Geometrical structures among known APN functions

Jules Baudrin, Anne Canteaut & Léo Perrin

Inria, Paris, France

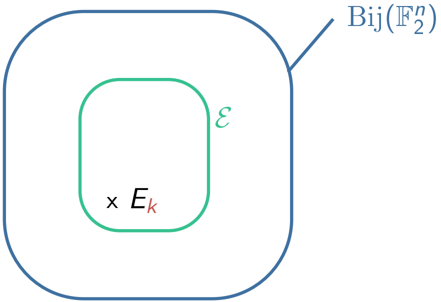
July 5th, 2024

Contact: jules.baudrin@inria.fr

A bit of context

Block cipher

A family of bijections $\mathcal{E} = (E_k)_{k \in K}$: $\forall\, k \in K, \quad E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n.$



$$y = E_k(x) \iff x = (E_k)^{-1}(y)$$

Kerckhoffs

- Publicly known bijections $\mathcal{E}$
- Only the choice of E_k by A and B is unknown

Block ciphers in practice

$$y = E_k(x) \iff x = (E_k)^{-1}(y)$$

Indistinguishability

$[\ E \xleftarrow{\$} \mathcal{E}\ ]$ indistinguishable from $[\ F \xleftarrow{\$} \mathrm{Bij}(\mathbb{F}_2^n)\ ]$.

Major constraints

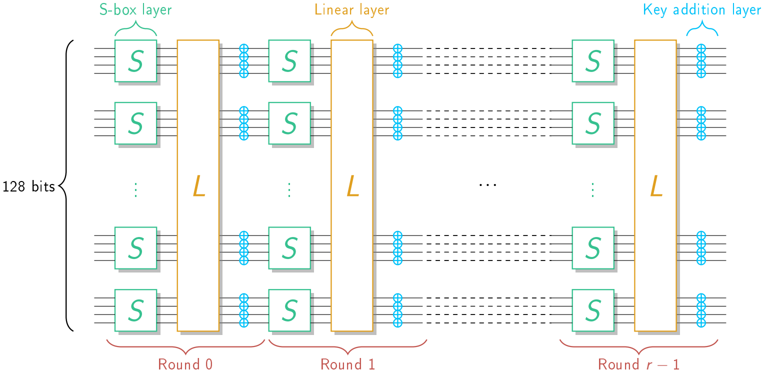
$|K| = 2^{128}$, $n = 64, 128$

- $\mathcal{E}$ should be easily implemented,
- $\mathcal{E}$ should be "easily" analyzed.

Substitution Permutation Network (SPN)

3-step round function

- Local non-linear layer, global linear layer, and key/constant addition
- Repeat r times



$\mathcal{E}$ should be easily implemented ☑

Differential distinguisher

Differential distinguisher

Find α, β st. for many k, $E_k(x + \alpha) = E_k(x) + \beta$ has many solutions x.

Random permutation F

$F(x + \alpha) + F(x) = \beta$ with proba 2^{-n}.

Differential distinguisher

Differential distinguisher

Find α, β st. for many k, $E_k(x+\alpha) = E_k(x) + \beta$ has many solutions x.

Random permutation F

$F(x+\alpha) + F(x) = \beta$ with proba 2^{-n}.

Wide trail strategy

- Sbox layer, $\rightsquigarrow$ $S(x+\alpha) = S(x) + \beta$ must have few solutions for all α, β
- Linear layer must diffuse a lot
- Key schedule should be built carefully.

Differential distinguisher

Differential distinguisher

Find α, β st. for many k, $E_k(x+\alpha) = E_k(x) + \beta$ has many solutions x.

Random permutation F

$F(x+\alpha) + F(x) = \beta$ with proba 2^{-n}.

Wide trail strategy

- Sbox layer, $\rightsquigarrow S(x+\alpha) = S(x) + \beta$ must have few solutions for all α, β
- Linear layer must diffuse a lot
- Key schedule should be built carefully.

How much **differentially-resistant** can an Sbox be?

Vectorial Boolean functions

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

Vectorial Boolean functions

$$F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$$

Representations

- Multivariate $F = (F_1, \ldots, F_n)$ where $F_i\colon \mathbb{F}_2^n \to \mathbb{F}_2$ — n coordinates in n variables ($\mathbb{F}_2$)
- Univariate: (up to identification) $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ — 1 coordinate, 1 variable ($\mathbb{F}_{2^n}$)

Vectorial Boolean functions

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

Representations

- Multivariate $F = (F_1, \ldots, F_n)$ where $F_i : \mathbb{F}_2^n \to \mathbb{F}_2$ — n coordinates in n variables ($\mathbb{F}_2$)
- Univariate: (up to identification) $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ — 1 coordinate, 1 variable ($\mathbb{F}_{2^n}$)

Every function is polynomial

- Multivariate degree $\max_{i=1,\ldots,n}(\deg(F_i))$
- Univariate degree $\deg(F)$
- Linear, quadratic. . . refer to multivariate

Vectorial Boolean functions

$$F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$$

Representations

- Multivariate $F = (F_1, \ldots, F_n)$ where $F_i\colon \mathbb{F}_2^n \to \mathbb{F}_2$ — n coordinates in n variables ($\mathbb{F}_2$)
- Univariate: (up to identification) $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ — 1 coordinate, 1 variable ($\mathbb{F}_{2^n}$)

Every function is polynomial

- Multivariate degree $\max_{i=1,\ldots,n}(\deg(F_i))$
- Univariate degree $\deg(F)$
- Linear, quadratic. . . refer to multivariate

$F\colon \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}, X \mapsto X^3 + X^{10} + uX^{24}$ — $\deg(F) = 24$

Vectorial Boolean functions

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

Representations

- Multivariate $F = (F_1, \ldots, F_n)$ where $F_i : \mathbb{F}_2^n \to \mathbb{F}_2$ — n coordinates in n variables ($\mathbb{F}_2$)
- Univariate: (up to identification) $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ — 1 coordinate, 1 variable ($\mathbb{F}_{2^n}$)

Every function is polynomial

- Multivariate degree $\max_{i=1,\ldots,n}(\deg(F_i))$
- Univariate degree $\deg(F)$
- Linear, quadratic. . . refer to multivariate

$F : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}, X \mapsto X^3 + X^{10} + uX^{24}$ — $\deg(F) = 24$

$F_1 = x_1x_4 + x_1x_5 + x_2x_3 + x_2x_6 + x_3 + x_4x_5 + x_4x_6 + x_4 + x_5$ — $\deg(F_1) = 2$

$\vdots$

$F_6 = x_1x_2 + x_1x_4 + x_2x_4 + x_2x_5 + x_2 + x_3x_4 + x_3x_6 + x_4 + x_5x_6 + x_6$ — $\deg(F_6) = 2$

Vectorial Boolean functions

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

Representations

- Multivariate $F = (F_1, \dots, F_n)$ where $F_i : \mathbb{F}_2^n \to \mathbb{F}_2$ — n coordinates in n variables ($\mathbb{F}_2$)
- Univariate: (up to identification) $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ — 1 coordinate, 1 variable ($\mathbb{F}_{2^n}$)

Every function is polynomial

- Multivariate degree $\max_{i=1,\dots,n}(\deg(F_i))$
- Univariate degree $\deg(F)$
- Linear, quadratic... refer to multivariate

$F : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}, X \mapsto X^3 + X^{10} + uX^{24}$ — $\deg(F) = 24$

F is quadratic

Vectorial Boolean functions

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

Representations

- Multivariate $F = (F_1, \dots, F_n)$ where $F_i : \mathbb{F}_2^n \to \mathbb{F}_2$ — n coordinates in n variables $(\mathbb{F}_2)$
- Univariate: (up to identification) $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ — 1 coordinate, 1 variable $(\mathbb{F}_{2^n})$

Every function is polynomial

- Multivariate degree $\max_{i=1,\dots,n}(\deg(F_i))$
- Univariate degree $\deg(F)$
- Linear, quadratic. . . refer to multivariate

$F : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}, X \mapsto X^3 + X^{10} + uX^{24}$ — $\deg(F) = 24$

F is quadratic — $3 = 0b000011$, $10 = 0b001010$, $24 = 0b011000$

APN functions

$$\forall \alpha, \beta, \quad \delta_F(\alpha, \beta) := |\{x \in \mathbb{F}_{2^n},\ F(x+\alpha) + F(x) = \beta\}|$$

APN functions

$$\forall \alpha, \beta, \quad \delta_F(\alpha, \beta) := |\{x \in \mathbb{F}_{2^n},\ F(x+\alpha) + F(x) = \beta\}|$$

Differential uniformity

The differential uniformity of F is $\Delta_F := \max_{\alpha \neq 0, \beta} \delta_F(\alpha, \beta)$.

A function is Almost Perfect Non-linear (APN) if $\Delta_F = 2$.

APN functions

$$\forall \alpha, \beta, \quad \delta_F(\alpha, \beta) := |\{x \in \mathbb{F}_{2^n}, \; F(x+\alpha) + F(x) = \beta\}|$$

Differential uniformity

The differential uniformity of F is $\Delta_F := \max_{\alpha \neq 0, \beta} \delta_F(\alpha, \beta)$.

A function is Almost Perfect Non-linear (APN) if $\Delta_F = 2$.

