APN functions, projective and permutation polynomials

Faruk Göloğlu

Charles University, Prague

BFA 2020
September 17, 2020

APN functions

Setting:

- $Q = 2^n, \mathbb{F} = \mathbb{F}_Q$
- $f : \mathbb{F} \to \mathbb{F}$

Non-zero derivatives of f

$$D_A f = \{f(X) - f(X + A) \ : \ X \in \mathbb{F}\}$$

- (even characteristic) APN if $\# D_A f = \frac{Q}{2}$, i.e., maximal
- (odd characteristic) PN if $\# D_A f = Q$

APN exponents and permutations

Family	Monomial	Conditions	Proved by
Gold	X^{2^i+1}	$\gcd(i,n)=1$	Gold
Kasami	$X^{2^{2i}-2^i+1}$	$\gcd(i,n)=1$	Kasami
Welch	X^{2^t+3}	$n=2t+1$	Dobbertin
Niho	$X^{2^t+2^{\frac{t}{2}}-1}$, t even $X^{2^t+2^{\frac{3t+1}{2}}-1}$, t odd	$n=2t+1$	Dobbertin
Inverse	$X^{2^{2t}-1}$	$n=2t+1$	Nyberg
Dobbertin	$X^{2^{4t}+2^{3t}+2^{2t}+2^t-1}$	$n=5t$	Dobbertin

Table: Known infinite families of APN monomials on $\mathbb{F}_{2^n}$

- n odd: 1-to-1
- n even: 3-to-1

APN permutations

- Exists for all odd n
- Named "big APN problem" for even n
- Exists for $n = 6$, the Kim function (Browning-Dillon-McQuistan-Wolfe 2009) on $\mathbb{F}_{2^6}$

$$\kappa(X) = X^3 + X^{10} + AX^{24},$$

where A is a generator of $\mathbb{F}_{2^6}^*$, is *equivalent* to a permutation.

- "still big APN problem": Does there exist another APN permutation on even dimensions?

Equivalence

EA-equivalence

$$g(X) = L_1(f(L_2(X))) + L_3(X)$$

CCZ-equivalence

Define $G_f = \{(X, f(X))\}$.
f and g are said to be CCZ-equivalent if G_f and G_g are affine-equivalent.

- APN and Walsh properties invariant
- The Kim function κ is CCZ-equivalent to a permutation

Walsh transform

Walsh transform

The *Walsh transform* of f

$$\widehat{f}(A,B) = \sum_{X \in \mathbb{F}} \chi(Af(X) + BX)$$

and Walsh zeroes WZ_f of f is

$$WZ_f = \{(X,Y) \ : \ \widehat{f}(X,Y) = 0\} \cup \{(0,0)\}$$

where $\chi(\cdot) = (-1)^{\mathrm{Tr}(\cdot)}$.

Projective polynomials

Definition

Let $a_{q+1}, a_q, a_1, a_0 \in \mathbb{F}_{2^m}$ and $q = 2^i$. The polynomials of the form

$$a_{q+1}x^{q+1} + a_q x^q + a_1 x + a_0$$

are called projective polynomials.

S. S. Abhyankar, Projective polynomials, Proceedings of the American Mathematical Society 125 (1997), 16431650.

- Generally $a_{q+1} \neq 0$ is assumed.
- Number of zeroes:

$$\{0, 1, 2, 2^{\gcd(i,m)} + 1\}.$$

Antonia W. Bluher: On $x^{q+1} + ax + b$. Finite Fields Their Appl. 10(3): 285-305 (2004)

Projective polynomials

- Let $\mathbb{F} = \mathbb{F}_{2^{2m}}$ and $\mathbb{K} = \mathbb{F}_{2^m}$.
- The vectorial Boolean function

$$F : \mathbb{K} \times \mathbb{K} \to \mathbb{K} \times \mathbb{K}$$

We will set

$$F(x, y) = [f(x, y), g(x, y)],$$

with $q = 2^i, r = 2^j, i, j \geq 1$, and

$$f(x, y) = a_0 x^{q+1} + b_0 x^q y + c_0 x y^q + d_0 y^{q+1},$$
$$g(x, y) = a_1 x^{r+1} + b_1 x^r y + c_1 x y^r + d_1 y^{r+1}.$$

- $f(x, y)$ **bivariate** q**-projective polynomial**
- $F(x, y)$ **bivariate** (q, r)**-projective polynomial pair**
- $f(x, y) = a_0 x^{q+1} + b_0 x^q y + c_0 x y^q + d_0 y^{q+1} = (a_0, b_0, c_0, d_0)_q$.

