On Isotopic Construction of APN Functions

Irene Villa

joint work with

Lilya Budaghyan, Marco Calderini, Claude Carlet and Robert Coulter

BFA 2018

For p a prime and n a positive integer $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ has a unique representation as

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

- linear if $F(x) = \sum_{i=0}^{n-1} c_i x^{p^i}$,
- affine if $F(x) = \sum_{i=0}^{n-1} c_i x^{p^i} + c$,
- DO polynomial if $F(x) = \sum_{i,j=0}^{n-1} c_{ij} x^{p^i+p^j}$;
- quadratic if F is the sum of a DO polynomial and an affine function.

$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is differential δ-uniform if for any $a, b \in \mathbb{F}_{p^n}$ $a \neq 0$ the equation $F(x + a) - F(x) = b$ admits at most δ solutions

Differential uniformity measures the resistance of a function, used as an S-box inside a cryptosystem, to the differential attack. To small values of δ correspond a better resistance to the attack.

- If $\delta = 1$, then F called perfect nonlinear (PN) or planar exists only for $p \neq 2$.
- If $\delta = 2$, then F called almost perfect nonlinear (APN) has best resistance in the case $p = 2$.

Differential uniformity is invariant under some equivalence relations:

$F, F' : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are affine equivalent if $F' = A_1 \circ F \circ A_2$ with A_1, A_2 affine permutations.

$F, F' : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are EA-equivalent if $F' = A_1 \circ F \circ A_2 + A$ with A_1, A_2 affine permutations and A affine map.

$F, F' : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are CCZ-equivalent if there exists an affine permutation $\mathcal{L}$ such that $\mathcal{L}(\Gamma_F) = \Gamma_{F'}$.

$\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}$ is the graph of F

Finite presemifield $\mathcal{S} = (\mathbb{F}_{p^n}, +, \star)$

- ring with left and right distributivity and no zero divisor (not necessarily associative);
- it is isotopic equivalent to $\mathcal{S}' = (\mathbb{F}_{p^n}, +, \circ)$ if for any $x, y \in \mathbb{F}_{p^n}$ $T(x \circ y) = M(x) \star N(y)$, with T, M, N linear permutations;
- if $N = M$ then $\mathcal{S}$ and $\mathcal{S}'$ are strongly isotopic;
- every commutative presemifields of odd order define a planar DO polynomial and vice versa;
- two quadratic planar functions are isotopic if their corresponding presemifields are isotopic;
- F and F' are CCZ-equivalent if and only if $\mathcal{S}_F$ and $\mathcal{S}_{F'}$ are strongly isotopic.

Theorem 1

Quadratic planar functions F and F' are isotopic equivalent if and only if F' is affine equivalent to

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

for some linear permutation L.

Idea: transpose isotopic equivalence to the case of characteristic 2, applying the construction to known APN functions.

Isotopic shifts of Gold functions over $\mathbb{F}_{2^n}$

Gold function $F_i(x) = x^{2^i+1}$ (i and n coprime)
Isotopic shift $F_i'(x) = x^{2^i} L(x) + xL(x)^{2^i}$, for $L(x)$ linear function

Proposition 2

Let $L(x) = \sum_{j=0}^{n-1} b_j x^{2^j}$, then an equivalent function F'' can be constructed with linear map

$$\sum_{j=0}^{n-1} (b_j \alpha^{k(2^j-1)})^{2^t} x^{2^j}$$

for any k, t integers where α primitive element of $\mathbb{F}_{2^n}^{\star}$.

Isotopic shifts of Gold functions over $\mathbb{F}_{2^n}$

L with 1 term

Lemma 3

- For $L(x) = ux$, $u \neq 0, 1$, F'_i linearly equivalent to F_i.
- For $L(x) = ux^{2^i}$, n odd and $u \neq 0$, F'_i lin. eq. to F_{2i} and CCZ-ineq. to F_i.
- For $L(x) = ux^{2^j}$, $n = 2j$ and $ux^{2^i} + u^{2^i} x^{2^{j+i}}$ permutation, F'_i lin. eq. to $F_{|j-i|}$.

L with 2 terms

Lemma 4

For m even and $n = 2m$ let $L(x) = ux^{2^m} + vx$ with $u = w^{2^m-1}$ and $v^{2^i} + v = 1$ for $v, w \in \mathbb{F}^{\star}_{2^n}$. Then F'_i is EA-equivalent to F_{m-i}.

Isotopic shifts of Gold functions over $\mathbb{F}_{2^n}$

L with 3 terms and $F(x) = F_1(x) = x^3$

Lemma 5

For $n = 3m$ and $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$ if F' is APN then $L(x)$ and $L(x) + x$ are permutations.