The linear case

F linear.

$$F(x+\alpha) + F(x) \quad = \quad F(x) + F(\alpha) + F(x) \quad = \quad F(\alpha)$$

$\alpha \neq 0$. $\qquad \delta_F(\alpha, \beta) = \begin{cases} 2^n & \text{if } \beta = F(\alpha) \\ 0 & \text{otherwise.} \end{cases}$

APN functions

$$\forall \alpha, \beta, \quad \delta_F(\alpha, \beta) := |\{x \in \mathbb{F}_{2^n},\ F(x+\alpha) + F(x) = \beta\}|$$

Differential uniformity

The differential uniformity of F is $\Delta_F := \max_{\alpha \neq 0, \beta} \delta_F(\alpha, \beta)$.

A function is Almost Perfect Non-linear (APN) if $\Delta_F = 2$.

The linear case

F linear.

$$F(x+\alpha) + F(x) = F(x) + F(\alpha) + F(x) = F(\alpha)$$

$\alpha \neq 0$. $$\delta_F(\alpha, \beta) = \begin{cases} 2^n & \text{if } \beta = F(\alpha) \\ 0 & \text{otherwise.} \end{cases}$$

The APN case

F APN. Then $\forall\ \alpha \neq 0, \quad |\{\beta,\ \ \delta_F(\alpha, \beta) > 0\}| = 2^{n-1}$.

Equivalence relations

$F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n, \qquad \mathcal{G}_F = \left\{ \begin{pmatrix} x \\ F(x) \end{pmatrix}, x \in \mathbb{F}_{2^n} \right\}, \qquad \mathcal{G}_G = \left\{ \begin{pmatrix} x \\ G(x) \end{pmatrix}, x \in \mathbb{F}_{2^n} \right\}$

Equivalence relations

$F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n, \qquad \mathcal{G}_F = \left\{ \begin{pmatrix} x \\ F(x) \end{pmatrix}, x \in \mathbb{F}_{2^n} \right\}, \qquad \mathcal{G}_G = \left\{ \begin{pmatrix} x \\ G(x) \end{pmatrix}, x \in \mathbb{F}_{2^n} \right\}$

Affine equivalence

$$F \sim_A G \iff \exists\, A, B \quad A \circ F \circ B = G \iff \begin{pmatrix} B^{-1} & 0 \\ 0 & A \end{pmatrix} \mathcal{G}_F = \mathcal{G}_G$$

with A, B affine, bijective.

Equivalence relations

$F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n, \quad \mathcal{G}_F = \left\{ \begin{pmatrix} x \\ F(x) \end{pmatrix}, x \in \mathbb{F}_{2^n} \right\}, \quad \mathcal{G}_G = \left\{ \begin{pmatrix} x \\ G(x) \end{pmatrix}, x \in \mathbb{F}_{2^n} \right\}$

Affine equivalence

$$F \sim_A G \iff \exists\, A, B \quad A \circ F \circ B = G \iff \begin{pmatrix} B^{-1} & 0 \\ 0 & A \end{pmatrix} \mathcal{G}_F = \mathcal{G}_G$$

with A, B affine, bijective.

Extended-affine equivalence

$$F \sim_{EA} G \iff \exists\, A, B, C \quad A \circ F \circ B + C = G \iff \begin{pmatrix} B^{-1} & 0 \\ CB^{-1} & A \end{pmatrix} \mathcal{G}_F = \mathcal{G}_G$$

with A, B, C affine, A, B bijective.

Equivalence relations

$F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n, \qquad \mathcal{G}_F = \left\{ \begin{pmatrix} x \\ F(x) \end{pmatrix}, x \in \mathbb{F}_{2^n} \right\}, \qquad \mathcal{G}_G = \left\{ \begin{pmatrix} x \\ G(x) \end{pmatrix}, x \in \mathbb{F}_{2^n} \right\}$

Affine equivalence

$$F \sim_A G \iff \exists\, A, B \quad A \circ F \circ B = G \iff \begin{pmatrix} B^{-1} & 0 \\ 0 & A \end{pmatrix} \mathcal{G}_F = \mathcal{G}_G$$

with A, B affine, bijective.

Extended-affine equivalence

$$F \sim_{\mathrm{EA}} G \iff \exists\, A, B, C \quad A \circ F \circ B + C = G \iff \begin{pmatrix} B^{-1} & 0 \\ CB^{-1} & A \end{pmatrix} \mathcal{G}_F = \mathcal{G}_G$$

with A, B, C affine, A, B bijective.

CCZ equivalence

$F \sim_{\mathrm{CCZ}} G \iff \exists\, \mathcal{A}$ affine, bijective $\quad \mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G$. $\qquad \mathcal{A} = \mathcal{L} + c$

CCZ equivalence and differential properties

$F \sim_{\mathsf{EA}} G \iff \exists\, A, B, C \quad A \circ F \circ B + C = G$

$F \sim_{\mathsf{CCZ}} G \iff \exists\, \mathcal{A}$ affine, bijective $\quad \mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G. \qquad \mathcal{A} = \mathcal{L} + c$

Example

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ bijective. Then $F \sim_{\mathsf{CCZ}} F^{-1}$.

$$\mathcal{G}_{F^{-1}} = \begin{pmatrix} 0 & \mathrm{Id} \\ \mathrm{Id} & 0 \end{pmatrix} \mathcal{G}_F$$

CCZ equivalence and differential properties

$F \sim_{\mathrm{EA}} G \iff \exists\, A, B, C \quad A \circ F \circ B + C = G$

$F \sim_{\mathrm{CCZ}} G \iff \exists\, \mathcal{A}$ affine, bijective $\quad \mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G$. $\qquad \mathcal{A} = \mathcal{L} + c$

Example

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ bijective. Then $F \sim_{\mathrm{CCZ}} F^{-1}$.

$$\mathcal{G}_{F^{-1}} = \begin{pmatrix} 0 & \mathrm{Id} \\ \mathrm{Id} & 0 \end{pmatrix} \mathcal{G}_F$$

Main usage of CCZ equivalence

Let $F \sim_{\mathrm{CCZ}} G$. Then $\forall\, \alpha, \beta, \quad \delta_G(\alpha, \beta) = \delta_F(\mathcal{L}^{-1}(\alpha, \beta))$.

CCZ equivalence and differential properties

$F \sim_{\mathrm{EA}} G \iff \exists\, A, B, C \quad A \circ F \circ B + C = G$

$F \sim_{\mathrm{CCZ}} G \iff \exists\, \mathcal{A}$ affine, bijective $\quad \mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G$. $\qquad \mathcal{A} = \mathcal{L} + c$

Example

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ bijective. Then $F \sim_{\mathrm{CCZ}} F^{-1}$.

$$\mathcal{G}_{F^{-1}} = \begin{pmatrix} 0 & \mathrm{Id} \\ \mathrm{Id} & 0 \end{pmatrix} \mathcal{G}_F$$

Main usage of CCZ equivalence

Let $F \sim_{\mathrm{CCZ}} G$. Then $\forall\, \alpha, \beta, \quad \delta_G(\alpha, \beta) = \delta_F(\mathcal{L}^{-1}(\alpha, \beta))$.

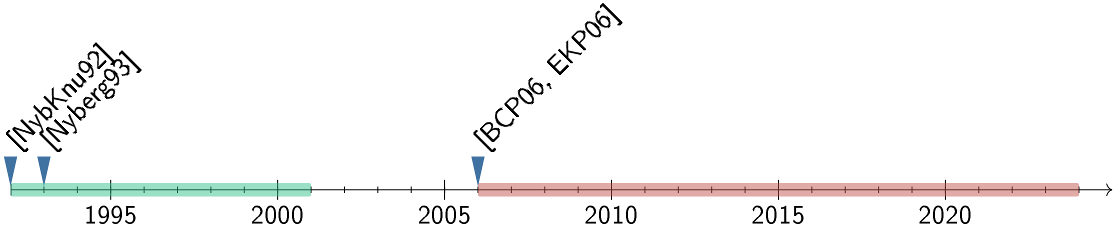
Invariants

$F \sim_{\mathrm{CCZ}} G \implies \Delta_F = \Delta_G$.

$F \sim_{\mathrm{CCZ}} G \not\Longrightarrow \mathrm{multideg}(F) = \mathrm{multideg}(G)$.

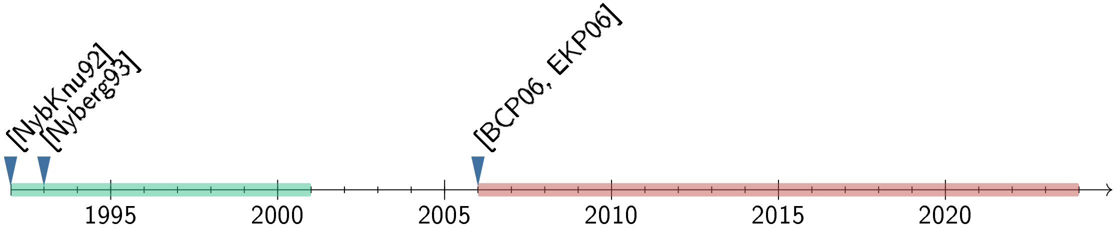
But $F \sim_{\mathrm{EA}} G \implies \mathrm{multideg}(F) = \mathrm{multideg}(G)$.

Known APN constructions



- 1992: APN definition [NybKnu92]
- 1993: First APN power mappings $x \mapsto x^{2^i+1}$ [Nyberg93]
- 1993-2001: 5 more families of APN non-quadratic power mappings

Known APN constructions



- 1992: APN definition [NybKnu92]
- 1993: First APN power mappings $x \mapsto x^{2^i+1}$ [Nyberg93]
- 1993-2001: 5 more families of APN non-quadratic power mappings

- 2006: First APN functions CCZ-inequivalent to a power function. [BCP06, EKP06]
- 2007-2024 : $\simeq$ 20 infinite families of quadratic APN functions.