- The κ function on $\mathbb{F}_{2^6}$, for some $b \in \mathbb{F}_{2^3}$:

$$\kappa'(x, y) = [(0, b, b, b+1)_2, (b, 1, 0, b)_2]$$

APN functions which are (q, r)-projective

- The κ function on $\mathbb{F}_{2^6}$, for some $b \in \mathbb{F}_{2^3}$:

$$\kappa'(x, y) = [(0, b, b, b + 1)_2, (b, 1, 0, b)_2]$$

- Gold functions $\mathrm{G}_i(X) = X^{2^i+1}$. When m is odd:

$$\mathrm{G}_i(x, y) = [(1, 0, 1, 1)_{2^i}, (0, 1, 1, 0)_{2^i}].$$

APN functions which are (q, r)-projective

- The κ function on $\mathbb{F}_{2^6}$, for some $b \in \mathbb{F}_{2^3}$:

$$\kappa'(x, y) = [(0, b, b, b+1)_2, (b, 1, 0, b)_2]$$

- Gold functions $\mathrm{G}_i(X) = X^{2^i+1}$. When m is odd:

$$\mathrm{G}_i(x, y) = [(1, 0, 1, 1)_{2^i}, (0, 1, 1, 0)_{2^i}].$$

- Pott-Zhou APN family:

$$F(x, y) = [(1, 0, 0, d)_{2^i}, (0, 0, 1, 0)_{2^j}], \quad d \in \mathbb{K}^\times,$$

  are APN if and only if $\gcd(i, m) = 1$, m is even and $d \neq a^{2^i+1}(b^{2^i} + b)^{1-2^j}$ for some $a, b \in \mathbb{K}$.

APN functions which are (q, r)-projective

- The κ function on $\mathbb{F}_{2^6}$, for some $b \in \mathbb{F}_{2^3}$:

$$\kappa'(x, y) = [(0, b, b, b+1)_2, (b, 1, 0, b)_2]$$

- Gold functions $\mathrm{G}_i(X) = X^{2^i+1}$. When m is odd:

$$\mathrm{G}_i(x, y) = [(1, 0, 1, 1)_{2^i}, (0, 1, 1, 0)_{2^i}].$$

- Pott-Zhou APN family:

$$F(x, y) = [(1, 0, 0, d)_{2^i}, (0, 0, 1, 0)_{2^j}], \quad d \in \mathbb{K}^\times,$$

  are APN if and only if $\gcd(i, m) = 1$, m is even and $d \neq a^{2^i+1}(b^{2^i} + b)^{1-2^j}$ for some $a, b \in \mathbb{K}$.

- Taniguchi APN family of the form

$$F(x, y) = [(1, 0, c, d)_{2^i}, (0, 1, 0, 0)_{2^{2i}}],$$

  where $\gcd(i, m) = 1$, $f(x, 1) \neq 0$ for any $x \in \mathbb{K}$.

$q = 1$

We should allow $q = 2^0$ to include the first bivariate construction.

- Carlet family:

$$F(x,y) = [xy, (a_1, b_1, c_1, d_1)_r],$$

Carlet shows that F is APN if and only if $g(x,1) \neq 0$ for any $x \in \mathbb{K}$.
Note that

$$ax^2 + bxy + cy^2$$

is the most general, but can be omitted.

Our objective

- Find APN functions imitating the κ function. That is, using (q, r)-projective APN polynomials.
- Hope that it is equivalent to a permutation.

Hybrid Gold APN functions

Recall

- Gold functions $\mathrm{G}_i(X) = X^{2^i+1}$. When m is odd:

$$\mathrm{G}_i(x, y) = [(1,0,1,1)_{2^i}, (0,1,1,0)_{2^i}].$$

- After an $\mathbb{F}_{2^m}$-linear transformation:

$$\mathrm{G}'_i(x, y) = [(1,0,1,1)_{2^i}, (1,1,0,1)_{2^i}].$$

Hybrid Gold APN functions

Recall

- Gold functions $\mathrm{G}_i(X) = X^{2^i+1}$. When m is odd:

$$\mathrm{G}_i(x, y) = [(1, 0, 1, 1)_{2^i}, (0, 1, 1, 0)_{2^i}].$$

- After an $\mathbb{F}_{2^m}$-linear transformation:

$$\mathrm{G}'_i(x, y) = [(1, 0, 1, 1)_{2^i}, (1, 1, 0, 1)_{2^i}].$$

Theorem

The following bivariate (q, r)-projective polynomial pairs $F(x, y) = [f(x, y), g(x, y)]$ are APN on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

$(\mathcal{F}_1)$ $F = [(1, 0, 1, 1)_{2^i}, (1, 1, 0, 1)_{2^{2i}}]$, $\gcd(3i, m) = 1$,

$(\mathcal{F}_2)$ $F = [(1, 0, 1, 1)_{2^i}, (0, 1, 1, 0)_{2^{3i}}]$, $\gcd(3i, m) = 1$, m odd,

$(\mathcal{F}_3)$ $F = [(0, 1, 1, 0)_{2^i}, (1, b, c, d)_{2^{3i}}]$, $i \in \{1, 2\}$, $m = 5$, $(1, b, c, d) \in S_i$.

Proof of $\mathcal{F}_1$

Notation:

- $\mathbb{F}_{2^m} = \mathbb{K}$,
- $3 \nmid m$,
- $q = 2^i$, $\gcd(i, m) = 1$.

Lemma

$\phi_q(u) := u^{q+1} + u + 1 \neq 0$, *for* $u \in \mathbb{K}$.

Proof of $\mathcal{F}_1$

Notation:

- $\mathbb{F}_{2^m} = \mathbb{K}$,
- $3 \nmid m$,
- $q = 2^i$, $\gcd(i, m) = 1$.

Lemma

$\phi_q(u) := u^{q+1} + u + 1 \neq 0$, *for* $u \in \mathbb{K}$.

