Optimal Cryptographic Functions over Finite Fields

Lilya Budaghyan

Selemer Center
Department of Informatics
University of Bergen
NORWAY

Carleton Finite Fields eSeminar
June 10, 2020

Functions over finite fields

For p a prime, n and m positive integers

(n, m, p)-functions: $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$

Boolean functions: $F : \mathbb{F}_{2^n} \to \mathbb{F}_2$

Vectorial Boolean (n, m)-functions: $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Modern applications of functions over finite fields, especially, Boolean functions:

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

Cryptographic properties of functions

Functions used in block ciphers (S-boxes) 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 (n, m, p)-functions (in particular, vectorial Boolean functions) optimal for primary cryptographic criteria (APN, AB, PN, planar 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 (13 AB, 19 APN);
- are "HARD-TO-PREDICT" - most conjectures are proven to be false.

Outline

Univariate representation of functions

The univariate representation of $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ for $m|n$:

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

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

Example

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

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

Algebraic degree of univariate function

For p a prime and n a positive integer, p-ary expansion of an integer k, $0 \leq k < p^n$ is

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

where k_s, $0 \leq k_s < p$. Then p-weight of k:

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

Algebraic degree of F

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

$$d^\circ(F) = \max_{0 \leq i < p^n, c_i \neq 0} w_p(i).$$

Special Functions

- F is linear if
$$F(x) = \sum_{i=0}^{n-1} b_i x^{p^i}.$$
- F is affine if it is a linear function plus a constant.
- F is quadratic if for some affine A
$$F(x) = \sum_{i,j=0}^{n-1} b_{ij} x^{p^i+p^j} + A(x).$$
- 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 functions

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

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

Absolute trace function:

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

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

$$tr_m(vF(x))$$

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.
- $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is differentially δ-uniform if

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

  has at most δ solutions.
- Differential uniformity measures the resistance to differential attack [Nyberg 1993].

PN, APN and Planar Functions

- $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is perfect nonlinear (PN) if $\delta = p^{n-m}$.
- If $n = m$ then PN functions have $\delta = 1$ and are called planar.
- Planar functions exist only for $p > 2$.
- $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if $\delta = 2$.
- Planar, PN and APN functions are optimal for differential cryptanalysis.

Examples of planar functions:

- x^2 on $\mathbb{F}_{p^n}$ with $p > 2$, n any positive integer;
- x^{p^i+1} on $\mathbb{F}_{p^n}$ with $p > 2$, $n/\gcd(i, n)$ odd.

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.

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

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

- Walsh coefficients of F are the values of its Walsh transform.
- Walsh spectrum of F is the set of all Walsh coefficients of F.
- The extended Walsh spectrum of F is the set of absolute values of all Walsh coefficients of F.
- 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.
- An (n,m)-function is bent iff it is PN.
- Bent (n,m)-functions exist iff n is even and $m \leq n/2$.

Almost Bent Functions

For (n, n)-functions $N_F \leq 2^{n-1} - 2^{\frac{n-1}{2}}$ and functions achieving this bound 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.

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 $\mathbb{F}_{p^n}$ are cyclotomic equivalent if $d' = p^i \cdot d \mod (p^n - 1)$ for some $0 \leq i < n$
or, $d' = p^i/d \mod (p^n - 1)$ in case $\gcd(d, p^n - 1) = 1$.

Invariants and Relation Between Equivalences

- Linear equivalence $\subset$ affine equivalence $\subset$ EA-equivalence $\subset$ EAI-equivalence.
- Cyclotomic equivalence $\subset$ EAI-equivalence.
- APNness, ABness, bentness, planarity 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.

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 $n = 8$.

Outline

CCZ-Equivalence

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

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

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

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, planar and PN 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.

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
$\mathcal{L}(x, y) = (L_1(x), L_2(x)) = (x + tr_n(x) + tr_n(y), y + tr_n(y) + tr_n(x))$
and for n even $\mathcal{L}(x, y) = (L_1, L_2)(x, y) = (x + tr_n(y), y)$.

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

Among more than 480 known AB functions over $\mathbb{F}_{2^7}$ only 6 of them, that are power functions, are CCZ-equivalent to permutations.

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 $m \mid n$ $\gcd(i, n) = 1$

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.

CCZ-construction of APN permutation for n even

- No quadratic APN permutations for n even [Nyberg 1993].

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

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

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 $\mathbb{F}_{2^n}$. If n is odd then this function 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.

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

Another APN quadrinomial family

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

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

Let $n = 2m$ with m odd and $3 \nmid m$, β primitive in $\mathbb{F}_{2^2}$, $(a, b, c) = (\beta, \beta^2, 1)$ and $i = m - 2$ or $i = (m-2)^{-1} \mod n$. Then

$$x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$$

is APN on $\mathbb{F}_{2^n}$. F_{bin} is a particular case of this quadrinomial with $n = 10$, $a = \beta$, $b = c = 0$, $i = 3$, $k = 2$ [B., Helleseth, Kaleyski 2020].

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

B., 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 $\mathbb{F}_2$.