LOTS of open questions

Two major classes

1) Power mappings $x \mapsto x^d$
2) Quadratic functions

All known APN functions are CCZ-equiv to 1) or 2) ... except one.

More APN functions CCZ-inequivalent to monomials and quadratic functions?

LOTS of open questions

Two major classes

1) Power mappings $x \mapsto x^d$
2) Quadratic functions

All known APN functions are CCZ-equiv to 1) or 2) ... except one.

More APN functions CCZ-inequivalent to monomials and quadratic functions?

APN bijections

- Some are known for odd n (e.g. APN powers)
- None are known for even n ... except one.

Big APN problem: More APN bijections in even dimension ?

Zoo of APN functions

ID	Functions	Conditions	Source
F1-F2	$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk, \gcd(k,3) = \gcd(s,3k) = 1, p \in \{3,4\}, i = sk \bmod p, m = p - i, n \geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$	[10]
F3	$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)} + cx^{2^iq+1} + c^q x^{2^i+q}$	$q = 2^m, n = 2m, \gcd(i,m) = 1, c \in \mathbb{F}_{2^n}, s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q, X^{2^i+1} + cX^{2^i} + c^qX + 1$ has no solution x s.t. $x^{q+1} = 1$	[9]
F4	$x^3 + a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a \neq 0$	[11]
F5	$x^3 + a^{-1}\mathrm{Tr}_3^n(a^3x^9 + a^6x^{18})$	$3 \mid n,\ a \neq 0$	[12]
F6	$x^3 + a^{-1}\mathrm{Tr}_3^n(a^6x^{18} + a^{12}x^{36})$	$3 \mid n, a \neq 0$	[12]
F7-F9	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k, \gcd(k,3) = \gcd(s,3k) = 1, v, w \in \mathbb{F}_{2^k}, vw \neq 1, 3 \mid (k+s), u$ primitive in $\mathbb{F}_{2^n}^*$	[7]
F10	$a^2x^{2^{2m+1}+1} + b^2x^{2^{m+1}+1} + ax^{2^{2m}+2} + bx^{2^m+2} + (c^2+c)x^3$	$n = 3m, m$ odd, $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$ satisfies the conditions of Lemma 8 of [8]	[8]
F11	$x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$	$n = 2m = 10$, $(a,b,c) = (\beta,1,0,0)$, $i = 3$, $k = 2$, β primitive in $\mathbb{F}_{2^2}$ $n = 2m$, m odd, $3 \nmid m$, $(a,b,c) = (\beta,\beta^2,1)$, β primitive in $\mathbb{F}_{2^2}$, $i \in \{m-2, m, 2m-1, (m-2)^{-1} \bmod n\}$	[13]
F12	$a\mathrm{Tr}_m^n(bx^{2^i+1}) + a^q\mathrm{Tr}_m^n(cx^{2^s+1})$	$n = 2m, m$ odd, $q = 2^m$, $a \notin \mathbb{F}_q$, $\gcd(i,n) = 1$, i, s, b, c satisfy the conditions of Theorem 2	[37]
F13	$L(z)^{2^m+1} + vz^{2^m+1}$	$\gcd(s,m) = 1, v \in \mathbb{F}_{2^m}^*, \mu \in \mathbb{F}_{2^{3m}}^*, L(z) = z^{2^{m+s}} + \mu z^{2^s} + z$ permutes $\mathbb{F}_{2^{3m}}$	[30]

ID	Functions	Conditions	Source
F14	$(xy, x^{2^k+1} + \alpha y^{(2^k+1)2^i})$	$\gcd(k,m) = 1$, m even, α not a cube	[38]
F15	$(xy, x^{2^{2m}+2^{3m}} + ax^{2^{2m}}y^{2^m} + by^{2^m+1})$	$x^{2^m+1} + ax + b$ has no root in $\mathbb{F}_{2^m}$	[34]
F16	$(xy, x^{2^i+1} + x^{2^{i+m/2}}y^{2^{m/2}} + bxy^{2^i} + cy^{2^i+1})$	$(cx^{2^i+1} + bx^{2^i} + 1)^{2^{m/2}+1} + x^{2^{m/2}+1}$ has no roots in $\mathbb{F}_{2^m}$	[15]
F17	$(x^{2^i+1} + xy^{2i} + y^{2^i+1}, x^{2^{2i}+1} + x^{2^{2i}}y + y^{2^{2i}+1})$	$\gcd(3i,m) = 1$	[26]
F18	$(x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{3i}}y + xy^{2^{3i}})$	$\gcd(3i,m) = 1$, m odd	[26]
F19	$(x^3 + xy^2 + y^3 + xy, x^5 + x^4y + y^5 + xy + x^2y^2)$	$\gcd(3,m) = 1$	[30]
F20	$(x^{q+1} + By^{q+1}, x^ry + \frac{a}{B}xy^r)$	$0 < k < m$, $q = 2^k$, $r = 2^{k+m/2}$, $m \equiv 2 \pmod 4$, $\gcd(k,m) = 1$, $a \in \mathbb{F}_{2^{m/2}}^*$, $B \in \mathbb{F}_{2^m}$, B not a cube, $B^{q+r} \neq a^{q+1}$	[27]
F21	$(x^{q+1} + xy^q + \alpha y^{q+1}, x^{q^2+1} + \alpha x^{q^2}y + (1+\alpha)^q xy^{q^2} + \alpha y^{q^2+1})$	$k, m > 0$, $\gcd(k,m) = 1$, $q = 2^k$, $\alpha \in \mathbb{F}_{2^m}$, $x^{q+1} + x + \alpha$ has no roots in $\mathbb{F}_{2^m}$	[16]
F22	$(x^3 + xy + xy^2 + \alpha y^3, x^5 + xy + \alpha x^2y^2 + \alpha x^4y + (1+\alpha)^2xy^4 + \alpha y^5)$	$\alpha \in \mathbb{F}_{2^m}$, $x^3 + x + \alpha$ has no roots in $\mathbb{F}_{2^m}$	[16]

Zoo of APN functions

ID	Functions	Conditions	Source
F1-F2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk, \gcd(k,3) = \gcd(s,3k) = 1, p \in$ [illegible]	[10]
F3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+$ [illegible] $c^q x^{2^i+q}$	[illegible] has no solution x s.t. [illegible]	[illegible]
F4	$x^3+a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a \neq 0$	[11]
F5	$x^3+a^{-1}\mathrm{Tr}_3^n(a^3x^9+a^6x^{18})$	$3 \mid n$, $a \neq 0$	[12]
F6	$x^3+a^{-1}\mathrm{Tr}_3^n(a^6x^{18}+a^{12}x^{36})$	$3 \mid n, a \neq 0$	[12]
F7-F9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k, \gcd(k,3) = \gcd(s,3k) = 1, v, w \in \mathbb{F}_{2^k}, vw \neq 1, 3 \mid (k+s), u$ primitive in $\mathbb{F}_{2^n}^*$	[7]
F10	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$	$n = 3m, m$ odd, $L(x) = ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions of Lemma 8 of [8]	[8]
F11	$x^3+a(x^{2^i+1})^{2^k}+bx^{3\cdot 2^m}+c(x^{2^{i+m}+2^m})^{2^k}$	$n = 2m = 10$, $(a,b,c) = (\beta,$ [illegible] $k = 2$, β primitive in $\mathbb{F}_{2^2}$ $n = 2m$, m odd, $3 \nmid m$, $(a,b,$ [illegible] β primitive in $\mathbb{F}_{2^2}$, $i \in \{m$ [illegible] $1, (m-2)^{-1} \mod n\}$	[illegible]
F12	$a\mathrm{Tr}_m^n(bx^{2^i+1})+a^q\mathrm{Tr}_m^n(cx^{2^s+1})$	$n = 2m, m$ odd, $q = 2^m, a \notin \mathbb{F}_q, \gcd(i,n) = 1, i, s, b, c$ satisfy the conditions of Theorem 2	[37]
F13	$L(z)^{2^m+1}+vz^{2^m+1}$	$\gcd(s,m) = 1, v \in \mathbb{F}_{2^m}^*, \mu \in \mathbb{F}_{2^{3m}}^*, L(z) = z^{2^{m+s}}+\mu z^{2^s}+z$ permutes $\mathbb{F}_{2^{3m}}$	[30]

ID	Functions	Conditions	Source
F14	$(xy, x^{2^k+1}+\alpha y^{(2^k+1)2^i})$	$\gcd(k,m) = 1$, m even, α not a cube	[38]
F15	$(xy, x^{2^{2m}+2^{3m}}+ax^{2^{2m}}y^{2^m}+by^{2^m+1})$	$x^{2^m+1}+ax+b$ has no root in $\mathbb{F}_{2^m}$	[34]
[illegible]	[illegible] $+$ [illegible] $+\, bxy^{2^i}+$ [illegible]	$(cx^{2^i+1}+bx^{2^i}+1)^{2^{m/2}+1}+x^{2^{m/2}+1}$ has no roots in $\mathbb{F}_{2^m}$	[15]
[illegible]	[illegible] $xy^{2i}+y^{2^i+1}, x^{2^{2i}+1}+x^{2^{2i}}y+y^{2^{2i}+1})$	$\gcd(3i,m) = 1$	[26]
F18	$(x^{2^i+1}+xy^{2^i}+y^{2^i+1}, x^{2^{3i}}y+xy^{2^{3i}})$	$\gcd(3i,m) = 1$, m odd	[26]
F19	$(x^3+xy^2+y^3+xy, x^5+x^4y+y^5+xy+x^2y^2)$	$\gcd(3,m) = 1$	[30]
F20	$(x^{q+1}+By^{q+1}, x^ry+$ [illegible]	$0 < k < m$, $q = 2^k$, $r = 2^{k+m/2}$, [illegible] $\gcd(k,m) = 1$, [illegible] B not a cube, [illegible]	[27]
[illegible]	[illegible] $(1+\alpha)^q xy^{q^2}+\alpha y^{q^2+1})$	[illegible] $= 1$, $q = 2^k$, [illegible] $+\, \alpha$ has no roots in $\mathbb{F}_{2^m}$	[16]
F22	$(x^3+xy+xy^2+\alpha y^3, x^5+xy+\alpha x^2y^2+\alpha x^4y+(1+\alpha)^2xy^4+\alpha y^5)$	$\alpha \in \mathbb{F}_{2^m}$, $x^3+x+\alpha$ has no roots in $\mathbb{F}_{2^m}$	[16]

Relationships between each others?

