In search of equivalence relations for cryptographic Boolean functions

Lilya Budaghyan

Selemer Center in Secure Communication
University of Bergen
NORWAY

Africacrypt 2022
Fes, Morocco
July 18, 2022

Outline

Vectorial Boolean functions

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

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;
- algebra, projective geometry, 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

Functions used in block ciphers, S-boxes, should possess certain properties to ensure resistance of the ciphers to cryptographic attacks.

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

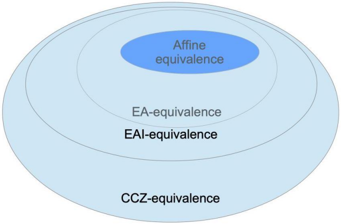
Optimal cryptographic functions

- are vectorial Boolean functions optimal for primary cryptographic criteria;
- 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;
- are "HARD-TO-PREDICT" - most conjectures are proven to be false.

Equivalence relations for cryptographic functions

Equivalence relations preserving main cryptographic properties

- affine equivalence - $A \circ F \circ A'$ with A and A' affine permutations;
- extended affine (EA-) equivalence $A \circ F \circ A' + A$ with A affine;
- EAI-equivalence - combination of EA-equivalence with inverses of permutations;
- CCZ-equivalence.



Importance of Equivalence Relations for Functions

Equivalence relations preserving main cryptographic properties divide the set of all functions into classes.

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

Outline

Univariate representation of functions

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

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

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

Algebraic degree of univariate function

For n a positive integer, binary expansion of an integer k, $0 \leq k < 2^n$ is

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

where k_s, $0 \leq k_s \leq 1$. Then binary weight of k:

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

Algebraic degree of F

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

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

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
$$F(x) = \sum_{i,j=0}^{n-1} b_{ij} x^{2^i+2^j} + A(x).$$
- 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 $m|n$:

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

Absolute trace function:

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

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

$$\mathrm{tr}_n(vF(x))$$

is a component function of F.

Outline

Differential uniformity and APN functions

- Differential cryptanalysis of block ciphers was introduced by Biham and Shamir in 1991.
- $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ 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^{-1} on $\mathbb{F}_{2^n}$ with n odd.

Quadratic and Power APN Functions

- $F(x) = x^d$ on $\mathbb{F}_{2^n}$, then F is APN iff for any $b \in \mathbb{F}_{2^n}$

$$(x+1)^d + x^d = b$$

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

Walsh transform of an (n, n)-function F

Walsh coefficients of F:

$$\lambda_F(u, v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_n(v\ F(x)) + \mathrm{tr}_n(ax)}, \quad u \in \mathbb{F}_{2^n},\ v \in \mathbb{F}_{2^n}^*$$

- 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

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

Nonlinearity of functions

- Linear cryptanalysis was discovered by Matsui in 1993.
- Nonlinearity measures the resistance to linear attack [Chabaud and Vaudenay 1994].

The nonlinearity of F:

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

Functions achieving this bound are called almost bent (AB).

- AB functions are optimal for linear cryptanalysis.
- F is maximally nonlinear if n is even and $N_F = 2^{n-1} - 2^{\frac{n}{2}}$ (conjectured optimal).

Almost bent functions

- F is AB iff $\lambda_F(u, v) \in \{0, \pm 2^{\frac{n+1}{2}}\}$.
- AB functions exist only for n odd.
- 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 $\frac{n+1}{2}$ [Carlet, Charpin, Zinoviev 1998].

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.

Almost bent power functions

- 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 $a \in \mathbb{F}_2$, $b \in \mathbb{F}_{2^n}^*$.
- 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 $a \in \mathbb{F}_{2^n}$.

Outline

Cyclotomic, affine, EA- and EAI- equivalences

- F and F' are affine equivalent if
$$F' = A_1 \circ F \circ A_2$$
for some affine permutations A_1 and A_2.

- F and F'' are *extended affine equivalent* (EA-equivalent) if
$$F'' = F' + A$$
where F' is affine equivalent to F and A is affine.

- 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 $d' = 2^i \cdot d \mod (2^n - 1)$ for some $0 \leq i < n$ or, $d' = 2^i / d \mod (2^n - 1)$ in case $\gcd(d, 2^n - 1) = 1$.

