Linear self-equivalence : a unifying point-of-view on the known families of APN functions

Jules Baudrin

based on a joint work with Anne Canteaut & Léo Perrin

UCLouvain

Journées Codage & Cryptographie, April 3rd, 2025

Contact: jules.baudrin@uclouvain.be

Linear self-equivalence : a unifying PoV on the known families of APN functions

Univariate
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$
$L(x)^{2^k+1} + bx^{2^k+1}$

Multivariate
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{2s}+1} + x^{2^{2s}}y + y^{2^{2s}+1} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{3s}}y + xy^{2^{3s}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$

Linear self-equivalence : a unifying PoV on the known families of APN functions

Univariate
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx$ …
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}($ …
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9$ … $)$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$
$L(x)^{2^k+1} + bx^{2^k+1}$

Multivariate
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
… $+1 + xy^{2^s} + y^{2^s+1}$; … $+1 + x^{2^{2s}}y + y^{2^{2s}+1}$
$(x,y) \mapsto \begin{pmatrix} \ldots +1 + xy^{2^s} + y^{2^s+1} \\ x^{2^{3s}}y + xy^{2^{3s}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$

Hopefully clearer in 20 min ?

Outline

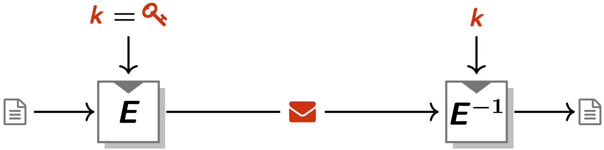
- From Differential cryptanalysis to APN functions
- Polynomial representations of vectorial Boolean functions
- APN state of the art
- Our unified point of view on the known APN functions

Security of block ciphers

Block cipher

A family of bijections $\mathcal{E}$ of $\mathbb{F}_2^n$.

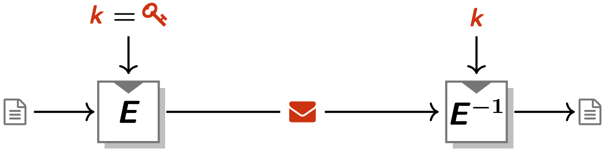
$$\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa}$$



Block cipher

A family of bijections $\mathcal{E}$ of $\mathbb{F}_2^n$.

$$\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa}$$



Ideal block cipher

A *random* family of bijections.

In practice, $\mathcal{E}$ should be *indistinguishable* from a random family of bijections

- to satisfy assumptions of security proofs
- to avoid stronger attack (*e.g.* key recoveries)

Differential cryptanalysis

$F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$.

Principle

Studies for each input difference $\Delta^{\text{in}} \neq 0$, the ***distribution of output differences***:

$$\forall \Delta^{\text{out}} \in \mathbb{F}_2^n, \quad \mathbb{P}_{x \xleftarrow{\$} \mathbb{F}_2^n} \left[F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}} \right] = ?$$

Differential cryptanalysis

$F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$.

Principle

Studies for each input difference $\Delta^{\text{in}} \neq 0$, the *distribution of output differences*:

$$\forall \Delta^{\text{out}} \in \mathbb{F}_2^n, \quad \mathbb{P}_{x \xleftarrow{\$} \mathbb{F}_2^n} \left[F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}} \right] = ?$$

$$x \overset{\Delta^{\text{in}}}{\longleftrightarrow} y \qquad\qquad F(x) \overset{\Delta^{\text{out}}}{\longleftrightarrow} F(y)$$

Average over all bijections

For all $(\Delta^{\text{in}} \neq 0, \Delta^{\text{out}})$, the equation $F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}$ has 1 solution x *on average*.

Differential cryptanalysis

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

Principle

Studies for each input difference $\Delta^{\text{in}} \neq 0$, the *distribution of output differences*:

$$\forall \Delta^{\text{out}} \in \mathbb{F}_2^n, \quad \mathbb{P}_{x \xleftarrow{\$} \mathbb{F}_2^n}\left[F(x+\Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}\right] = ?$$

Average over all bijections

For all $(\Delta^{\text{in}} \neq 0, \Delta^{\text{out}})$, the equation $F(x+\Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}$ has 1 solution x *on average*.