Is this classification that wide?

The (only ?) solution to the big APN problem

Big APN problem

Does there exist an APN bijection in even dimension ?

Known facts [Hou06]

An APN bijection for $n = 2t$

- does not exist for $n \in \{2, 4\}$
- cannot be quadratic

The (only ?) solution to the big APN problem

Big APN problem

Does there exist an APN bijection in even dimension ?

Known facts [Hou06]

An APN bijection for $n = 2t$

- does not exist for $n \in \{2, 4\}$
- cannot be quadratic

Kim mapping

$$\kappa : \begin{cases} \mathbb{F}_{2^6} & \to \mathbb{F}_{2^6} \\ x & \mapsto x^3 + x^{10} + ux^{24} \end{cases}$$

APN, quadratic, not bijective

The (only ?) solution to the big APN problem

Big APN problem

Does there exist an APN bijection in even dimension ?

Known facts [Hou06]

An APN bijection for $n = 2t$

- does not exist for $n \in \{2, 4\}$
- cannot be quadratic

Kim mapping

$$\kappa : \begin{cases} \mathbb{F}_{2^6} & \to \mathbb{F}_{2^6} \\ x & \mapsto x^3 + x^{10} + ux^{24} \end{cases}$$

APN, quadratic, not bijective

$\not\sim_{EA}$

The (only ?) solution to the big APN problem

Big APN problem

Does there exist an APN bijection in even dimension ?

Known facts [Hou06]

An APN bijection for $n = 2t$

- does not exist for $n \in \{2, 4\}$
- cannot be quadratic

Kim mapping

$$\kappa : \begin{cases} \mathbb{F}_{2^6} & \to \mathbb{F}_{2^6} \\ x & \mapsto x^3 + x^{10} + ux^{24} \end{cases}$$

APN, quadratic, not bijective

$\not\sim_{EA}$

$\sim_{CCZ}$

Dillon et al.'s permutation

$$P : \begin{cases} \mathbb{F}_{2^6} & \to \mathbb{F}_{2^6} \\ x & \mapsto P(x) \end{cases}$$

APN, not quadratic, bijective

[BDMW10]

Walsh transform

Walsh transform

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. $\alpha, \beta \in \mathbb{F}_{2^n}$.

$$\widehat{F}(\alpha, \beta) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\alpha \cdot x + \beta \cdot F(x)}$$

Walsh transform

Walsh transform

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. $\alpha, \beta \in \mathbb{F}_{2^n}$.

$$\widehat{F}(\alpha, \beta) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\alpha \cdot x + \beta \cdot F(x)}$$

Walsh transform and CCZ-equivalence

$F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

$$\mathcal{A} = \mathcal{L} + c \qquad \mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G \qquad \iff \qquad \widehat{G}(\alpha, \beta) = (-1)^{c \cdot (\alpha, \beta)} \widehat{F}(\mathcal{L}^\top(\alpha, \beta)) \quad \forall \alpha, \beta \in \mathbb{F}_{2^n}$$

A cryptanalytic point of view

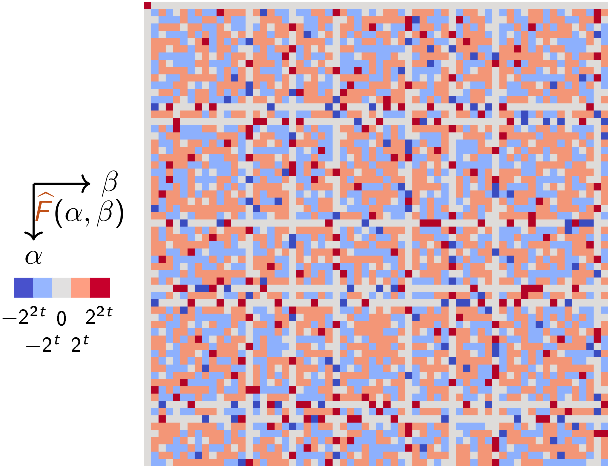
$F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ $\qquad \widehat{F}(\alpha, \beta) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\alpha \cdot x + \beta \cdot F(x)}$.

$\mathcal{A} = \mathcal{L} + c \qquad \mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G \qquad \iff \qquad \widehat{G}(\alpha, \beta) = (-1)^{c \cdot (\alpha, \beta)} \widehat{F}(\mathcal{L}^\top(\alpha, \beta)) \quad \forall \alpha, \beta \in \mathbb{F}_{2^n}$

A cryptanalytic point of view

$F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ $\qquad \widehat{F}(\alpha, \beta) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\alpha \cdot x + \beta \cdot F(x)}$.

$\mathcal{A} = \mathcal{L} + c \qquad \mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G \iff \widehat{G}(\alpha, \beta) = (-1)^{c \cdot (\alpha, \beta)} \widehat{F}(\mathcal{L}^\top(\alpha, \beta)) \quad \forall \alpha, \beta \in \mathbb{F}_{2^n}$

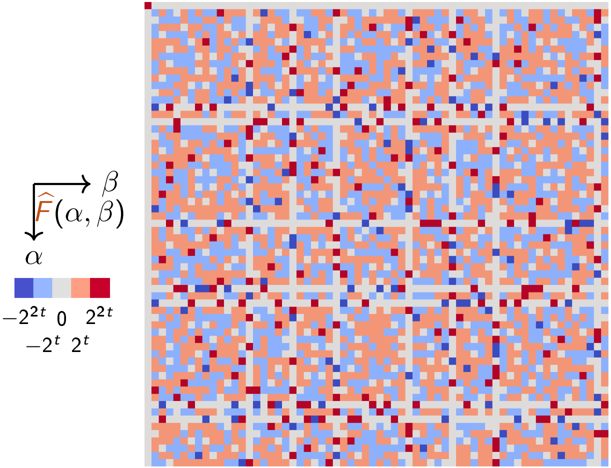


Dillon APN bijection

A cryptanalytic point of view

$F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ $\qquad \widehat{F}(\alpha, \beta) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\alpha \cdot x + \beta \cdot F(x)}$.

$\mathcal{A} = \mathcal{L} + c \qquad \mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G \iff \widehat{G}(\alpha, \beta) = (-1)^{c \cdot (\alpha, \beta)} \widehat{F}(\mathcal{L}^\top(\alpha, \beta)) \quad \forall \alpha, \beta \in \mathbb{F}_{2^n}$



Dillon APN bijection

$\widehat{F}(\{0\} \times \mathbb{F}_{2^n}^*) = \{0\}$.

$\widehat{F}(\mathbb{F}_{2^n}^* \times \{0\}) = \{0\}$.

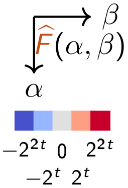
$\mathbb{F}_{2^n} \times \{0\} \bigcap \{0\} \times \mathbb{F}_{2^n} = \{0\}$

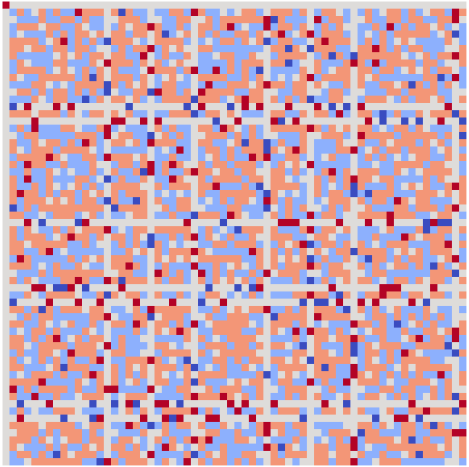
$\mathcal{L}^\top$ linear bijection.

A cryptanalytic point of view

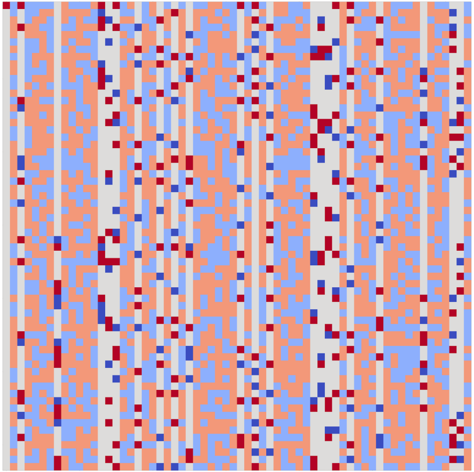
$F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ $\qquad \widehat{F}(\alpha, \beta) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\alpha \cdot x + \beta \cdot F(x)}$.

