCZ-eq. but EAI-ineq. F and F' II

1. Find a *permutation* $L_1(x, F(x)) = A_1 \circ F(x) + A_2(x)$ where $A_1, A_2 \neq 0$ are linear (necessary but not sufficient).
2. Then find linear function $L_2(x, y) = A_3(y) + A_4(x)$ such that

$$\begin{aligned} A_1(y) + A_2(x) &= 0 \\ A_3(y) + A_4(x) &= 0 \end{aligned}$$

has only $(0, 0)$ solution.

- For found A_1 and A_2 there always exist suitable A_3 and A_4.
- For given A_1 and A_2 different pairs of A_3 and A_4 produce EA-equivalent functions.

- To construct a permutation F' both $L_1(x, F(x))$ and $L_2(x, F(x))$ must be permutations.

Outline

CCZ-eq. is more general than EAI-eq.

Example: APN maps $F(x) = x^{2^i+1}$, $\gcd(i, n) = 1$, over $\mathbb{F}_{2^n}$ and $F'(x) = x^{2^i+1} + (x^{2^i} + x + tr_n(1) + 1)tr_n(x^{2^i+1} + x\ tr_n(1))$ (with $d(F') = 3$) are CCZ-equivalent but EAI-inequivalent.

Take for n odd $\mathcal{L}(x, y) = (x + tr_n(x) + tr_n(y), y + tr_n(y) + tr_n(x))$ and for n even $\mathcal{L}(x, y) = (x + tr_n(y), y)$.

F' is EA-inequivalent to permutations. This disproved the conjecture from 1998 that every AB function is EA-equivalent to permutation.

- For an AB function F there does not always exist linear L such that $F + L$ is a permutation.

First Classes of APN Maps EAI-ineq. to Monomials

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

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

Relation Between Equivalences

- Two power functions are CCZ-equivalent iff they are cyclotomic equivalent.
- For Gold APN monomials and quadratic APN polynomials CCZ$>$EAI.
- CCZ$=$EAI for non-quadratic power APN with $n \leq 7$.
- CCZ$>$EAI for non-power non-quadratic APN functions.

Cases when CCZ-equivalence coincides with EA-equivalence:

- Boolean functions.
- All bent functions.
- Two quadratic APN functions.
- A quadratic APN function is CCZ-equivalent to a power function iff it is EA-equivalent to one of the Gold functions.

Cases when CCZ-equivalence differs from EA-equivalence:

- For functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \geq 2$.

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

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

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

Outline

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 $\mathbb{F}_{2^n}^*$.

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

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

This binomials disproved the conjecture from 1998 on nonexistence of quadratic AB functions inequivalent to Gold functions.

Brute force proof for CCZ-inequivalence

If expression for F and F' are not complicated:

$$\begin{aligned} F'(x) &= F_2 \circ F_1^{-1}(x) \\ F' \circ F_1(x) &= F_2(x) \\ F'(L_1(x, F(x))) &= L_2(x, F(x)) \\ F'(A_4(x) + A_3(F(x))) &+ A_2(x) + A_1(F(x)) = 0 \end{aligned}$$

for some affine A_1, A_2, A_3, A_4.
Then coefficients for every monomial in the last expression should be 0.

Extensions of a class of APN binomials

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

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

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

Add more quadratic terms [McGuire et al 2008-2011]:

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

where $b, d \in \mathbb{F}_{2^k}$, $bd \neq 1$.

From APN binomials to 2^t-uniform functions

Let $n = 3k$, $\gcd(3k, s) = t$, $\gcd(3, k) = 1$, k/t is odd, $3|(k+s)$ and α is primitive in $\mathbb{F}_{2^n}$. Then the derivatives of

$$F(x) = x^{2^s+1} + \alpha^{2^k-1} x^{2^{-k}+2^{k+s}}$$

are 2^t-to-1 and F is a permutation [Bracken et al. 2012].

Problems for APN binomials families

Problems for APN binomials family with $4|n$:

- Can it be extended to trinomials and quadrinomials?