Differential distinguisher

[BihSha91]

$(\Delta^{\text{in}}, \Delta^{\text{out}})$ such that for many k, $\quad E_k(x+\Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has many solutions x.

Resisting against differential attacks

Differential distinguisher [BihSha91]

$(\Delta^{\text{in}}, \Delta^{\text{out}})$ s.t for many k, $E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has many solutions x.

Resisting against differential attacks

Differential distinguisher [BihSha91]

$(\Delta^{\text{in}}, \Delta^{\text{out}})$ s.t for many k, $\quad E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has many solutions x.

Differential resistance

For all $(\Delta^{\text{in}}, \Delta^{\text{out}})$ and all keys k, $\quad E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has *few* solutions.

Resisting against differential attacks

Differential distinguisher [BihSha91]

$(\Delta^{\text{in}}, \Delta^{\text{out}})$ s.t for many k, $E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has many solutions x.

Differential resistance

For all $(\Delta^{\text{in}}, \Delta^{\text{out}})$ and all keys k, $E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has *few* solutions.

How to achieve this

For all $(\Delta^{\text{in}}, \Delta^{\text{out}})$, $S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}$ has *few* solutions.

Resisting against differential attacks

Differential distinguisher

[BihSha91]

$(\Delta^{\text{in}}, \Delta^{\text{out}})$ s.t for many k, $\quad E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has many solutions x.

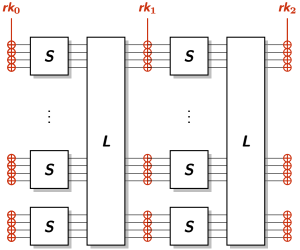
Differential resistance

For all $(\Delta^{\text{in}}, \Delta^{\text{out}})$ and all keys k, $\quad E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has *few* solutions.

How to achieve this

For all $(\Delta^{\text{in}}, \Delta^{\text{out}})$, $\quad S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}$ has *few* solutions.

$$\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) = \left|\{x \mid S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\}\right|$$



$$\mathbb{P}[\Delta^{\text{in}}, \Delta, \Delta^{\text{out}}] \leq \left(\frac{\max_{a \neq 0, b} \delta_S(a,b)}{2^m}\right)^{d(L)}$$

Differentially-optimal functions

How to achieve this

For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ $\quad \delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) = \left|\{x \mid S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\}\right|$ should be *low*.

Differentially-optimal functions

How to achieve this

For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ $\quad \delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) = \left|\{x \mid S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\}\right|$ should be *low*.

- For all Δ^{in}, there exists Δ^{out} such that $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) > 0$

Differentially-optimal functions

How to achieve this

For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ $\quad \delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) = \left|\{x \mid S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\}\right|$ should be *low*.

- For all Δ^{in}, there exists Δ^{out} such that $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) > 0$
- For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$, x is a solution iff $x + \Delta^{\text{in}}$ is a solution. $\quad \delta_S(\Delta^{\text{in}}, \Delta^{\text{out}})$ is even.

Differentially-optimal functions

How to achieve this

For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ $\quad \delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) = \left|\{x \mid S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\}\right|$ should be *low*.

- For all Δ^{in}, there exists Δ^{out} such that $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) > 0$
- For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$, x is a solution iff $x + \Delta^{\text{in}}$ is a solution. $\qquad \delta_S(\Delta^{\text{in}}, \Delta^{\text{out}})$ is even.

Almost perfect non-linear (APN) function [NybKnu92]

A function F is APN if: $\quad \forall \Delta^{\text{in}} \neq 0, \Delta^{\text{out}}, \quad \delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) \leq 2.$

Almost perfect non-linear (APN) function

Definition (APN function) [NybKnu92]

A function F is APN if: $\forall\, \Delta^{\text{in}} \neq \mathbf{0}, \Delta^{\text{out}}, \quad \delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) \leq \mathbf{2}.$

Almost perfect non-linear (APN) function

Definition (APN function) [NybKnu92]

A function F is APN if: $\forall \Delta^{\text{in}} \neq 0, \Delta^{\text{out}}, \quad \delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) \leq 2.$

A typical classification problem

- Easy definition
- Hard to find new instances (even for small n)
- Hard to classify the known instances
- Lots of open problems

Almost perfect non-linear (APN) function

Definition (APN function) [NybKnu92]

A function F is APN if: $\forall \Delta^{\text{in}} \neq 0, \Delta^{\text{out}}, \quad \delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) \leq 2.$

A typical classification problem

- Easy definition
- Hard to find new instances (even for small n)
- Hard to classify the known instances
- Lots of open problems

Big APN problem [BDMW10]

Find $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ which is APN, *bijective* for an *even* n.