$\mathcal{A} = \mathcal{L} + c \qquad \mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G \qquad \iff \qquad \widehat{G}(\alpha, \beta) = (-1)^{c \cdot (\alpha, \beta)} \widehat{F}(\mathcal{L}^\top(\alpha, \beta)) \quad \forall \alpha, \beta \in \mathbb{F}_{2^n}$





Dillon APN bijection

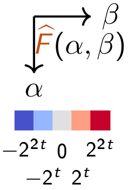


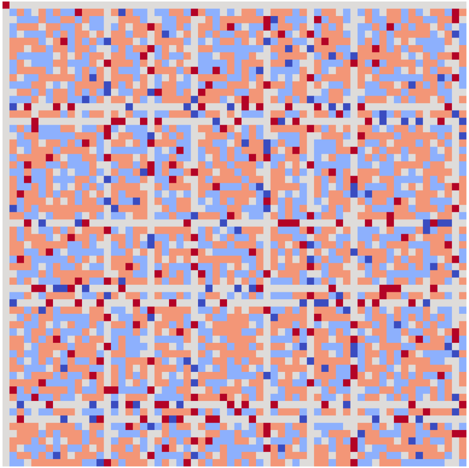
Kim mapping

A cryptanalytic point of view

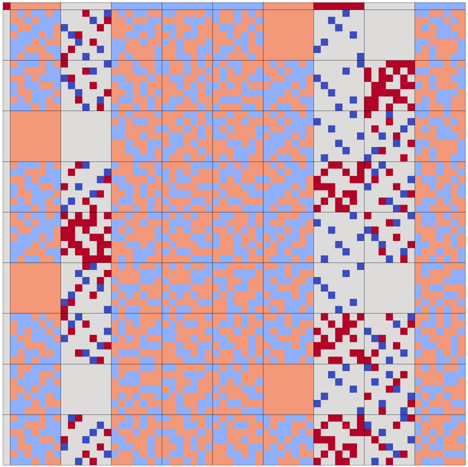
$F, G \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ $\qquad \widehat{F}(\alpha, \beta) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\alpha \cdot x + \beta \cdot F(x)}$.

$\mathcal{A} = \mathcal{L} + c \qquad \mathcal{A}(\mathcal{G}_F) = \mathcal{G}_G \quad \Longleftrightarrow \quad \widehat{G}(\alpha, \beta) = (-1)^{c \cdot (\alpha, \beta)} \widehat{F}(\mathcal{L}^\top(\alpha, \beta)) \quad \forall \alpha, \beta \in \mathbb{F}_{2^n}$





Dillon APN bijection



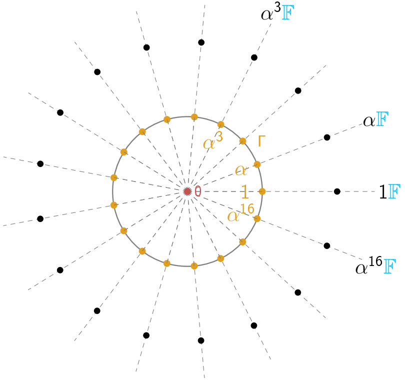
Kim mapping

Cosets of a subfield

Partition into cosets

- $\mathbb{F} \subset \mathbb{L}$ finite fields of characteristic 2.
- $\mathbb{F}^*$ multiplicative subgroup of $\mathbb{L}^* \implies \mathbb{L}^* = \bigsqcup_{\gamma \in \Gamma} \gamma\mathbb{F}^*$

Any $\lambda \in \mathbb{L}^*$ can be uniquely written as $\lambda = \gamma\varphi$ with $\gamma \in \Gamma, \varphi \in \mathbb{F}^*$.



The enigmatic Kim function

$\mathbb{L} = \mathbb{F}_{2^6}, \mathbb{F} = \mathbb{F}_{2^3}$ $\lambda \in \mathbb{L}, \varphi \in \mathbb{F}, \gamma \in \Gamma.$

Kim mapping [BDMW10]

$$\kappa : \begin{array}{ccc} \mathbb{L} & \to & \mathbb{L} \\ \lambda & \mapsto & \lambda^3 + \lambda^{10} + u\lambda^{24}; \end{array}$$

for a specific $u \in \mathbb{L}$.

The enigmatic Kim function

$\mathbb{L} = \mathbb{F}_{2^6}, \mathbb{F} = \mathbb{F}_{2^3}$ $\lambda \in \mathbb{L}, \varphi \in \mathbb{F}, \gamma \in \Gamma.$

Kim mapping [BDMW10]

$$\kappa : \begin{array}{ccc} \mathbb{L} & \to & \mathbb{L} \\ \lambda & \mapsto & \lambda^3 + \lambda^{10} + u\lambda^{24}; \end{array}$$

for a specific $u \in \mathbb{L}$.

Key observation [BDMW10]

$\varphi \in \mathbb{F}, \lambda \in \mathbb{L}$

$$\kappa(\varphi\lambda) = (\varphi\lambda)^3 + (\varphi\lambda)^{10} + u(\varphi\lambda)^{24} = \varphi^3\kappa(\lambda)$$

because $3 \equiv 10 \equiv 24 \mod 7$ and $|\mathbb{F}^*| = 7$.

Cyclotomic mappings

$\kappa\colon \lambda \mapsto \lambda^3 + \lambda^{10} + u\lambda^{24}.$ $\quad \kappa(\varphi\lambda) = \varphi^3\kappa(\lambda) \quad \forall \varphi \in \mathbb{F}, \lambda \in \mathbb{L}.$

Cyclotomic mappings

$\kappa : \lambda \mapsto \lambda^3 + \lambda^{10} + u\lambda^{24}$. $\kappa(\varphi\lambda) = \varphi^3\kappa(\lambda) \quad \forall \varphi \in \mathbb{F}, \lambda \in \mathbb{L}$.

Cyclotomic mapping [Wang07]

$\mathbb{G} \subset \mathbb{L}^*$ a subgroup. $F : \mathbb{L} \to \mathbb{L}$ is a cyclotomic mapping of order d over $\mathbb{G}$ if:

$$\forall\ \lambda \in \mathbb{L}, \forall\ \varphi \in \mathbb{G}, \quad F(\varphi\lambda) = \varphi^d F(\lambda).$$

Here: $\mathbb{G} = \mathbb{F}^*$

Cyclotomic mappings

$\kappa : \lambda \mapsto \lambda^3 + \lambda^{10} + u\lambda^{24}$. $\kappa(\varphi\lambda) = \varphi^3\kappa(\lambda) \quad \forall \varphi \in \mathbb{F}, \lambda \in \mathbb{L}$.

Cyclotomic mapping [Wang07]

$\mathbb{G} \subset \mathbb{L}^*$ a subgroup. $F : \mathbb{L} \to \mathbb{L}$ is a cyclotomic mapping of order d over $\mathbb{G}$ if:

$$\forall\ \lambda \in \mathbb{L}, \forall\ \varphi \in \mathbb{G}, \quad F(\varphi\lambda) = \varphi^d F(\lambda).$$

Here: $\mathbb{G} = \mathbb{F}^*$

Polynomial characterization

$F : \lambda \mapsto \sum_{i=0}^{2^n-1} a_i\lambda^i$ is a cyclotomic mapping of order d over $\mathbb{G}$ iff $a_i \neq 0 \implies i \equiv d \bmod |\mathbb{G}|$.

Cyclotomic mappings

$\kappa : \lambda \mapsto \lambda^3 + \lambda^{10} + u\lambda^{24}.$ $\qquad \kappa(\varphi\lambda) = \varphi^3\kappa(\lambda) \quad \forall \varphi \in \mathbb{F}, \lambda \in \mathbb{L}.$

Cyclotomic mapping [Wang07]

$\mathbb{G} \subset \mathbb{L}^*$ a subgroup. $F : \mathbb{L} \to \mathbb{L}$ is a cyclotomic mapping of order d over $\mathbb{G}$ if:

$$\forall\, \lambda \in \mathbb{L}, \forall\, \varphi \in \mathbb{G}, \quad F(\varphi\lambda) = \varphi^d F(\lambda).$$

Here: $\mathbb{G} = \mathbb{F}^*$

Polynomial characterization

$F : \lambda \mapsto \sum_{i=0}^{2^n-1} a_i\lambda^i$ is a cyclotomic mapping of order d over $\mathbb{G}$ iff $a_i \neq 0 \implies i \equiv d \bmod |\mathbb{G}|$.

- Also known as Wan Lidl polynomials [WanLidl91]
- Studies about graphs or permutations [AkbWan07, BorPanWan23, Laigle-Chapuy07]
- only a few about cryptographic properties [ChenCoulter23, Gologlu23, BeiBriLea21]

Properties of the Kim mapping (1/2)

$\kappa : \lambda \mapsto \lambda^3 + \lambda^{10} + u\lambda^{24}$ is a cyclotomic mapping over $\mathbb{F}_{2^3}$ of order 3

Immediate corollary

F cyclotomic $\implies F(\lambda\mathbb{F}) \subset F(\lambda)\mathbb{F}$

Properties of the Kim mapping (1/2)

$\kappa : \lambda \mapsto \lambda^3 + \lambda^{10} + u\lambda^{24}$ is a cyclotomic mapping over $\mathbb{F}_{2^3}$ of order 3

Immediate corollary

F cyclotomic $\implies F(\lambda\mathbb{F}) \subset F(\lambda)\mathbb{F}$

The Kim mapping case

$\varphi \mapsto \varphi^3$ is a bijection over $\mathbb{F}_{2^3}$ $\implies F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$.