Invariants and relation between equivalences

- EA-equivalence and cyclotomic equivalence are particular cases of EAI-equivalence.
- APNness and ABness are preserved by EAI-equivalence.
- Algebraic degree is preserved by EA-equivalence but not by EAI-equivalence.
- Univariate degree is not preserved by any of the equivalences.
- 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	$2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$	$n = 5m$

- Power APN functions are permutations for n odd and 3-to-1 for n even [Dobbertin 1999].
- 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.

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 [B., Carlet, Pott 2005].
- was used to disprove two conjectures of 1998:
  - On nonexistence of AB functions EA-inequivalent to any permutation [disproved by B., Carlet, Pott 2005];
  - On nonexistence of APN permutations for n even [disproved for $n = 6$ by Dillon et al. 2009].

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

Outline

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 $A_1, A_2 \neq 0$ are linear (necessary but not sufficient).
   - 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 $L_1(x, y) = L(y)$.
2. Then 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, always exist.

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

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

Example: APN maps $F(x) = x^{2^i+1}$, $\gcd(i, n) = 1$, over $\mathbb{F}_{2^n}$ and $F'(x) = x^{2^i+1} + \left(x^{2^i} + x + \mathrm{tr}_n(1) + 1\right)\mathrm{tr}_n\left(x^{2^i+1} + x\,\mathrm{tr}_n(1)\right)$ are CCZ-equivalent but EAI-inequivalent.

Take for n odd $\mathcal{L}(x, y) = (L_1(x), L_2(x)) = \left(x+\mathrm{tr}_n(x)+\mathrm{tr}_n(y), y+\mathrm{tr}_n(y)+\mathrm{tr}_n(x)\right)$ and for n even $\mathcal{L}(x, y) = (L_1, L_2)(x, y) = (x + \mathrm{tr}_n(y), y)$.

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

First classes of APN and AB maps EAI-inequivalent to monomials

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

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

CCZ- and EA-classification of all functions for $n \leq 4$

Brinkmann 2019: For $n \leq 3$ for all functions over $\mathbb{F}_{2^n}$ CCZ-class=EA-class.

- $n = 1$ - $4 = 2^2$ functions: 1 CCZ-class;
  - it is affine functions, the class contains bijection;
- $n = 2$ - $256 = 2^8$ functions: 2 CCZ-classes;
  - one is affine, contains bijection;
  - another is quadratic, has no bijections.
- $n = 3$ - $16777216 = 2^{24}$ functions: 7 CCZ-classes;
  - one affine, contains bijection;
  - 3 of them are quadratic, contain bijections;
  - 3 of them are cubic, have no bijections.
- $n = 4$ - $18446744073709551616 = 2^{64}$ functions: 4713 EA-classes;
  - 194 contain bijections;
  - for 4151 CCZ-class=EA-class;
  - some CCZ-classes can contain several EA-classes containing permutations.

Outline

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 family

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

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	$x^3 + a^{-1}\mathrm{Tr}_n(a^3 x^9)$	$a \neq 0$
C5	$x^3 + a^{-1}\mathrm{Tr}_n^3(a^3 x^9 + a^6 x^{18})$	$3 \mid n$, $a \neq 0$
C6	$x^3 + a^{-1}\mathrm{Tr}_n^3(a^6 x^{18} + a^{12} x^{36})$	$3 \mid n, a \neq 0$
C7-C9	$ux^{2^s+1} + u^{2^k} x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1} + wu^{2^k+1} x^{2^s+2^{k+s}}$	$n = 3k, \gcd(k,3) = \gcd(s,3k) = 1, v, w \in \mathbb{F}_{2^k}$, $vw \neq 1, 3 \mid (k+s), u$ 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. For *n* odd they are AB otherwise have optimal nonlinearity.
- In general, these families are pairwise CCZ-inequivalent [B., Calderini, Villa, 2020].