A *single* example is known for $n = 6$.

Linear self-equivalence : a unifying PoV on the known families of APN functions

Univariate
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$
$L(x)^{2^k+1} + bx^{2^k+1}$

Multivariate
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{2s}+1} + x^{2^{2s}}y + y^{2^{2s}+1} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{3s}}y + xy^{2^{3s}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$

Univariate
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx$ …
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}($ …
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9$ … $)$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$
$L(x)^{2^k+1} + bx^{2^k+1}$

Multivariate
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
… $+1 + xy^{2^s} + y^{2^s+1}$ … $+1 + x^{2^{2s}}y + y^{2^{2s}+1}$
… $+1 + xy^{2^s} + y^{2^s+1}$ … $x^{2^{3s}}y + xy^{2^{3s}}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$

Hopefully clearer in 12 min ?

Polynomial representations of Boolean functions

Polynomial representations (1/2)

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^n, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} F_1(x_1, \ldots, x_n) \\ \vdots \\ F_n(x_1, \ldots, x_n) \end{pmatrix}.$$

Polynomial representations (1/2)

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^n, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} F_1(x_1, \dots, x_n) \\ \vdots \\ F_n(x_1, \dots, x_n) \end{pmatrix}.$$

Theorem (Lagrange multivariate interpolation)

$f : (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a polynomial representation in $\mathbb{F}_q[X_1, \dots, X_m]/(X_1^q + X_1, \dots, X_m^q + X_m)$.

Polynomial representations (1/2)

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^n, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} F_1(x_1, \ldots, x_n) \\ \vdots \\ F_n(x_1, \ldots, x_n) \end{pmatrix}.$$

Theorem (Lagrange multivariate interpolation)

$f : (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a polynomial representation in $\mathbb{F}_q[X_1, \ldots, X_m]/(X_1^q + X_1, \ldots, X_m^q + X_m)$.

Algebraic Normal Form (ANF)

$(q = 2, m = n)$. Each coordinate is a polynomial of $\mathbb{F}_2[X_1, \ldots, X_n]/(X_1^2 + X_1, \ldots, X_n^2 + X_n)$

Polynomial representations (1/2)

$$F: \mathbb{F}_2^n \to \mathbb{F}_2^n, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} F_1(x_1, \ldots, x_n) \\ \vdots \\ F_n(x_1, \ldots, x_n) \end{pmatrix}.$$

Theorem (Lagrange multivariate interpolation)

$f: (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a polynomial representation in $\mathbb{F}_q[X_1, \ldots, X_m]/(X_1^q + X_1, \ldots, X_m^q + X_m)$.

Algebraic Normal Form (ANF)

$(q = 2, m = n)$. Each coordinate is a polynomial of $\mathbb{F}_2[X_1, \ldots, X_n]/(X_1^2 + X_1, \ldots, X_n^2 + X_n)$

$$F: \mathbb{F}_2^4 \to \mathbb{F}_2^4, \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_0x_2 + x_0 + x_1x_2 + x_1x_3 \\ x_0x_1 + x_0x_2 + x_2x_3 + x_3 \\ x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2 \\ x_1x_3 + x_1 + x_2x_3 + x_2 + x_3 \end{pmatrix}$$

Polynomial representations (2/2)

Theorem (Lagrange multivariate interpolation)

$f: (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a polynomial representation in $\mathbb{F}_q[X_1, \ldots, X_m]/(X_1^q + X_1, \ldots, X_m^q + X_m)$.

Theorem (Lagrange multivariate interpolation)

$f : (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a polynomial representation in $\mathbb{F}_q[X_1, \ldots, X_m]/(X_1^q + X_1, \ldots, X_m^q + X_m)$.