Lemma 6

For m an odd number, let $n = 3m$ and U the multiplicative subgroup of $\mathbb{F}_{2^n}^{\star}$ of order $2^{2m} + 2^m + 1$. Then with $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$ the function F' is APN if and only if

- $L(v) \neq 0, v$ for any $v \in U$;
- $\frac{t^2L(v)+vL(t)^2}{v^2L(t)+tL(v)^2} \notin \mathbb{F}_{2^m}$ for any $t, v \in U$ such that $v^2L(t) + tL(v)^2 \neq 0$.

Computational results

Using the software MAGMA we obtained the following

Computational results

Using the software MAGMA we obtained the following

- L with 1 term from $n = 6$ to $n = 12$ all APN maps found are described in the Lemma 3;

Computational results

Using the software MAGMA we obtained the following

- L with 1 term from $n = 6$ to $n = 12$ all APN maps found are described in the Lemma 3;
- L with 2 terms and $F = x^3$ from $n = 7$ to $n = 11$ all APN maps found are for $n = 2m$ and $L(x) = ux^{2^m} + vx$ (more cases possible for $n = 6$)
  - if $4|n$ then F' is eq. to x^3 or $x^{2^{m-1}+1}$,
  - otherwise F' is eq. to x^3;

Computational results

Using the software MAGMA we obtained the following

- L with 1 term from $n = 6$ to $n = 12$ all APN maps found are described in the Lemma 3;
- L with 2 terms and $F = x^3$ from $n = 7$ to $n = 11$ all APN maps found are for $n = 2m$ and $L(x) = ux^{2^m} + vx$ (more cases possible for $n = 6$)
  - if $4|n$ then F' is eq. to x^3 or $x^{2^{m-1}+1}$,
  - otherwise F' is eq. to x^3;
- L with 3 terms and $F(x) = x^3$
  - $n = 6$ APN maps for $L(x) = ax^{2^4} + bx^{2^2} + cx$ eq. to x^3 or to $x^3 + \alpha^{-1} Tr(\alpha^3 x^9)$ (classified);
  - $n = 7$ no proper trinomial found;
  - $n = 8$ APN maps for $L(x) = ax^{2^6} + bx^{2^4} + cx^{2^2}$ eq. to $x^3 + Tr(x^9)$ (classified);
  - $n = 9$ APN maps for $L(x) = ax^{2^6} + bx^{2^3} + cx$ not equivalent to any classified function.

On isotopic shifts of x^3 with $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$

For $n = 3m$ necessary and sufficient condition for APN given in Lemma 6.

- $n = 6$ F' APN is eq. to x^3 or to $x^3 + \alpha^{-1} Tr(\alpha^3 x^9)$.
- $n = 9$, up to equivalence in Proposition 2, only APN case for $L(x) = \alpha^{424} x^{2^6} + \alpha x^{2^3} + \alpha^{118} x$ obtaining

$$F'(x) = \alpha^{337} x^{129} + \alpha^{424} x^{66} + \alpha^2 x^{17} + \alpha x^{10} + \alpha^{34} x^3.$$

- $n = 12$ F' APN is eq. to x^3.

On isotopic shifts of x^3 with $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$

For $n = 3m$ necessary and sufficient condition for APN given in Lemma 6.

- $n = 6$ F' APN is eq. to x^3 or to $x^3 + \alpha^{-1} Tr(\alpha^3 x^9)$.
- $n = 9$, up to equivalence in Proposition 2, only APN case for $L(x) = \alpha^{424} x^{2^6} + \alpha x^{2^3} + \alpha^{118} x$ obtaining

$$F'(x) = \alpha^{337} x^{129} + \alpha^{424} x^{66} + \alpha^2 x^{17} + \alpha x^{10} + \alpha^{34} x^3.$$

- $n = 12$ F' APN is eq. to x^3.

New APN family

For $n = 3m$ with m an odd integer, the family defined over $\mathbb{F}_{2^n}$

$$a^2 x^{2^{2m+1}+1} + b^2 x^{2^{m+1}+1} + ax^{2^{2m}+2} + bx^{2^m+2} + (c^2 + c)x^3$$

is APN for $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$ satisfying the condition in Lemma 6. Moreover it is not equivalent to already known APN families.

The case $n = 6$

For $n = 6$ we checked over general linear functions $L(x)$.
Up to CCZ-equivalence all possible 13 quadratic APN functions can be obtained with one of the following 4 possibilities:

- from an isotopic shift of x^3
  - with the restriction L a permutation,
  - with the restriction L a 2-to-1 map;
- from an isotopic shift of $x^3 + \alpha^{-1} Tr(\alpha^3 x^9)$
  - with the restriction L a permutation,
  - with the restriction L a 2-to-1 map.

Thank you for your attention