Note that

$$x\phi_q(x^{q-1}) = x^{q^2} + x^q + x,$$

is a permutation polynomial.

Proof of $\mathcal{F}_1$

We get

$$\psi_q(x) = x^q + x = \frac{(u+1)y^q + y}{\phi_q(u)} =: \mu_u(y),$$

and

$$\psi_{q^2}(x) = x^{q^2} + x = \frac{y^{q^2} + (u+1)^{q^2} y}{\phi_{q^2}(u+1)} =: \nu_u(y).$$

Proof of $\mathcal{F}_1$

We get

$$\psi_q(x) = x^q + x = \frac{(u+1)y^q + y}{\phi_q(u)} =: \mu_u(y),$$

and

$$\psi_{q^2}(x) = x^{q^2} + x = \frac{y^{q^2} + (u+1)^{q^2} y}{\phi_{q^2}(u+1)} =: \nu_u(y).$$

Trivial zeroes: $(x, y) \in \{(0,0), (1,0)\}$.

Proof of $\mathcal{F}_1$

We get

$$\psi_q(x) = x^q + x = \frac{(u+1)y^q + y}{\phi_q(u)} =: \mu_u(y),$$

and

$$\psi_{q^2}(x) = x^{q^2} + x = \frac{y^{q^2} + (u+1)^{q^2} y}{\phi_{q^2}(u+1)} =: \nu_u(y).$$

Trivial zeroes: $(x, y) \in \{(0,0), (1,0)\}$. Note that $(x^q + x) + (x^q + x)^q = x^{q^2} + x$.

Proof of $\mathcal{F}_1$

We get

$$\psi_q(x) = x^q + x = \frac{(u+1)y^q + y}{\phi_q(u)} =: \mu_u(y),$$

and

$$\psi_{q^2}(x) = x^{q^2} + x = \frac{y^{q^2} + (u+1)^{q^2} y}{\phi_{q^2}(u+1)} =: \nu_u(y).$$

Trivial zeroes: $(x, y) \in \{(0,0), (1,0)\}$. Note that
$(x^q + x) + (x^q + x)^q = x^{q^2} + x$.
We will show that

$$\lambda''_u(y) := \mu_u(y) + \mu_u(y)^q + \nu_u(y)$$

is a permutation for every $u \in \mathbb{K} \setminus \mathbb{F}_4$, where

$$\phi_q(u) := u^{q+1} + u + 1 \neq 0,$$
$$\phi_{q^2}(u+1) := u^{q^2+1} + u^{q^2} + 1 \neq 0.$$

Proof of $\mathcal{F}_1$

Show $\lambda_u(y)$ is a permutation:

$$\lambda_u(y) = (\phi_q(u))^2 y^{q^2} + (\phi_{q^2}(u+1))^2 y^q + (\phi_q(u))^{2q} y.$$

Proof of $\mathcal{F}_1$

Show $\lambda_u(y)$ is a permutation:

$$\lambda_u(y) = (\phi_q(u))^2 y^{q^2} + (\phi_{q^2}(u+1))^2 y^q + (\phi_q(u))^{2q} y.$$

The projective polynomial defined by

$$\pi(x) = (\phi_q(u))^2 x^{q+1} + (\phi_{q^2}(u+1))^2 x + (\phi_q(u))^{2q},$$

Proof of $\mathcal{F}_1$

Show $\lambda_u(y)$ is a permutation:

$$\lambda_u(y) =(\phi_q(u))^2 y^{q^2} + (\phi_{q^2}(u+1))^2 y^q + (\phi_q(u))^{2q} y.$$

The projective polynomial defined by

$$\pi(x) = (\phi_q(u))^2 x^{q+1} + (\phi_{q^2}(u+1))^2 x + (\phi_q(u))^{2q},$$

satisfies

$$\pi(x) = (\epsilon_3 x + \epsilon_4)^{q+1} \phi_q \left(\frac{\epsilon_1 x + \epsilon_2}{\epsilon_3 x + \epsilon_4} \right),$$

with

$$\begin{pmatrix} \epsilon_1 & \epsilon_2 \\ \epsilon_3 & \epsilon_4 \end{pmatrix} = \begin{pmatrix} 1 & (u+1)^{2q} \\ (u+1)^2 & u^{2q} \end{pmatrix},$$

whose determinant is conveniently

$$\begin{vmatrix} 1 & (u+1)^{2q} \\ (u+1)^2 & u^{2q} \end{vmatrix} = (\phi_q(u))^2 \neq 0,$$

for any $u \in \mathbb{K} \setminus \mathbb{F}_4$.

Proof of $\mathcal{F}_2$

We want to count the common solutions of

$$\psi_q(x) = x^q + x = \frac{(u+1)y^q + y}{\phi_q(u)} =: \mu_u(y),$$

$$\psi_{q^3}(x) = x^{q^3} + x = \frac{uy^{q^3} + u^{q^3}y}{u^{q^3} + u} =: \sigma_u(y).$$

Proof of $\mathcal{F}_2$

We want to count the common solutions of

$$\psi_q(x) = x^q + x = \frac{(u+1)y^q + y}{\phi_q(u)} =: \mu_u(y),$$

$$\psi_{q^3}(x) = x^{q^3} + x = \frac{uy^{q^3} + u^{q^3}y}{u^{q^3} + u} =: \sigma_u(y).$$

We are going to show that

$$\tau'_u(y) = \mu_u(y) + \mu_u(y)^q + \mu_u(y)^{q^2} + \sigma_u(y)$$

is a 2-to-1 map.