$\mathbb{F}_2$-space isomorphisms

$$\mathbb{F}_2^n \quad \simeq \quad \mathbb{F}_{2^n} \quad \simeq \quad \mathbb{F}_{2^k}^{\ell}, \text{ with } n = \ell k.$$

Theorem (Lagrange multivariate interpolation)

$f : (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a polynomial representation in $\mathbb{F}_q[X_1, \ldots, X_m]/(X_1^q + X_1, \ldots, X_m^q + X_m)$.

$\mathbb{F}_2$-space isomorphisms

$$\mathbb{F}_2^n \quad \simeq \quad \mathbb{F}_{2^n} \quad \simeq \quad \mathbb{F}_{2^k}^\ell, \text{ with } n = \ell k.$$

Univariate representations ($q = 2^n, m = 1$)

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be seen as $\widetilde{F} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

$$\begin{aligned}\widetilde{F} : \mathbb{F}_{2^4} &\to \mathbb{F}_{2^4} \\ X &\mapsto \alpha_0 X^{12} + \alpha_1 X^6 + \alpha_2 X^3\end{aligned}$$

Polynomial representations (2/2)

Theorem (Lagrange multivariate interpolation)

$f : (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a polynomial representation in $\mathbb{F}_q[X_1, \ldots, X_m]/(X_1^q + X_1, \ldots, X_m^q + X_m)$.

$\mathbb{F}_2$-space isomorphisms

$$\mathbb{F}_2^n \simeq \mathbb{F}_{2^n} \simeq \mathbb{F}_{2^k}^\ell, \text{ with } n = \ell k.$$

Univariate representations $(q = 2^n, m = 1)$

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be seen as $\widetilde{F} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

$$\begin{aligned} \widetilde{F} : \mathbb{F}_{2^4} &\to \mathbb{F}_{2^4} \\ X &\mapsto \alpha_0 X^{12} + \alpha_1 X^6 + \alpha_2 X^3 \end{aligned}$$

Multivariate representations $(q = 2^k, m = \ell)$

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be seen as $\widetilde{F} : \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell$.

$$\begin{aligned} \widetilde{F} : \mathbb{F}_{2^2}^2 &\to \mathbb{F}_{2^2}^2 \\ \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} &\mapsto \begin{pmatrix} \alpha_0 x_0^3 + x_0^2 x_1 + \alpha_1 x_0 x_1^2 + \alpha_2 x_1^3 \\ \alpha_3 x_0^3 + \alpha_4 x_0^2 x_1 + \alpha_5 x_0 x_1^2 \end{pmatrix} \end{aligned}$$

Up to a choice of bases!

Polynomial representations and APN functions

$$\delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) = \left|\left\{x, F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}\right\}\right|$$

Polynomial representations and APN functions

$$\delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) = \left|\left\{x, F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}\right\}\right|$$

$A: (\mathbb{F}_2^n, +) \rightarrow (U, +_u)$ and $B: (V, +_v) \rightarrow (\mathbb{F}_2^n, +)$ linear bijective mappings.
Then $A \circ F \circ B: (V, +_v) \rightarrow (U, +_u)$

Polynomial representations and APN functions

$$\delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) = \left|\{x, F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}\}\right|$$

$A\colon (\mathbb{F}_2^n, +) \to (U, +_u)$ and $B\colon (V, +_v) \to (\mathbb{F}_2^n, +)$ linear bijective mappings.
Then $A \circ F \circ B\colon (V, +_v) \to (U, +_u)$

Proposition

- $\forall \Delta^{\text{in}}, \Delta^{\text{out}}, \quad \delta_F(B(\Delta^{\text{in}}), A^{-1}(\Delta^{\text{out}})) = \delta_{AFB}(\Delta^{\text{in}}, \Delta^{\text{out}})$
- F is APN if and only if $A \circ F \circ B$ is APN.

Definition (Linear equivalence)

$F_1 \sim_{\text{lin}} F_2$ if $\quad \exists\, A, B,$ bijective linear s.t. $\quad A \circ F_1 \circ B = F_2$.