Properties of the Kim mapping (1/2)

$\kappa : \lambda \mapsto \lambda^3 + \lambda^{10} + u\lambda^{24}$ is a cyclotomic mapping over $\mathbb{F}_{2^3}$ of order 3

Immediate corollary

F cyclotomic $\implies F(\lambda\mathbb{F}) \subset F(\lambda)\mathbb{F}$

The Kim mapping case

$\varphi \mapsto \varphi^3$ is a bijection over $\mathbb{F}_{2^3}$ $\implies F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$.

The subspace property [BDMW10]

$F : \mathbb{L} \to \mathbb{L}$ satisfies the $\mathbb{F}$-subspace property if:

$$F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F} \quad \forall\, \lambda \in \mathbb{L}.$$

$F(\varphi\lambda) = F(\lambda)G_\lambda(\varphi)$ where $G_\lambda : \mathbb{F} \to \mathbb{F}$ is bijective.

Properties of the Kim mapping (2/2)

Subspace prop: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$

Cyclotomic: $\exists\ d, \forall\ \lambda, \forall\ \varphi, \quad F(\varphi\lambda) = F(\lambda)\varphi^{d}$

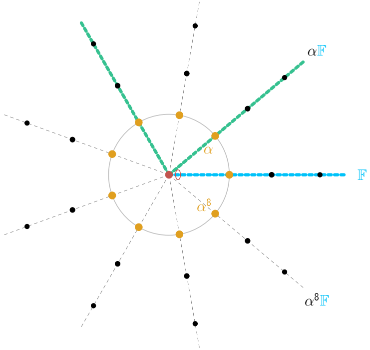
$\kappa(\lambda) = \lambda^{3} + \lambda^{10} + u\lambda^{24}.$

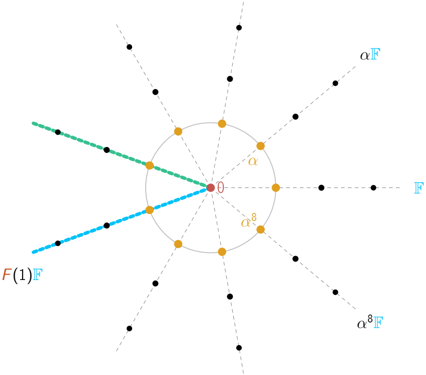
Properties of the Kim mapping (2/2)

Subspace prop: $\forall\ \lambda,\quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$

Cyclotomic: $\exists\ d, \forall\ \lambda, \forall\ \varphi,\quad F(\varphi\lambda) = F(\lambda)\varphi^d$

$\kappa(\lambda) = \lambda^3 + \lambda^{10} + u\lambda^{24}.$



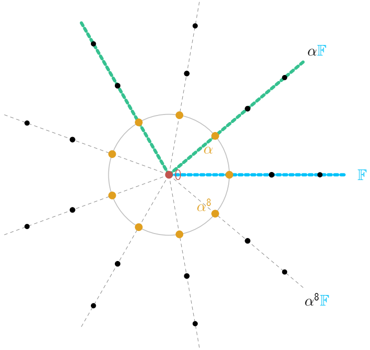


Properties of the Kim mapping (2/2)

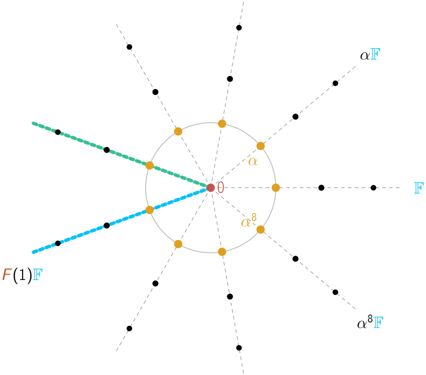
Subspace prop: $\forall\ \lambda,\quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$

Cyclotomic: $\exists\ d, \forall\ \lambda, \forall\ \varphi,\quad F(\varphi\lambda) = F(\lambda)\varphi^d$

$\kappa(\lambda) = \lambda^3 + \lambda^{10} + u\lambda^{24}.$



Not bijective

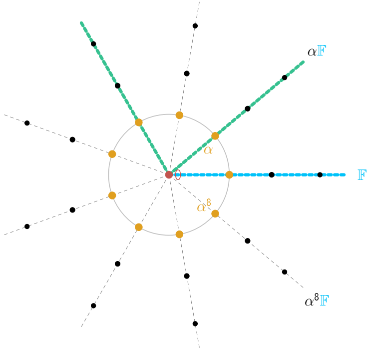


Properties of the Kim mapping (2/2)

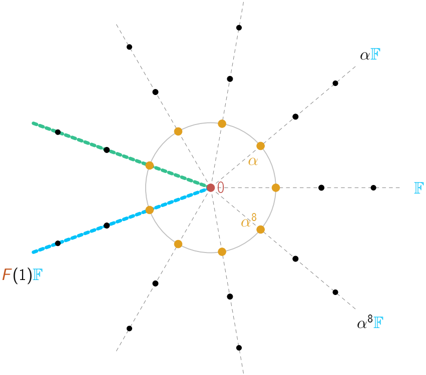
Subspace prop: $\forall\ \lambda,\quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$

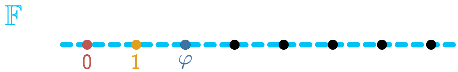
Cyclotomic: $\exists\ d, \forall\ \lambda, \forall\ \varphi,\quad F(\varphi\lambda) = F(\lambda)\varphi^d$

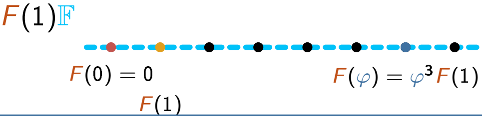
$\kappa(\lambda) = \lambda^3 + \lambda^{10} + u\lambda^{24}$.



Not bijective





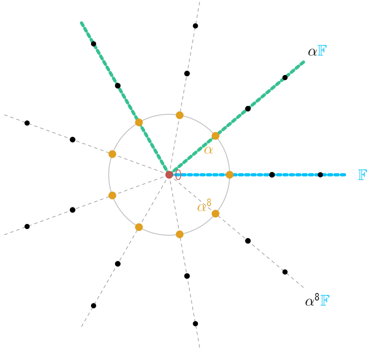


Properties of the Kim mapping (2/2)

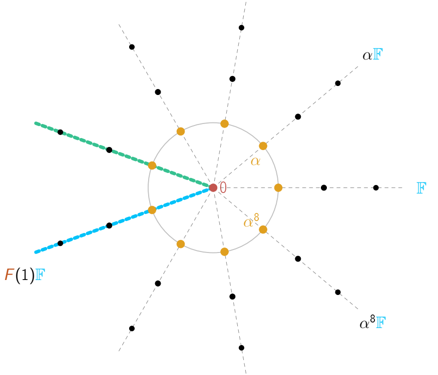
Subspace prop: $\forall\ \lambda$, $F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$

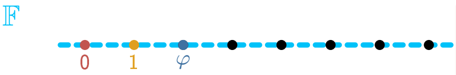
Cyclotomic: $\exists\ d, \forall\ \lambda, \forall\ \varphi$, $F(\varphi\lambda) = F(\lambda)\varphi^d$

$\kappa(\lambda) = \lambda^3 + \lambda^{10} + u\lambda^{24}$.

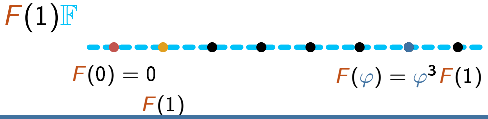


Not bijective





Bijective, monomial

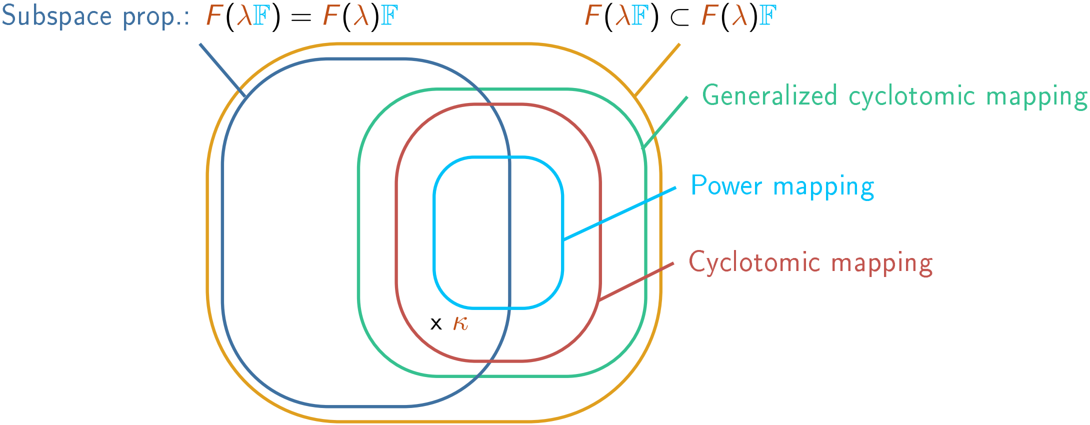


Subspace property and Cyclotomy

Subspace prop: $\forall\ \lambda,\qquad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$

Cyclotomic: $\exists\ d, \forall\ \lambda, \forall\ \varphi,\qquad F(\varphi\lambda) = \varphi^{d} F(\lambda)$

Gen. cyclotomic: $\forall\ \lambda, \exists\ d_\lambda, \forall\ \varphi,\qquad F(\varphi\lambda) = \varphi^{d_\lambda} F(\lambda)$



Spectral point of view (1/2)