Proof of $\mathcal{F}_2$

We want to count the common solutions of

$$\psi_q(x) = x^q + x = \frac{(u+1)y^q + y}{\phi_q(u)} =: \mu_u(y),$$

$$\psi_{q^3}(x) = x^{q^3} + x = \frac{uy^{q^3} + u^{q^3}y}{u^{q^3} + u} =: \sigma_u(y).$$

We are going to show that

$$\tau'_u(y) = \mu_u(y) + \mu_u(y)^q + \mu_u(y)^{q^2} + \sigma_u(y)$$

is a 2-to-1 map. Simplifying, we get

$$\begin{aligned}\tau_u(y) = & \frac{(\phi_q(u))^{2q}}{(\phi_{q^2}(u+1))^{q-1}(\phi_q(u))^{q^2-1}} y^{q^3} \\ & + \frac{(\phi_q(u))^q \psi_{q^3}(u)}{(\phi_q(u))^{q^2-1}} y^{q^2} \\ & + \frac{(\phi_q(u))^q \psi_{q^3}(u)}{(\phi_{q^2}(u+1))^{q-1}} y^q \\ & + (\phi_q(u))^{2q} y.\end{aligned}$$

Proof of $\mathcal{F}_2$

It can be shown that

$$\tau_u(y) = \lambda_u(y) + \frac{(\lambda_u(y))^q}{C},$$

where

$$C = (\phi_{q^2}(u+1))^{q-1}(\phi_q(u))^{q^2-1},$$

and

$$\lambda_u(y) = (\phi_q(u))^2 y^{q^2} + (\phi_{q^2}(u+1))^2 y^q + (\phi_q(u))^{2q} y,$$

which was defined for Family $\mathcal{F}_1$ previously.

Proof of $\mathcal{F}_2$

It can be shown that

$$\tau_u(y) = \lambda_u(y) + \frac{(\lambda_u(y))^q}{C},$$

where

$$C = (\phi_{q^2}(u+1))^{q-1}(\phi_q(u))^{q^2-1},$$

and

$$\lambda_u(y) = (\phi_q(u))^2 y^{q^2} + (\phi_{q^2}(u+1))^2 y^q + (\phi_q(u))^{2q} y,$$

which was defined for Family $\mathcal{F}_1$ previously.
Now, the kernel satisfies $\ker \tau'_u = \{0, \frac{u^2+u+1}{u}\}$. We then show that:

$$\mu_u\left(\frac{u^2+u+1}{u}\right) = \frac{1}{u^q} + \frac{1}{u} + 1. \quad \square$$

Inequivalence to known APN functions

Define

$$\mathsf{NB}_F := \{U \in \mathbb{F}_{2^n} \ : \ \widehat{F}(U,V) = 0 \text{ for some } V \in \mathbb{F}_{2^n}\}.$$

An *EA*-invariance vector:

$$\mathsf{N}_F := \left[\eta_d(\mathsf{NB}_F) \ : \ 0 \leq d \leq n\right],$$

where $\eta_d(S)$ is the number of $\mathbb{F}_2$-vector spaces of dimension d in S.

Inequivalence to known APN functions

Define

$$\mathrm{NB}_F := \{U \in \mathbb{F}_{2^n} \ : \ \widehat{F}(U,V) = 0 \text{ for some } V \in \mathbb{F}_{2^n}\}.$$

An *EA*-invariance vector:

$$\mathrm{N}_F := \left[\eta_d(\mathrm{NB}_F) \ : \ 0 \le d \le n\right],$$

where $\eta_d(S)$ is the number of $\mathbb{F}_2$-vector spaces of dimension d in S.

Table: EA-invariants N_F for Families $\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2$ and $\mathcal{F}_3$ on $\mathbb{F}_{2^{10}}$

Family	N_F
$\mathcal{F}_0$	$[0, 341, 6820, 3565]$ $[0, 341, 6820, 3720, 31]$
$\mathcal{F}_1$	$[0, 341, 6820, 3565]\dagger$ $[0, 341, 6820, 3720, 31]\dagger$
$\mathcal{F}_2$	$[0, 341, 6820, 3720, 62, 1]$ $[0, 341, 6820, 4030, 62, 1]$
$\mathcal{F}_3$	$[0, 341, 6324, 2573, 62, 2]$

Inequivalence to known APN functions

Table: EA-invariants N_F for Families $\mathcal{F}_0, \mathcal{F}_1$ and $\mathcal{F}_2$ on $\mathbb{F}_{2^{14}}$

Family	N_F
$\mathcal{F}_0$	$[0, 5461, 1681988, 13290042, 428625]$
	$[0, 5461, 1681988, 13313156, 436626]$
	$[0, 5461, 1681988, 13267817, 401828]$
$\mathcal{F}_1$	$[0, 5461, 1681988, 13250164, 394843]^\dagger$
	$[0, 5461, 1681988, 13286867, 438531]^\dagger$
	$[0, 5461, 1681988, 13238480, 398399]$
$\mathcal{F}_2$	$[0, 5461, 1681988, 13293725, 430784, 2667, 127, 1]$
	$[0, 5461, 1681988, 13219303, 413004, 2667, 127, 1]$
	$[0, 5461, 1681988, 13290423, 418084, 2667, 127, 1]$