Proper representatives for easier proofs

4 linearly-equivalent functions

$$F : \mathbb{F}_2^4 \to \mathbb{F}_2^4, \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_0x_2 + x_0 + x_1x_2 + x_1x_3 \\ x_0x_1 + x_0x_2 + x_2x_3 + x_3 \\ x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2 \\ x_1x_3 + x_1 + x_2x_3 + x_2 + x_3 \end{pmatrix}$$

$$F : \mathbb{F}_4^2 \to \mathbb{F}_4^2, \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \mapsto \begin{pmatrix} \alpha_0 x_0^3 + x_0^2 x_1 + \alpha_1 x_0 x_1^2 + \alpha_2 x_1^3 \\ \alpha_3 x_0^3 + \alpha_4 x_0^2 x_1 + \alpha_5 x_0 x_1^2 \end{pmatrix}$$

$$F : \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto \alpha_0 X^{12} + \alpha_1 X^6 + \alpha_2 X^3$$

Proper representatives for easier proofs

4 linearly-equivalent functions

$$F : \mathbb{F}_2^4 \to \mathbb{F}_2^4, \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_0x_2 + x_0 + x_1x_2 + x_1x_3 \\ x_0x_1 + x_0x_2 + x_2x_3 + x_3 \\ x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2 \\ x_1x_3 + x_1 + x_2x_3 + x_2 + x_3 \end{pmatrix}$$

$$F : \mathbb{F}_4^2 \to \mathbb{F}_4^2, \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \mapsto \begin{pmatrix} \alpha_0 x_0^3 + x_0^2 x_1 + \alpha_1 x_0 x_1^2 + \alpha_2 x_1^3 \\ \alpha_3 x_0^3 + \alpha_4 x_0^2 x_1 + \alpha_5 x_0 x_1^2 \end{pmatrix}$$

$$F : \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto \alpha_0 X^{12} + \alpha_1 X^6 + \alpha_2 X^3$$

$$F : \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto X^3$$

Proper representatives for easier proofs

4 linearly-equivalent functions

$$F : \mathbb{F}_2^4 \to \mathbb{F}_2^4, \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_0x_2 + x_0 + x_1x_2 + x_1x_3 \\ x_0x_1 + x_0x_2 + x_2x_3 + x_3 \\ x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2 \\ x_1x_3 + x_1 + x_2x_3 + x_2 + x_3 \end{pmatrix}$$

$$F : \mathbb{F}_4^2 \to \mathbb{F}_4^2, \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \mapsto \begin{pmatrix} \alpha_0 x_0^3 + x_0^2 x_1 + \alpha_1 x_0 x_1^2 + \alpha_2 x_1^3 \\ \alpha_3 x_0^3 + \alpha_4 x_0^2 x_1 + \alpha_5 x_0 x_1^2 \end{pmatrix}$$

$$F : \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto \alpha_0 X^{12} + \alpha_1 X^6 + \alpha_2 X^3$$

$$F : \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto X^3$$

$$F(X + \Delta) + F(X) = \Delta^{\text{out}}$$

Proper representatives for easier proofs

4 linearly-equivalent functions

$$F : \mathbb{F}_2^4 \to \mathbb{F}_2^4, \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_0x_2 + x_0 + x_1x_2 + x_1x_3 \\ x_0x_1 + x_0x_2 + x_2x_3 + x_3 \\ x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2 \\ x_1x_3 + x_1 + x_2x_3 + x_2 + x_3 \end{pmatrix}$$

$$F : \mathbb{F}_4^2 \to \mathbb{F}_4^2, \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \mapsto \begin{pmatrix} \alpha_0 x_0^3 + x_0^2 x_1 + \alpha_1 x_0 x_1^2 + \alpha_2 x_1^3 \\ \alpha_3 x_0^3 + \alpha_4 x_0^2 x_1 + \alpha_5 x_0 x_1^2 \end{pmatrix}$$

$$F : \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto \alpha_0 X^{12} + \alpha_1 X^6 + \alpha_2 X^3$$

$$F : \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto X^3$$

$$F(X + \Delta) + F(X) = \Delta^{\text{out}}$$

$$(X + \Delta)^3 + X^3 = \Delta^{\text{out}}$$

Proper representatives for easier proofs

4 linearly-equivalent functions

$$F : \mathbb{F}_2^4 \to \mathbb{F}_2^4, \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_0x_2 + x_0 + x_1x_2 + x_1x_3 \\ x_0x_1 + x_0x_2 + x_2x_3 + x_3 \\ x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2 \\ x_1x_3 + x_1 + x_2x_3 + x_2 + x_3 \end{pmatrix}$$