Subspace prop: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}.$ $\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$$\widehat{F}(\alpha, \beta) := \sum_{\lambda \in \mathbb{L}} (-1)^{\alpha\cdot\lambda + \beta\cdot F(\lambda)}$$

Spectral point of view (1/2)

Subspace prop: $\forall \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$. $\quad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$$\widehat{F}(\alpha, \beta) := \sum_{\lambda \in \mathbb{L}} (-1)^{\alpha\cdot\lambda + \beta\cdot F(\lambda)}$$

Decomposition of Walsh coefficients

Γ system of representatives, $\alpha, \beta \in \mathbb{L}$. $F : \mathbb{L} \to \mathbb{L}$ satisfying the $\mathbb{F}$-subspace property. Then:

$$\widehat{F}(\alpha, \beta) = C + \sum_{\gamma \in \Gamma} \widehat{G}_\lambda \left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\alpha\gamma), \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\beta F(\gamma))\right).$$

Spectral point of view (1/2)

Subspace prop: $\forall\ \lambda, \quad F(\lambda \mathbb{F}) = F(\lambda)\mathbb{F}$. $\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$\widehat{F}(\alpha, \beta) := \sum_{\lambda \in \mathbb{L}} (-1)^{\alpha\cdot\lambda + \beta\cdot F(\lambda)}$

Decomposition of Walsh coefficients

Γ system of representatives, $\alpha, \beta \in \mathbb{L}$. $F : \mathbb{L} \to \mathbb{L}$ satisfying the $\mathbb{F}$-subspace property. Then:

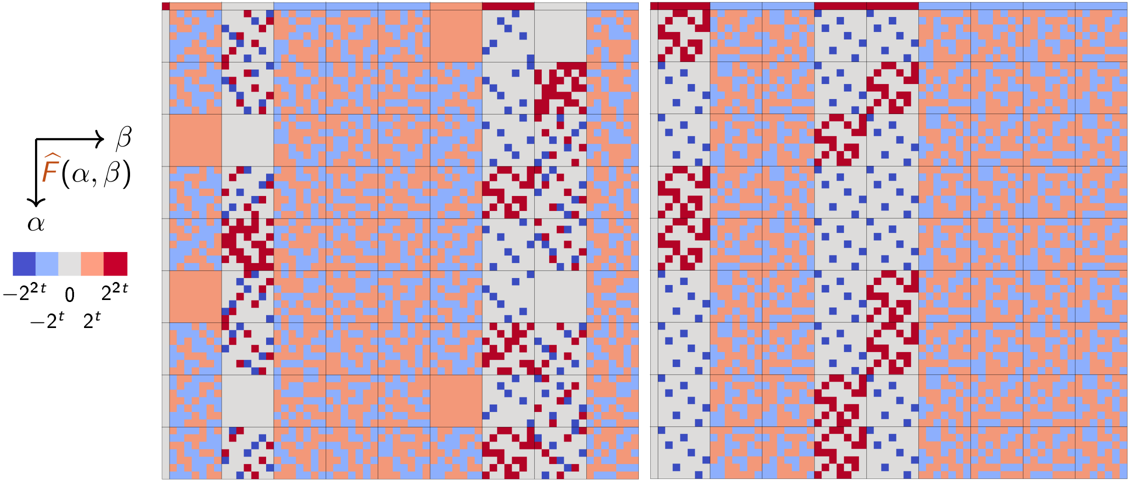
$$\widehat{F}(\alpha, \beta) = C + \sum_{\gamma \in \Gamma} \widehat{G_\lambda}\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\alpha\gamma), \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\beta F(\gamma))\right).$$

Symmetries of Walsh coefficients

Let $G : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$. F satisfies the subspace property with $G_\lambda = G\ \forall\ \lambda$ if and only if:

$$\forall \alpha, \beta \in \mathbb{L},\ \forall \varphi \in \mathbb{F}^*, \quad \widehat{F}(\alpha, \beta G(\varphi)) = \widehat{F}(\alpha\varphi^{-1}, \beta).$$

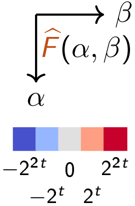
Spectral point of view (2/2)

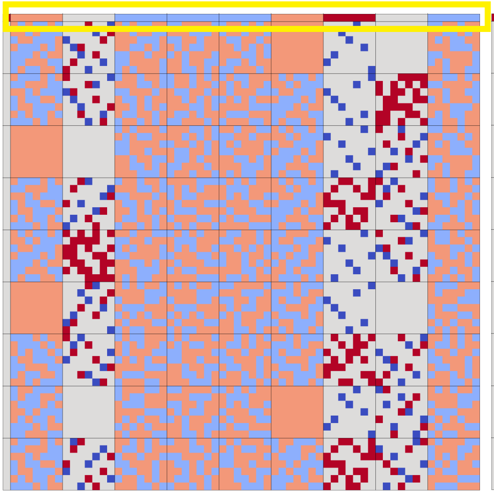


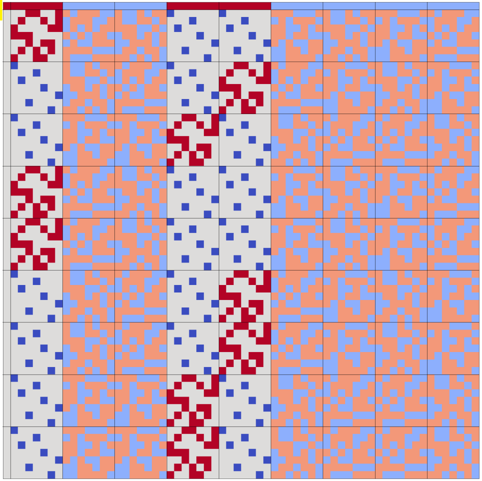
Kim mapping $\kappa\colon \lambda \mapsto \lambda^3 + \lambda^{10} + u\lambda^{24}$

Cube over $\mathbb{F}_{64}$ $\lambda \mapsto \lambda^3$

Spectral point of view (2/2)







Kim mapping $\kappa\colon \lambda \mapsto \lambda^3 + \lambda^{10} + u\lambda^{24}$

Cube over $\mathbb{F}_{64}$ $\lambda \mapsto \lambda^3$

Walsh coefficients $\widehat{F}(0, \beta)$

Subspace prop: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$. $\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$$\widehat{F}(\alpha, \beta) := \sum_{\lambda \in \mathbb{L}} (-1)^{\alpha\cdot\lambda + \beta\cdot F(\lambda)} \qquad N_\lambda := \frac{\left|F^{-1}(\lambda\mathbb{F})\right|}{|\mathbb{F}|}$$

Walsh coefficients $\widehat{F}(0, \beta)$

Subspace prop: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$. $\quad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$$\widehat{F}(\alpha, \beta) := \sum_{\lambda \in \mathbb{L}} (-1)^{\alpha\cdot\lambda + \beta\cdot F(\lambda)} \qquad N_\lambda := \frac{\left|F^{-1}(\lambda\mathbb{F})\right|}{|\mathbb{F}|}$$

Walsh coefficients in zero

F satisfying the subspace property. $[\mathbb{L} : \mathbb{F}] = 2$. Then

$$\forall\ \beta \in \mathbb{L}^*, \quad \widehat{F}(0, \beta) = 2^t(N_{\beta^{-1}} - 1)$$

Walsh coefficients $\widehat{F}(0, \beta)$

Subspace prop: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$. $\quad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

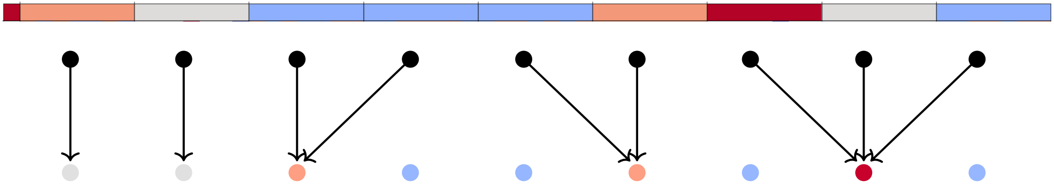
$$\widehat{F}(\alpha, \beta) := \sum_{\lambda \in \mathbb{L}} (-1)^{\alpha\cdot\lambda + \beta\cdot F(\lambda)} \qquad N_\lambda := \frac{\left|F^{-1}(\lambda\mathbb{F})\right|}{|\mathbb{F}|}$$

Walsh coefficients in zero

F satisfying the subspace property. $[\mathbb{L} : \mathbb{F}] = 2$. Then

$$\forall\ \beta \in \mathbb{L}^*, \quad \widehat{F}(0, \beta) = 2^t(N_{\beta^{-1}} - 1)$$

Kim mapping



Walsh coefficients $\widehat{F}(0, \beta)$

Subspace prop: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}.$ $\quad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

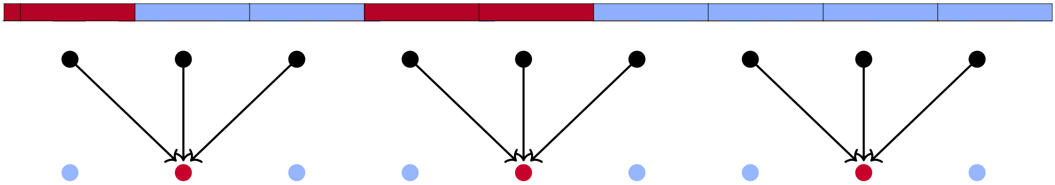
$$\widehat{F}(\alpha, \beta) := \sum_{\lambda \in \mathbb{L}} (-1)^{\alpha\cdot\lambda + \beta\cdot F(\lambda)} \qquad N_\lambda := \frac{\left|F^{-1}(\lambda\mathbb{F})\right|}{|\mathbb{F}|}$$