$\dagger$ corresponds to the cases involving x^3 found independently in: Lilya Budaghyan, Tor Helleseth, Nikolay S. Kaleyski: A new family of APN quadrinomials. IACR Cryptol. ePrint Arch. 2019: 994 (2019)

Inequivalence to known APN functions

Table: EA-invariants N_F for known quadratic APN functions on $\mathbb{F}_{2^{10}}$

Function F	N_F
x^3	$[0, 341, 6820, 5115, 341, 11]$
x^9	$[0, 341, 6820, 5115, 341, 11]$
$x^6 + x^{33} + u^{31}x^{192}$	$[0, 341, 6820, 3720, 31]$
$x^{33} + x^{72} + u^{31}x^{258}$	$[0, 341, 6820, 3720, 31]$
$x^3 + \mathrm{Tr}\left(x^9\right)$	$[0, 341, 6820, 4215, 66, 1]$
$x^3 + u^{341}x^{36}$	$[0, 341, 6820, 4400]$
$x^3 + u^{1022}\mathrm{Tr}\left(u^3x^9\right)$	$[0, 341, 6820, 4250, 66, 1]$
x^{57}	N/A
x^{339}	N/A

Some properties of the new functions

- Quadratic (more generally plateaued) APN functions with $\eta_m(\mathrm{NB}_F) \geq 2$: Kasami, Gold, κ, $\mathcal{F}_3$.

Some properties of the new functions

- Quadratic (more generally plateaued) APN functions with $\eta_m(\mathrm{NB}_F) \geq 2$: Kasami, Gold, κ, $\mathcal{F}_3$.
- Quadratic (more generally plateaued) APN functions with $\eta_m(\mathrm{NB}_F) = 1$: $x^3 + u^{-1}\mathrm{Tr}\left(u^3x^9\right)$, $\mathcal{F}_2$.

Some properties of the new functions

- Quadratic (more generally plateaued) APN functions with $\eta_m(\mathrm{NB}_F) \geq 2$: Kasami, Gold, κ, $\mathcal{F}_3$.
- Quadratic (more generally plateaued) APN functions with $\eta_m(\mathrm{NB}_F) = 1$: $x^3 + u^{-1}\mathrm{Tr}\left(u^3x^9\right)$, $\mathcal{F}_2$.
- Bivariate functions not employing $f(x, y) = xy$.

CCZ-equivalence to permutations

- These functions do not seem to be equivalent to permutations.

CCZ-equivalence to permutations

- These functions do not seem to be equivalent to permutations.
- What about (q, q)-projective functions?

CCZ-equivalence to permutations

- These functions do not seem to be equivalent to permutations.
- What about (q, q)-projective functions?
- What about (q, r)-projective functions in general?

CCZ-equivalence to permutations

- These functions do not seem to be equivalent to permutations.
- What about (q, q)-projective functions?
- What about (q, r)-projective functions in general?
- A few observations on the κ function.

Walsh zeroes of a permutation f

$$\mathbb{F} = \mathbb{F}_{2^{2m}}, \quad \mathbb{K} = \mathbb{F}_{2^m}$$

$$\widehat{F}(A,B) = \sum_{X \in \mathbb{F}} \chi(AF(X) + BX)$$

$A \backslash B$	0	$v_1\mathbb{K}^*$	$v_2\mathbb{K}^*$	$\cdots$	$v_t\mathbb{K}^*$
0					
$u_1\mathbb{K}^*$					
$u_2\mathbb{K}^*$					
$\vdots$					
$u_t\mathbb{K}^*$					

Properties of κ

- An APN function f on $\mathbb{F}_{2^n}$ is CCZ-equivalent to a permutation if the Walsh zeroes of f contains two subspaces of dimension n intersecting only trivially.
- Walsh zeroes of κ has more structure with respect to some subspaces, i.e.,

$$\{(u_1 x, v_1 y) \ : \ x, y \in \mathbb{K}\}, \{(u_2 x, v_2 y) \ : \ x, y \in \mathbb{K}\} \subseteq WZ_f$$

for some $u_1, u_2, v_1, v_2 \in \mathcal{P}_7$, i.e., 7th powers in $\mathbb{F}^*$.

Walsh zeroes of the Kim function

$$\kappa(X) = X^3 + X^{10} + AX^{24}$$

$$\widehat{f}(A,B) = \sum_{X \in \mathbb{F}} \chi\left(Af(X) + BX\right)$$

	0	$v_1\mathbb{K}^*$	$v_2\mathbb{K}^*$	$\cdots$	$v_t\mathbb{K}^*$
0					
$u_1\mathbb{K}^*$					
$u_2\mathbb{K}^*$					
$\vdots$					
$u_t\mathbb{K}^*$					

CCZ-equivalence

$F \sim_{CCZ} G$ means:
Bijective $\mathcal{L}$

$$\mathcal{L}(X, Y) = (A(X) + B(Y) + a, C(X) + D(Y) + b)$$

such that $\mathcal{L}(G_F) = G_G$. That is to say $G = \pi_2 \circ \pi_1^{-1}$, with

$$A(X) + B(f(X)) + a = \pi_1(X),$$
$$C(X) + D(f(X)) + b = \pi_2(X),$$

where A, B, C, D are $\mathbb{F}_2$-linear maps and π_1 is a permutation.