$$F : \mathbb{F}_4^2 \to \mathbb{F}_4^2, \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \mapsto \begin{pmatrix} \alpha_0 x_0^3 + x_0^2 x_1 + \alpha_1 x_0 x_1^2 + \alpha_2 x_1^3 \\ \alpha_3 x_0^3 + \alpha_4 x_0^2 x_1 + \alpha_5 x_0 x_1^2 \end{pmatrix}$$

$$F : \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto \alpha_0 X^{12} + \alpha_1 X^6 + \alpha_2 X^3$$

$$F : \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto X^3$$

$$F(X + \Delta) + F(X) = \Delta^{\text{out}}$$
$$(X + \Delta)^3 + X^3 = \Delta^{\text{out}}$$
$$\Delta X^2 + \Delta^2 X + \Delta^3 + \Delta^{\text{out}} = 0$$

Proper representatives for easier proofs

4 linearly-equivalent functions

$$F: \mathbb{F}_2^4 \to \mathbb{F}_2^4, \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_0x_2 + x_0 + x_1x_2 + x_1x_3 \\ x_0x_1 + x_0x_2 + x_2x_3 + x_3 \\ x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2 \\ x_1x_3 + x_1 + x_2x_3 + x_2 + x_3 \end{pmatrix}$$

$$F: \mathbb{F}_4^2 \to \mathbb{F}_4^2, \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \mapsto \begin{pmatrix} \alpha_0 x_0^3 + x_0^2 x_1 + \alpha_1 x_0 x_1^2 + \alpha_2 x_1^3 \\ \alpha_3 x_0^3 + \alpha_4 x_0^2 x_1 + \alpha_5 x_0 x_1^2 \end{pmatrix}$$

$$F: \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto \alpha_0 X^{12} + \alpha_1 X^6 + \alpha_2 X^3$$

$$F: \mathbb{F}_{16} \to \mathbb{F}_{16}, X \mapsto X^3$$

$$F(X + \Delta) + F(X) = \Delta^{\text{out}}$$

$$(X + \Delta)^3 + X^3 = \Delta^{\text{out}}$$

$$\Delta X^2 + \Delta^2 X + \Delta^3 + \Delta^{\text{out}} = 0$$

$\implies$ at most 2 solutions $\implies$ APN !

Linear self-equivalence : a unifying PoV on the known families of APN functions

Univariate
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$
$L(x)^{2^k+1} + bx^{2^k+1}$

Multivariate
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{2s}+1} + x^{2^{2s}}y + y^{2^{2s}+1} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{3s}}y + xy^{2^{3s}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$

Linear self-equivalence : a unifying PoV on the known families of APN functions

Univariate
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2\dots}$ …
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a\dots$ …
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a\dots x\dots)$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$
$L(x)^{2^k+1} + bx^{2^k+1}$

Multivariate
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
… $\dots{}^{s}+1 + xy^{2^s} + y^{2^s+1}$, $\dots+1 + x^{2^{2s}}y + y^{2^{2s}+1}$)
$(x,y) \mapsto$ (… $\dots+1 + xy^{2^s} + y^{2^s+1}$, $x^{2^{3s}}y + xy^{2^{3s}}$)
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$

Hopefully clearer in 5 min ?

A unified point-of-view on the known APN functions

One of the first non-power functions

An APN binomial

[BudCarLea08]

$$G : \mathbb{F}_{2^{12}} \rightarrow \mathbb{F}_{2^{12}} \quad x \mapsto x^3 + \alpha x^{528}$$

$G(x) = x^3(1 + x^{525}) = x^3 P(x^{15})$, where $P = 1 + X^{35}$ $\qquad (525 = 35 \times 15)$

One of the first non-power functions

An APN binomial

[BudCarLea08]

$$G : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3 + \alpha x^{528}$$

$G(x) = x^3(1 + x^{525}) = x^3 P(x^{15})$, where $P = 1 + X^{35}$ $(525 = 35 \times 15)$

$\mathbb{F}_{2^4}^* \subset \mathbb{F}_{2^{12}}^*$.