Walsh coefficients in zero

F satisfying the subspace property. $[\mathbb{L} : \mathbb{F}] = 2$. Then

$$\forall\ \beta \in \mathbb{L}^*, \quad \widehat{F}(0, \beta) = 2^t(N_{\beta^{-1}} - 1)$$

Cube



Subspace property and APNness

Subspace prop: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$. $\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$N_\lambda := \frac{\left|F^{-1}(\lambda\mathbb{F})\right|}{|\mathbb{F}|} \qquad \mathcal{N}_i := \{\gamma \in \Gamma, N_\gamma = i\}$

Subspace prop. when $\mathbb{L} = \mathbb{F}_{2^{2t}}, \mathbb{F} = \mathbb{F}_{2^t} \implies \quad \widehat{F}(0,\beta) = 2^t(N_{\beta^{-1}} - 1)$

Subspace property and APNness

Subspace prop: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$. $\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$N_\lambda := \frac{|F^{-1}(\lambda\mathbb{F})|}{|\mathbb{F}|} \qquad \mathcal{N}_i := \{\gamma \in \Gamma, N_\gamma = i\}$

Subspace prop. when $\mathbb{L} = \mathbb{F}_{2^{2t}}, \mathbb{F} = \mathbb{F}_{2^t} \implies \widehat{F}(0, \beta) = 2^t(N_{\beta^{-1}} - 1)$

Necessary condition to be APN

F quadratic satisfying the subspace property. $[\mathbb{L} : \mathbb{F}] = 2$.

- If F is APN then $\mathcal{N}_0 + \mathcal{N}_2 \geq \frac{2(2^t+1)}{3}$
- If $\mathcal{L}(F) = 2^{t+1}$ and $\mathcal{N}_0 + \mathcal{N}_2 \geq \frac{2(2^t+1)}{3}$ then F is APN.

Proof: [BerCanChaLai06]

Subspace property and APNness

Subspace prop: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}. \qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$N_\lambda := \frac{|F^{-1}(\lambda\mathbb{F})|}{|\mathbb{F}|} \qquad \mathcal{N}_i := \{\gamma \in \Gamma, N_\gamma = i\}$

Subspace prop. when $\mathbb{L} = \mathbb{F}_{2^{2t}}, \mathbb{F} = \mathbb{F}_{2^t} \implies \widehat{F}(0,\beta) = 2^t(N_{\beta^{-1}} - 1)$

Necessary condition to be APN

F quadratic satisfying the subspace property. $[\mathbb{L} : \mathbb{F}] = 2$.

- If F is APN then $\mathcal{N}_0 + \mathcal{N}_2 \geq \frac{2(2^t+1)}{3}$
- If $\mathcal{L}(F) = 2^{t+1}$ and $\mathcal{N}_0 + \mathcal{N}_2 \geq \frac{2(2^t+1)}{3}$ then F is APN.

Proof: [BerCanChaLai06]

One already-solved case [Gologlu2023, ChaLis21]

F quadratic cyclotomic when $[\mathbb{L} : \mathbb{F}] = 2$.

- If $t \neq 3$: $\quad F$ APN $\iff F \sim_{CCZ}$ Gold power
- If $t = 3$: $\quad F$ APN $\iff F \sim_{CCZ}$ Gold power or $F \sim_{CCZ} \kappa$.

Cyclotomic mappings among the zoo of APN functions

$F:\lambda \mapsto \sum_{i=0}^{2^n-1} a_i\lambda^i$ is cyclotomic of order d over $\mathbb{G}$ iff $a_i \neq 0 \implies i \equiv d \bmod |\mathbb{G}|$

ID	Functions	Conditions	Source
F1-F2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk, \gcd(k,3)=\gcd(s,3k)=1, p\in\{3,4\}, i=sk \bmod p, m=p-i, n\geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$	[10]
F3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+cx^{2^iq+1}+c^qx^{2^i+q}$	$q=2^m, n=2m, \gcd(i,m)=1, c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q, X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$	[9]
F4	$x^3+a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a\neq 0$	[11]
F5	$x^3+a^{-1}\mathrm{Tr}_3^n(a^3x^9+a^6x^{18})$	$3\mid n,\ a\neq 0$	[12]
F6	$x^3+a^{-1}\mathrm{Tr}_3^n(a^6x^{18}+a^{12}x^{36})$	$3\mid n, a\neq 0$	[12]
F7-F9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k, \gcd(k,3)=\gcd(s,3k)=1, v,w\in\mathbb{F}_{2^k}, vw\neq 1, 3\mid(k+s), u$ primitive in $\mathbb{F}_{2^n}^*$	[7]
F10	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$	$n=3m, m$ odd, $L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions of Lemma 8 of [8]	[8]
F11	$x^3+a(x^{2^i+1})^{2^k}+bx^{3\cdot 2^m}+c(x^{2^{i+m}+2^m})^{2^k}$	$n=2m=10,\ (a,b,c)=(\beta,1,0,0),\ i=3,\ k=2,\ \beta$ primitive in $\mathbb{F}_{2^2}$ $n=2m,\ m$ odd, $3\nmid m,\ (a,b,c)=(\beta,\beta^2,1),\ \beta$ primitive in $\mathbb{F}_{2^2},\ i\in\{m-2,m,2m-1,(m-2)^{-1} \bmod n\}$	[13]
F12	$a\mathrm{Tr}_m^n(bx^{2^i+1})+a^q\mathrm{Tr}_m^n(cx^{2^s+1})$	$n=2m, m$ odd, $q=2^m, a\notin\mathbb{F}_q, \gcd(i,n)=1, i,s,b,c$ satisfy the conditions of Theorem 2	[37]
F13	$L(z)^{2^m+1}+vz^{2^m+1}$	$\gcd(s,m)=1, v\in\mathbb{F}_{2^m}^*, \mu\in\mathbb{F}_{2^{3m}}^*, L(z)=z^{2^{m+s}}+\mu z^{2^s}+z$ permutes $\mathbb{F}_{2^{3m}}$	[30]

ID	Functions	Conditions	Source
F14	$(xy, x^{2^k+1}+\alpha y^{(2^k+1)2^i})$	$\gcd(k,m)=1$, m even, α not a cube	[38]
F15	$(xy, x^{2^{2m}+2^{3m}}+ax^{2^{2m}}y^{2^m}+by^{2^m+1})$	$x^{2^m+1}+ax+b$ has no root in $\mathbb{F}_{2^m}$	[34]
F16	$(xy, x^{2^i+1}+x^{2^{i+m/2}}y^{2^{m/2}}+bxy^{2^i}+cy^{2^i+1})$	$(cx^{2^i+1}+bx^{2^i}+1)^{2^{m/2}+1}+x^{2^{m/2}+1}$ has no roots in $\mathbb{F}_{2^m}$	[15]
F17	$(x^{2^i+1}+xy^{2i}+y^{2^i+1}, x^{2^{2i}+1}+x^{2^{2i}}y+y^{2^{2i}+1})$	$\gcd(3i,m)=1$	[26]
F18	$(x^{2^i+1}+xy^{2^i}+y^{2^i+1}, x^{2^{3i}}y+xy^{2^{3i}})$	$\gcd(3i,m)=1$, m odd	[26]
F19	$(x^3+xy^2+y^3+xy, x^5+x^4y+y^5+xy+x^2y^2)$	$\gcd(3,m)=1$	[30]
F20	$(x^{q+1}+By^{q+1}, x^ry+\frac{a}{B}xy^r)$	$0<k<m$, $q=2^k$, $r=2^{k+m/2}$, $m\equiv 2 \pmod 4$, $\gcd(k,m)=1$, $a\in\mathbb{F}_{2^{m/2}}^*$, $B\in\mathbb{F}_{2^m}$, B not a cube, $B^{q+r}\neq a^{q+1}$	[27]
F21	$(x^{q+1}+xy^q+\alpha y^{q+1}, x^{q^2+1}+\alpha x^{q^2}y+(1+\alpha)^qxy^{q^2}+\alpha y^{q^2+1})$	$k,m>0$, $\gcd(k,m)=1$, $q=2^k$, $\alpha\in\mathbb{F}_{2^m}$, $x^{q+1}+x+\alpha$ has no roots in $\mathbb{F}_{2^m}$	[16]
F22	$(x^3+xy+xy^2+\alpha y^3, x^5+xy+\alpha x^2y^2+\alpha x^4y+(1+\alpha)^2xy^4+\alpha y^5)$	$\alpha\in\mathbb{F}_{2^m}$, $x^3+x+\alpha$ has no roots in $\mathbb{F}_{2^m}$	[16]

Cyclotomic mappings among the zoo of APN functions

[LiKaleyski23]

Let $\gcd(m, 7) = 1$,

$$F(x, y, z) = \left(x^3 + x^2 z + y z^2, x^2 z + y^3, x y^2 + y^2 z + z^3\right).$$

Conclusion

Cyclotomic mappings and APNness

- Natural generalization of monomials
- WANTED : more necessary conditions to be APN (in the quadratic case).

"Pen and paper" APN functions

- A lot of them are cyclotomic mappings $\rightsquigarrow$ is the zoo that broad after all ?
- PROBLEM : geometrical structure not CCZ-invariant
- Some ideas to detect it. But can we prove it ?

Computer search

- Most of the APN functions found are not cyclotomic (at first sight)
- Cyclotomic (with more conditions) seems a good search heuristic !

Thanks ! ☺