$\mathbb{K}$-CCZ equivalence

In the case of the κ function, A, B, C, D are $\mathbb{K}$-linear maps (with rank m), hence the "square" structure of Walsh-zero spaces.

Definition

If F is CCZ equivalent to G with $\mathbb{K}$-linear maps (with rank m) A, B, C, D, then we say F is $\mathbb{K}$-CCZ equivalent to G.

$\mathbb{K}$-CCZ equivalence

In the case of the κ function, A, B, C, D are $\mathbb{K}$-linear maps (with rank m), hence the "square" structure of Walsh-zero spaces.

Definition

If F is CCZ equivalent to G with $\mathbb{K}$-linear maps (with rank m) A, B, C, D, then we say F is $\mathbb{K}$-CCZ equivalent to G.

Proposition

If a (q, q)-projective APN polynomial $F = [f(x, y), g(x, y)]$ is $\mathbb{K}$-CCZ equivalent to a permutation then

$$f(x, y) = (a_0 x + b_0 y)^{q+1} + (c_0 x + d_0 y)^{q+1},$$
$$g(x, y) = (a_1 x + b_1 y)^{q+1} + (c_1 x + d_1 y)^{q+1},$$

for some "nonsingular" coefficients.

Hence we can assume w.l.o.g. $f(x, y) = (1, 0, 0, 1)_q$.

Equivalence problem to APN permutations

If for some $a, b, c, d \in \mathbb{K}$ the function $F = [(1, 0, 0, 1)_q, (a, b, c, d)_q]$ is APN, then:

$$\begin{aligned} U^{q+1}(X + X^q) + (Y + Y^q) &= 0, \\ aU^q(X + X^q) + bU^q(Y + X^q) + cU(X + Y^q) + d(Y + Y^q) &= 0. \end{aligned}$$

should hold only for $X = Y = 0$ and $X = Y = 1$ for all non-zero $U \in \mathbb{F}$.

Equivalence problem to APN permutations

If for some $a, b, c, d \in \mathbb{K}$ the function $F = [(1,0,0,1)_q, (a,b,c,d)_q]$ is APN, then:

$$\begin{aligned} U^{q+1}(X + X^q) + (Y + Y^q) &= 0, \\ aU^q(X + X^q) + bU^q(Y + X^q) + cU(X + Y^q) + d(Y + Y^q) &= 0. \end{aligned}$$

should hold only for $X = Y = 0$ and $X = Y = 1$ for all non-zero $U \in \mathbb{F}$. Equivalently, there is no (q, q)-projective bivariate APN polynomial which is equivalent to a permutation, if

$$\left(\frac{Y + Y^q}{X + X^q}\right)\left(\frac{X + Y^q}{Y + Y^q}\right)^{q+1} = A$$

is satisfied for all $A \in \mathbb{K}$ by some $X, Y \in \mathbb{K} \setminus \{0, 1\}$.

Equivalence problem

After some modifications we get the equivalent condition: If a (q, q)-projective APN function is $\mathbb{K}$-CCZ equivalent to a permutation then there exists $A \in \mathbb{K}^\times$ such that

$$X^{q+1} + X + A\frac{(\beta^2+\beta)^q}{(\beta^q+\beta)^{q+1}} = 0$$

has exactly two solutions (x_0, β_0) and (x_0, β_1) for $x \in \mathbb{K}^\times$ and $\beta \in \mathbb{K}^{\times\times}$.

Equivalence problem

After some modifications we get the equivalent condition: If a (q, q)-projective APN function is $\mathbb{K}$-CCZ equivalent to a permutation then there exists $A \in \mathbb{K}^\times$ such that

$$X^{q+1} + X + A\frac{(\beta^2 + \beta)^q}{(\beta^q + \beta)^{q+1}} = 0$$

has exactly two solutions (x_0, β_0) and (x_0, β_1) for $x \in \mathbb{K}^\times$ and $\beta \in \mathbb{K}^{\times\times}$.

Theorem (Helleseth,Kholosha 2008)

The projective polynomial $X^{q+1} + X + C$ has exactly one solution if and only if $C \in DD := \left\{ \frac{(\beta^2+\beta)^q}{(\beta^q+\beta)^{q+1}} : \beta \in \mathbb{K}^{\times\times} \right\}$.

Equivalence problem

After some modifications we get the equivalent condition: If a (q, q)-projective APN function is $\mathbb{K}$-CCZ equivalent to a permutation then there exists $A \in \mathbb{K}^\times$ such that

$$X^{q+1} + X + A\frac{(\beta^2 + \beta)^q}{(\beta^q + \beta)^{q+1}} = 0$$

has exactly two solutions (x_0, β_0) and (x_0, β_1) for $x \in \mathbb{K}^\times$ and $\beta \in \mathbb{K}^{\times\times}$.

Theorem (Helleseth,Kholosha 2008)

The projective polynomial $X^{q+1} + X + C$ has exactly one solution if and only if $C \in DD := \left\{\frac{(\beta^2+\beta)^q}{(\beta^q+\beta)^{q+1}} : \beta \in \mathbb{K}^{\times\times}\right\}$.