One of the first non-power functions

An APN binomial

[BudCarLea08]

$$G : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3 + \alpha x^{528}$$

$G(x) = x^3(1 + x^{525}) = x^3 P(x^{15})$, where $P = 1 + X^{35}$ $(525 = 35 \times 15)$

$\mathbb{F}_{2^4}^* \subset \mathbb{F}_{2^{12}}^*$.

$$\forall \varphi \in \mathbb{F}_{2^4}^*, \quad G(\varphi) = \varphi^3 P(\varphi^{15}) = \varphi^3 P(1).$$

One of the first non-power functions

An APN binomial [BudCarLea08]

$$G : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3 + \alpha x^{528}$$

$G(x) = x^3(1 + x^{525}) = x^3 P(x^{15})$, where $P = 1 + X^{35}$ $(525 = 35 \times 15)$

$\mathbb{F}_{2^4}^* \subset \mathbb{F}_{2^{12}}^*$.

$$\forall \varphi \in \mathbb{F}_{2^4}^*, \quad G(\varphi) = \varphi^3 P(\varphi^{15}) = \varphi^3 P(1).$$

Proposition

For any $\gamma \in \mathbb{F}_{2^{12}}^*$, the restriction of $G|_{\gamma \mathbb{F}_{2^4}^*}$ is (up to a constant) the power mapping $x \mapsto x^3$.

The multiplicative point of view

An APN binomial

[BudCarLea08]

- $G : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3 + \alpha x^{528}$
- $G|_{\mathbb{F}_{2^4}} : \varphi \mapsto c\varphi^3$

An APN binomial

[BudCarLea08]

- $G\colon \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3 + \alpha x^{528}$
- $G|_{\mathbb{F}_{2^4}} : \varphi \mapsto c\varphi^3$

Multivariate point-of-view

G is linearly equivalent to $\widetilde{G}\colon (\mathbb{F}_{2^4})^3 \to (\mathbb{F}_{2^4})^3 \ (x_1, x_2, x_3) \mapsto \left(\widetilde{G_1}(x), \widetilde{G_2}(x), \widetilde{G_3}(x)\right)$.

$$\widetilde{G}_1(x) = ?x_1^2x_2 + ?x_1x_2^2 + ?x_2^3 + ?x_1^2x_3 + ?x_2^2x_3 + ?x_1x_3^2 + ?x_2x_3^2 + ?x_3^3.$$

All coordinates of $\widetilde{G}$ are homogeneous of the same degree 3.

The multiplicative point of view

An APN binomial

[BudCarLea08]

- $G\colon \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3 + \alpha x^{528}$
- $G|_{\mathbb{F}_{2^4}} : \varphi \mapsto c\varphi^3$

Multivariate point-of-view

G is linearly equivalent to $\widetilde{G}\colon (\mathbb{F}_{2^4})^3 \to (\mathbb{F}_{2^4})^3$ $(x_1, x_2, x_3) \mapsto \left(\widetilde{G_1}(x), \widetilde{G_2}(x), \widetilde{G_3}(x)\right)$.

$$\widetilde{G}_1(x) = ?x_1^2 x_2 + ?x_1 x_2^2 + ?x_2^3 + ?x_1^2 x_3 + ?x_2^2 x_3 + ?x_1 x_3^2 + ?x_2 x_3^2 + ?x_3^3.$$

All coordinates of $\widetilde{G}$ are homogeneous of the same degree 3.

An APN bivariate functions

[ZhoPot13]

$$H\colon \mathbb{F}_{64}^2 \to \mathbb{F}_{64}^2, (x, y) \mapsto (xy, x^3 + ay^3)$$

- H_1 homogeneous of order 2.
- H_2 homogeneous of order 3.

Power mapping

$$F(x) = x^e$$

Let $\lambda \in \mathbb{F}_{2^n}^*$. Then for all x, $F(\lambda x) = \lambda^e x^e = \lambda^e F(x)$.
Thus $A \circ F \circ B = F$ with $B(x) := \lambda x,\ A(x) := \lambda^{-e} x$.

Linear self-equivalence

Power mapping

$$F(x) = x^e$$

Let $\lambda \in \mathbb{F}_{2^n}^*$. Then for all x, $F(\lambda x) = \lambda^e x^e = \lambda^e F(x)$.
Thus $A \circ F \circ B = F$ with $B(x) := \lambda x,\ A(x) := \lambda^{-e} x$.