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 13 quadratic APN functions of $\mathbb{F}_{2^6}$;
- only 4 out of 488 quadratic APN of $\mathbb{F}_{2^7}$;
- only 7 out of more than 21 000 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:

$$x^3 + c^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + \\ c^{14}\left(\mathrm{tr}_6(c^{52}x^3 + c^6x^5 + c^{19}x^7 + c^{28}x^{11} + c^2x^{13}) + \\ \mathrm{tr}_3(c^{18}x^9) + x^{21} + x^{42}\right)$$

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

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

Outline

CCZ- and EA- classification of APN functions

Brinkmann, Leander 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

- CCZ-equivalence of quadratic APN for $n = 7, 8$ by Yu et al. 2013, Leander et al 2021, etc.;
- EA-classification of APN functions for $n \geq 6$ by Calderini 2019;
- quadratic APN functions with coefficients in $\mathbb{F}_2$ for $n \leq 9$ by B., Kaleyski, Li, Yu 2020.

Relation between equivalences for APN monomials

- Two power functions are CCZ-equivalent iff they are cyclotomic equivalent [Dempwolff 2018, Yoshiara, 2018].
- For non-quadratic power APN with $n \leq 9$ CCZ- and EAI-equivalences coincide.
  Conjectured the same for all n [B., Calderini, Villa, 2020].

Gold function x^{2^i+1}

- CCZ-class$\neq$EAI-class.

Inverse function x^{-1} [Kolsch 2021]:

- CCZ-class$=$EA-class;
- has one affine class of permutations.

Relation between equivalences for quadratic APN

- Two quadratic APN functions are CCZ-equivalent iff they are EA-equivalent [Yoshiara 2017].
- For quadratic APN functions CCZ-equivalence is more general than EAI-equivalence [B., Carlet, Leander 2009].
- For $n = 6$, the 13 quadratic APN maps have from 3 to 91 EA-classes (algebraic degree from 2 to 4) [Calderini, 2020];

Relation between equivalences for non-quadratic APN

- For non-power non-quadratic APN functions CCZ-equivalence is more general than EAI-equivalence [B., Calderini, Villa, 2020].

- For the only known APN function ($n = 6$) CCZ-inequivalent to both quadratics and to monomials, the CCZ-class contains 25 EA-equivalence classes and does not contain permutations [Calderini 2020].

Outline

Application to crooked functions

- Every quadratic AB permutation with $F(0) = 0$ is crooked.
- 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 488 quadratic AB functions with $n = 7$, only Gold maps are CCZ-equivalent to permutations.
- For $n = 9$ two new crooked functions have been found by Beierle and Leander in 2022.

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 $n = 6$

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

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

obtain a nonquadratic APN permutation

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

Used in 2013 by Bogdanov et al. in design of Fides lightweight authenticated cipher.

CCZ-construction of infinite family of APN permutation for n even?

- The quadratic APN function $P(x) = x^3 + x^{10} + cx^{24}$ admits a "butterfly" structure leading to differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ with n even but not divisible by 4 [Perrin, Udovenko, Beryukov 2016].
- P is a part of a family of quadratic APN trinomials with n divisible by 3.
  - CCZ-equivalence application for construction of permutations still to be studied.
- CCZ-equivalence class of P consists of 13 EA-equivalence classes [Calderini 2020].
  - two of EA-equivalence classes contain permutations;
  - 4 affine equivalence classes contain permutations which can be represented as P_1, P_1^{-1}, P_2, P_3.

Outline

Equivalence of indicator of the graphs of functions

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.

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 $\mathbb{S} = (\mathbb{F}_{p^n}, +, \star)$.
- $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ 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, etc.]

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 [B., Calderini, Carlet, Coulter, Villa 2021].

Outline

Conclusion

- Optimal cryptographic functions - AB and APN functions
  - their infinite classes and special cases.
- Different equivalence relations preserving APNness and ABness;
  - relation between these equivalences;
  - application for construction of different types of APN and AB functions, in particular, permutations;
  - classification results with respect to these equivalences.
- Potential possibilities for a new equivalence.

Outline

Open problems

- New equivalence relations preserving differential and linear properties.
  - "isotopic" equivalence?
- Construction of an infinite family of APN permutations for n even
  - applying CCZ-equivalence to known quadratic APN family.
- Application of CCZ-equivalence in cryptanalysis.
- Classification of APN functions:
  - new families of power functions;
  - new families of APN and AB polynomials CCZ-inequivalent to quadratics;
  - classification over specific fields $\mathbb{F}_{2^n}$ with $n \geq 6$.