Thus we have a lot of solutions for $A = 1$. This is also easy to see from the original equation.

Equivalence problem

Theorem (Dillon, Dobbertin 1999)

The set DD is a difference set in $\mathbb{K}^*$ with Singer parameters $(|\mathbb{K}| - 1, \frac{|\mathbb{K}|}{2} - 1, \frac{|\mathbb{K}|}{4} - 1)$.

Equivalence problem

Theorem (Dillon, Dobbertin 1999)

The set DD is a difference set in $\mathbb{K}^*$ with Singer parameters $(|\mathbb{K}|-1, \frac{|\mathbb{K}|}{2}-1, \frac{|\mathbb{K}|}{4}-1)$.

That is to say, when x, y runs through DD,

$$\frac{x}{y} = \alpha$$

holds $\frac{|\mathbb{K}|}{4} - 1$ times for each $\alpha \in \mathbb{K}^{\times\times}$. Or, equivalently

$$|DD \cap \alpha DD| = \frac{|\mathbb{K}|}{4} - 1.$$

Equivalence problem

Theorem (Dillon, Dobbertin 1999)

The set DD is a difference set in $\mathbb{K}^*$ *with Singer parameters* $(|\mathbb{K}|-1, \frac{|\mathbb{K}|}{2}-1, \frac{|\mathbb{K}|}{4}-1)$.

That is to say, when x, y runs through DD,

$$\frac{x}{y} = \alpha$$

holds $\frac{|\mathbb{K}|}{4} - 1$ times for each $\alpha \in \mathbb{K}^{\times\times}$. Or, equivalently

$$|DD \cap \alpha DD| = \frac{|\mathbb{K}|}{4} - 1.$$

Therefore, our equation holds exactly twice, only if

$$\frac{|\mathbb{K}|}{4} - 1 = 1,$$

thus,

$$\mathbb{K} = \mathbb{F}_{2^3}.$$

The result

Theorem

If a (q, q)-projective APN polynomial F is $\mathbb{K}$-CCZ equivalent to a permutation then $F \sim \kappa : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$.

The result

Theorem

If a (q, q)-projective APN polynomial F is $\mathbb{K}$-CCZ equivalent to a permutation then $F \sim \kappa : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$.

A related result:

Theorem (Canteaut,Perrin,Tian 2019)

If a generalized butterfly

$$F = [(x + ay)^{q+1} + by^{q+1}, (ax + y)^{q+1} + bx^{q+1}]$$

is APN then $F \sim \kappa : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$.

The result

Theorem

If a (q,q)-projective APN polynomial F is $\mathbb{K}$-CCZ equivalent to a permutation then $F \sim \kappa : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$.

A related result:

Theorem (Canteaut,Perrin,Tian 2019)

If a generalized butterfly

$$F = [(x+ay)^{q+1} + by^{q+1}, (ax+y)^{q+1} + bx^{q+1}]$$

is APN then $F \sim \kappa : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$.

Recall

$$f(x,y) = (a_0x + b_0y)^{q+1} + (c_0x + d_0y)^{q+1},$$
$$g(x,y) = (a_1x + b_1y)^{q+1} + (c_1x + d_1y)^{q+1}.$$

Anne Canteaut, Lo Perrin, Shizhu Tian: If a generalised butterfly is APN then it operates on 6 bits. Cryptogr. Commun. 11(6): 1147-1164 (2019)

What happens when $q \neq r$

- One can choose $F = [f, g]$ where

$$f(x, y) = (a_0 x + b_0 y)^{q+1} + (c_0 x + d_0 y)^{q+1},$$
$$g(x, y) = (a_1 x + b_1 y)^{r+1} + (c_1 x + d_1 y)^{r+1}.$$

- Note that the "square" Walsh-zero structure of f is independent of the way we combine it with another function g. Thus these functions are (most of the time) $\mathbb{K}$-CCZ equivalent to permutations.

What happens when $q \neq r$

- One can choose $F = [f, g]$ where

$$f(x,y) = (a_0x + b_0y)^{q+1} + (c_0x + d_0y)^{q+1},$$
$$g(x,y) = (a_1x + b_1y)^{r+1} + (c_1x + d_1y)^{r+1}.$$

- Note that the "square" Walsh-zero structure of f is independent of the way we combine it with another function g. Thus these functions are (most of the time) $\mathbb{K}$-CCZ equivalent to permutations.
- One difficulty lies in the fact that the $\mathbb{K}$-linear combinations $\alpha f + \beta g$ are not anymore projective.

What happens when $q \neq r$

- One can choose $F = [f, g]$ where

$$f(x,y) = (a_0x + b_0y)^{q+1} + (c_0x + d_0y)^{q+1},$$
$$g(x,y) = (a_1x + b_1y)^{r+1} + (c_1x + d_1y)^{r+1}.$$

- Note that the "square" Walsh-zero structure of f is independent of the way we combine it with another function g. Thus these functions are (most of the time) $\mathbb{K}$-CCZ equivalent to permutations.
- One difficulty lies in the fact that the $\mathbb{K}$-linear combinations $\alpha f + \beta g$ are not anymore projective.
- Equations are extremely complicated.