Problems for APN trinomial and quadrinomial family with $3|n$:

- Relaxing some conditions can we derive to functions whose derivatives are 2^r-to-1 mappings (or permutations)?
- Possible adding of more tirms?

Not yet classified APN binomial

$$F_{bin}(x) = x^3 + wx^{36}$$

over $\mathbb{F}_{2^{10}}$, where w has the order 3 or 93 [Edel et al. 2005].

- Find a family to which F_{bin} belongs.

A class of APN hexanomials

Good candidates for being differentially 4-uniform [Dillon 2006]:

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

over $\mathbb{F}_{2^n}$ with $q = 2^m$ and $n = 2m$.

Budaghyan, Carlet 2008:

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

is APN on $\mathbb{F}_{2^n}$ when $\gcd(i, m) = 1$, $c, b \in \mathbb{F}_{2^n}$, $b \notin \mathbb{F}_q$ and $x^{2^i+1} + cx^{2^i} + c^q x + 1$ is irreducible over $\mathbb{F}_{2^n}$.

Elements c satisfying this condition always exist [Bluher 2012].

Bracken et al. 2014: $c = w\beta^{q+2^i} + \gamma^{q+2^i}$ where w has order 3 and $\gamma^{2^i+1} + w\beta^{2^i+1} + 1 = 0$ with $\gamma^{q-1} \neq \beta^{q-1}$.

A class of APN and AB functions $x^3 + \mathrm{tr}_n(x^9)$

Budaghyan, Carlet, Leander 2009:

$F(x) + \mathrm{tr}_n(G(x))$ is at most differentially 4-uniform for any APN function F and any function G.

- $x^3 + \mathrm{tr}_n(x^9)$ is APN over $\mathbb{F}_{2^n}$.
- It is the only APN polynomial CCZ-inequivalent to power functions which is defined for any n.
- It was the first APN polynomial CCZ-inequivalent to power functions with all coefficients in $\mathbb{F}_2$.

Two classes of APN functions for n divisible by 3

Budaghyan, Carlet, Leander 2009:

There are sufficient conditions on linear L_1, L_2 such that $L_1(x^3) + L_2(x^9)$ is APN.

- If n is even and $L_1(x) + L_2(x^3)$ is a permutation, then $L_1(x^3) + L_2(x^9)$ is APN.

$$\begin{aligned} F_1(x) &= x^3 + \alpha^{-1}\mathrm{tr}_n(\alpha^3 x^9), \\ F_2(x) &= x^3 + \alpha^{-1}\mathrm{tr}_n^3(\alpha^6 x^{18} + \alpha^{12} x^{36}), \\ F_3(x) &= x^3 + \alpha^{-1}\mathrm{tr}_n^3(\alpha^3 x^9 + \alpha^6 x^{18}) \end{aligned}$$

are APN over $\mathbb{F}_{2^n}$ when $\alpha \in \mathbb{F}_{2^n}^*$ and n is a positive integer for F_1 and n divisible by 3 for F_2 and F_3.

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	$x^3+a^{-1}\mathrm{Tr}_n^3(a^3x^9+a^6x^{18})$	$3\vert n, a\neq 0$
C6	$x^3+a^{-1}\mathrm{Tr}_n^3(a^6x^{18}+a^{12}x^{36})$	$3\vert n, a\neq 0$
C7-C9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k, \gcd(k,3)=\gcd(s,3k)=1, v,w\in\mathbb{F}_{2^k}, vw\neq 1, 3\vert(k+s), u$ 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 1000 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.

Further constructions of APN families?

Gologlu's family of quadratic APN trinomials on $\mathbb{F}_{2^n}$

$$G(x) = x^{2^k+1} + \left(\mathrm{tr}_n^m(x)\right)^{2^k+1},$$

with $\gcd(k, n) = 1$ and $n = 2m = 4t$ [2015].
It was claimed to CCZ-inequivalent to known APN families.