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	$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)} + cx^{2^i q+1} + c^q x^{2^i+q}$	$q = 2^m, n = 2m, gcd(i,m) = 1, c \in \mathbb{F}_{2^n}, s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^q X + 1$ 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	$L(x)^{2^i}x + L(x)x^{2^i}$	
C12	$ut(x)(x^q + x) + t(x)^{2^{2i}+2^{3i}} + at(x)^{2^{2i}}(x^q + x)^{2^i} + b(x^q + x)^{2^i+1}$	$n = 2m, q = 2^m, \gcd(m,i) = 1, t(x) = u^q x + x^q u$, $X^{2^i+1} + aX + b$ has no solution over $\mathbb{F}_{2^m}$
C13	$x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$	$n = 2m = 10, (a,b,c) = (\beta,1,0,0), i = 3, k = 2, \beta$ primitive in $\mathbb{F}_{2^2}$
		$n = 2m, m$ odd, $3 \nmid m, (a,b,c) = (\beta,\beta^2,1), \beta$ primitive in $\mathbb{F}_{2^2}$, $i \in \{m-2, m, 2m-1, (m-2)^{-1} \mod n\}$

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

Only one known example of APN polynomial CCZ-inequivalent to quadratics and to power functions for n=6 [Leander et al, Edel et al. 2008].

Representatives of APN polynomial families $n \leq 11$

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	$x^3+x^{17}+a^{48}x^{18}+a^3x^{33}+ax^{34}+x^{48}$	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
	$x^9+Tr_8(x^3)$	C11
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	$x^6+x^{33}+a^{31}x^{192}$	C3
	$x^{33}+x^{72}+a^{31}x^{258}$	C3
	$x^3+Tr_{10}(x^9)$	C4
	$x^3+a^{-1}Tr_{10}(a^3x^9)$	C4
	$x^3+a^{341}x^9+a^{682}x^{96}+x^{288}$	C13
	$x^3+a^{341}x^{129}+a^{682}x^{96}+x^{36}$	C13
	$x^3+a^{128}x^6+a^{384}x^{12}+a^{133}x^{33}+x^{34}+a^2x^{64}+x^{65}+a^{128}x^{68}+x^{96}+a^4x^{130}+a^{260}x^{136}+a^4x^{192}+a^{136}x^{260}+a^{12}x^{384}$	C12
	$x^3+a^{920}x^6+a^{153}x^{12}+a^{925}x^{33}+x^{34}+a^{794}x^{64}+x^{65}+a^{920}x^{68}+x^{96}+a^{796}x^{130}+a^{29}x^{136}+a^{796}x^{192}+a^{928}x^{260}+a^{804}x^{384}$	C12
	$x^3+a^{788}x^6+a^{21}x^{12}+a^{793}x^{33}+x^{34}+a^{662}x^{64}+x^{65}+a^{788}x^{68}+x^{96}+a^{664}x^{130}+a^{920}x^{136}+a^{664}x^{192}+a^{796}x^{260}+a^{672}x^{384}$	C12
	$x^5+a^{576}x^{18}+a^{512}x^{20}+a^{133}x^{33}+x^{36}+a^2x^{64}+a^{514}x^{80}+x^{129}+a^{512}x^{144}+x^{160}+a^{80}x^{514}+a^{16}x^{516}+a^{18}x^{576}+a^{16}x^{640}$	C12
	$x^5+a^{477}x^{18}+a^{413}x^{20}+a^{34}x^{33}+x^{36}+a^{926}x^{64}+a^{415}x^{80}+x^{129}+a^{413}x^{144}+x^{160}+a^{1004}x^{514}+a^{940}x^{516}+a^{942}x^{576}+a^{940}x^{640}$	C12
	$x^5+a^{81}x^{18}+a^{17}x^{20}+a^{661}x^{33}+x^{36}+a^{530}x^{64}+a^{19}x^{80}+x^{129}+a^{17}x^{144}+x^{160}+a^{608}x^{514}+a^{544}x^{516}+a^{546}x^{576}+a^{544}x^{640}$	C12
11	$x^3+Tr_{11}(x^9)$	C4

Infinite families are identified for

- only 3 out of 11 quadratic APN functions of $\mathbb{F}_{2^6}$;
- only 4 out of more than 480 quadratic APN of $\mathbb{F}_{2^7}$;
- only 7 out of more than 8180 quadratic APN of $\mathbb{F}_{2^8}$.

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).

There are some partial results for

- EA-classification of APN functions for $n \geq 6$ by Calderini 2019,
- CCZ-equivalence of quadratic APN for $n = 7, 8$ by Yu et al. 2013,
- quadratic APN functions with coefficients in $\mathbb{F}_2$ for $n \leq 9$ by B., Kaleyski, Yu 2020.

Outline

Application to commutative semifields

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

- $\mathbb{S} = (S, +, \star)$ is considered as $\mathbb{S} = (\mathbb{F}_{p^n}, +, \star)$.
- There is one-to-one correspondence between quadratic planar functions and commutative semifields [Coulter et al. 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 L is linear and F is APN.

It is not equivalence but a powerful construction method for APN functions:

- 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?

Application of APN constructions - 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 499 out of 8180 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].
  - Walsh spectrum is conjectured by B., Calderini, Carlet, Davidova, Kaleyski 2020.
- What is a low bound for nonlinearity of APN functions?