What happens when $q \neq r$

- One can choose $F = [f, g]$ where

$$f(x,y) = (a_0x + b_0y)^{q+1} + (c_0x + d_0y)^{q+1},$$
$$g(x,y) = (a_1x + b_1y)^{r+1} + (c_1x + d_1y)^{r+1}.$$

- Note that the "square" Walsh-zero structure of f is independent of the way we combine it with another function g. Thus these functions are (most of the time) $\mathbb{K}$-CCZ equivalent to permutations.
- One difficulty lies in the fact that the $\mathbb{K}$-linear combinations $\alpha f + \beta g$ are not anymore projective.
- Equations are extremely complicated.
- Partial theoretical results.

What happens when $q \neq r$

- One can choose $F = [f, g]$ where

$$f(x,y) = (a_0x + b_0y)^{q+1} + (c_0x + d_0y)^{q+1},$$
$$g(x,y) = (a_1x + b_1y)^{r+1} + (c_1x + d_1y)^{r+1}.$$

- Note that the “square” Walsh-zero structure of f is independent of the way we combine it with another function g. Thus these functions are (most of the time) $\mathbb{K}$-CCZ equivalent to permutations.
- One difficulty lies in the fact that the $\mathbb{K}$-linear combinations $\alpha f + \beta g$ are not anymore projective.
- Equations are extremely complicated.
- Partial theoretical results.
- Computer data suggest no such APN function up to dimension 30.

Non-projective extensions

- Find bivariate functions

$$g := \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$

with an n-dimensional Walsh-zero space (all 2^m components should be involved) and good differential properties ($2|\mathbb{K}|$-differential uniform, so that it can be extended to an APN function) and combine it with a q-projective f, hoping to get an APN function.

Non-projective extensions

- Find bivariate functions

$$g := \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$

  with an n-dimensional Walsh-zero space (all 2^m components should be involved) and good differential properties ($2|\mathbb{K}|$-differential uniform, so that it can be extended to an APN function) and combine it with a q-projective f, hoping to get an APN function.

- Combine a projective f with a non-quadratic function, possibly a monomial or a homogenous function.

Non-projective extensions

- Find bivariate functions

$$g := \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$

  with an n-dimensional Walsh-zero space (all 2^m components should be involved) and good differential properties ($2|\mathbb{K}|$-differential uniform, so that it can be extended to an APN function) and combine it with a q-projective f, hoping to get an APN function.

- Combine a projective f with a non-quadratic function, possibly a monomial or a homogenous function.

- For instance try quartic homogenous functions

$$ax^3y + bx^2y^2 + cxy^3.$$

Non-projective extensions

- Find bivariate functions
$$g := \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$
with an n-dimensional Walsh-zero space (all 2^m components should be involved) and good differential properties ($2|\mathbb{K}|$-differential uniform, so that it can be extended to an APN function) and combine it with a q-projective f, hoping to get an APN function.
- Combine a projective f with a non-quadratic function, possibly a monomial or a homogenous function.
- For instance try quartic homogenous functions
$$ax^3y + bx^2y^2 + cxy^3.$$
- Non-classical Walsh spectrum problem can be attacked similarly.

Non-classical Walsh spectrum

- Walsh spectrum of an APN function is defined as the set
$$\{\widehat{F}(u,v) : u \in \mathbb{F}, v \in \mathbb{F}^{\times}\}.$$
- All quadratic APN functions on an odd dimension n have the same Walsh spectrum
$$\{0, \pm 2^{\frac{n+1}{2}}\}.$$
- Majority of the quadratic APN functions (also plateaued ones) on an even dimension $n = 2m$ have the spectrum
$$\{0, \pm 2^{m}, \pm 2^{m+1}\},$$
which is called the classical spectrum.
- On $\mathbb{F}_{2^6}$, up to equivalence, one function, namely
$$F(X) = X^3 + U^{11}X^5 + U^{13}X^9 + X^{17} + U^{11}X^{33} + X^{48}$$
introduced in Browning, Dillon, Kibler, and McQuistan (2009) with a non-classical spectrum:
$$\{0, \pm 2^{m}, \pm 2^{m+1}, 2^{m+2}\},$$

Non-classical Walsh spectrum

We observe that (joint work with Michal Maršalek) the function

$$f := \mathbb{F}_{2^3} \times \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}$$

defined as

$$f(x, y) = x^2y + y^2x + xy$$

contains non-classical Walsh value 2^{m+2} if n is odd. Using bivariate maps we can write

$$F = [x^2y + xy^2 + xy, x^3 + ay^3 + L(x, y)].$$

Question

Can this be generalized?

Non-classical Walsh spectrum

Theorem

If n is odd, a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ of the type

$$F = [x^2y + xy^2 + xy, x^3 + ay^3 + L(x, y)].$$

is not APN if $n \geq 9$.

We prove after lengthy analysis that L should satisfy (polynomially)

$$\mathrm{Tr}\left(\frac{L(x, x+1)}{x^3}\right) = \sum_{i=1}^{2^n-2} x^i.$$

Counting the number of terms, we see that

$$n(n^2 + n)/2 \geq 2^n - 2$$

should hold, which is impossible if $n \geq 9$.

Thanks for your attention.