G is EA-equivalent to the Gold function $x^{2^{m-k}+1}$ [B., Carlet, Helleseth, Li, Sun 2017].

$$\begin{aligned} L_1(x) &= \gamma^{2^k} x^{2^{m+k}} + \gamma x^{2^k}, \\ L_2(x) &= \gamma x + \gamma^{2^k} x^{2^m}, \\ \left(L_1(x)\right)^{2^{m-k}+1} &= L_2 \circ G(x) \end{aligned}$$

where γ is a primitive element of $\mathbb{F}_{2^2}$.

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).

Outline

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.

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?

Crooked functions

F is crooked if $F(0) = 0$, for all distinct x, y, z and $\forall a \neq 0, b, c, d$
$F(x) + F(y) + F(z) + F(x + y + z) \neq 0$ and
$F(x) + F(y) + F(z) + F(x + a) + F(y + a) + F(z + a) \neq 0$.

- Every quadratic AB permutation with $F(0) = 0$ is crooked.
- Every crooked function is an AB permutation.
- Conjecture: Every crooked function is quadratic.
- Crookedness is preserved only by affine equivalence.

Known crooked functions over $\mathbb{F}_{2^n}$.

Functions	Exponents d	Conditions
Gold (1968)	x^{2^i+1}	n odd
AB binomials (2006)	$x^{2^s+1} + \alpha^{2^k-1} x^{2^{-k}+2^{k+s}}$	$n = 3k$ odd

Among all 480 known quadratic AB functions with $n = 7$, only Gold maps are CCZ-equivalent to permutations.

Outline

Exceptional APN functions

A function F is exceptional APN if it is APN over $\mathbb{F}_{2^n}$ for infinitely many values of n.

Gold and Kasami functions are the only known exceptional APN functions.

It is conjectured by Aubry, McGuire and Rodier (2010) that there are no more exceptional APN functions.

- Proven for power functions [Hernando, McGuire 2010].
- More partial results confirming this conjecture Jedlika, Hernando, Aubry, McGuire, Rodier, Caullery, Delgado and Janwa (2009-2016).

Nonliniarity properties of known APN families

All known APN families, except inverse and Dobbertin functions, have Gold-like Walsh spectra:

- for n odd they are AB;
- for n even Walsh spectra are $\{0, \pm 2^{n/2}, \pm 2^{n/2+1}\}$.

Sporadic examples of APN functions with non-Gold like Walsh spectra:

- For $n = 6$ only one example of quadratic APN function with $\{0, \pm 2^{n/2}, \pm 2^{n/2+1}, \pm 2^{n/2+2}\}$:

$$x^3 + a^{11}x^5 + a^{13}x^9 + x^{17} + a^{11}x^{33} + x^{48}.$$

- For $n = 8$ there are more quadratic APN functions.

Problems on Nonlinearity of APN functions

- Find a family of quadratic APN polynomials with non-Gold like nonliniarity.
- The only family of APN power functions with unknown Walsh spectrum is Dobbertin function:
  - All Walsh coefficients are divisible by $2^{\frac{2n}{5}}$ but not by $2^{\frac{2n}{5}+1}$ [Canteaut, Charpin, Dobbertin 2000].
  - Conjecture: $\max |\lambda_F(a,b)| = 2^{\frac{2n}{5}}(2^{\frac{n}{5}}+1)$ [Canteaut].
- What is a low bound for nonlinearity of APN functions?

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

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

Carlet, Charpin, Zinoviev 1998; B., Carlet, Helleseth 2011:

- F is APN if and only if γ_F has weight $2^{2n-1} - 2^{n-1}$.
- F is AB if and only if 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

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

[Carlet et al 1998].
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 $i \leq n/2-1$, $\gcd(n,i)=1$.
- BCP functions can have algebraic degree $m+2$ for $m|n$.

APN functions of algebraic degree n

Budaghyan, 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 two points in APN functions

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

If F is AB and $n \geq 5$ then F' is not AB.

F' is APN for $n = 4$ and $F(x) = x^3$ Gold APN. Then F and F' are CCZ-equivalent but EA-inequivalent.

Can this happen for $n \geq 5$?

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

B., Carlet, Helleseth, Kaleyski 2019:
The distance between known APN functions tends to grow with n.