Cyclotomic mapping w.r.t a subfield [Wang07]

$$G(x) = x^e P\left(x^{2^k - 1}\right), n = \ell k$$

Let $\varphi \in \mathbb{F}_{2^k}$. Then for all x, $G(\varphi x) = \varphi^e x^e P\left(x^{2^k-1}\right) = \varphi^e G(x)$.
Thus $A \circ G \circ B = G$ with $B(x) := \varphi x,\ A(x) := \varphi^{-e} x$.

Linear self-equivalence

Power mapping

$$F(x) = x^e$$

Let $\lambda \in \mathbb{F}_{2^n}^*$. Then for all x, $F(\lambda x) = \lambda^e x^e = \lambda^e F(x)$.
Thus $A \circ F \circ B = F$ with $B(x) := \lambda x$, $A(x) := \lambda^{-e} x$.

Cyclotomic mapping w.r.t a subfield [Wang07]

$$G(x) = x^e P\left(x^{2^k-1}\right), n = \ell k$$

Let $\varphi \in \mathbb{F}_{2^k}$. Then for all x, $G(\varphi x) = \varphi^e x^e P\left(x^{2^k-1}\right) = \varphi^e G(x)$.
Thus $A \circ G \circ B = G$ with $B(x) := \varphi x$, $A(x) := \varphi^{-e} x$.

ℓ-projective mapping [BCP24,Göloğlu22]

$$H\colon \mathbb{F}_{2^k}^{\ell} \to \mathbb{F}_{2^k}^{\ell}\ (x_1, \ldots, x_\ell) \mapsto (H_1(x), \ldots, H_\ell(x)),$$

$\forall\, i$, H_i is homogeneous of order e_i.
Thus $A \circ H \circ B = H$ with

$$B(x) = (\varphi x_1, \ldots, \varphi x_\ell),$$
$$A(x) = (\varphi^{-e_1} x_1, \ldots, \varphi^{-e_\ell} x_\ell)$$

Our main result (1/2)

Among the 22 known infinite APN families, 19 consist entirely of *cyclotomic* or *ℓ-projective* mappings, *up to linear equivalence*.

Univariate
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$
$L(x)^{2^k+1} + bx^{2^k+1}$

Our main result (1/2)

Among the 22 known infinite APN families, 19 consist entirely of ***cyclotomic*** or ***ℓ-projective*** mappings, ***up to linear equivalence***.

Univariate	Observations
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$	cyclotomic
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$	cyclotomic
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$	$\sim_{\text{lin}}$ biprojective
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$	cyclotomic/($\sim_{\text{lin}}$) frob.
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$	cyclotomic/($\sim_{\text{lin}}$) frob.
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$	cyclotomic/($\sim_{\text{lin}}$) frob.
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$	cyclotomic
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$	cyclotomic
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$	$\sim_{\text{lin}}$ biprojective
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$	$\sim_{\text{lin}}$ biprojective
$L(x)^{2^k+1} + bx^{2^k+1}$	?

Our main result (2/2)

Among the 22 known infinite APN families, 19 consist entirely of *cyclotomic* or *ℓ-projective* mappings, *up to linear equivalence*.

Multivariate	Observations
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ biprojective
$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ biprojective
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ 4-projective
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{2s}+1} + x^{2^{2s}}y + y^{2^{2s}+1} \end{pmatrix}$	biprojective
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{3s}}y + xy^{2^{3s}} \end{pmatrix}$	biprojective
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$	biprojective
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$	biprojective
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$	3-projective $\sim_{\text{lin}}$ cyclotomic
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$	3-projective $\sim_{\text{lin}}$ cyclotomic

Take away

Theorem

Among the 22 known infinite APN families, 19 consist entirely of ***cyclotomic*** or ***ℓ-projective*** mappings, ***up to linear equivalence***.

Sum up

- Characterization of ***very specific*** self-equivalences
- Unify most of the approaches
- Partial answer to the ***detection*** of such structures up to equivalence

Take away

Theorem

Among the 22 known infinite APN families, 19 consist entirely of *cyclotomic* or *ℓ-projective* mappings, *up to linear equivalence*.

Sum up

- Characterization of *very specific* self-equivalences
- Unify most of the approaches
- Partial answer to the *detection* of such structures up to equivalence

Open questions

- Link between self-equivalence and APN-ness [BeiBriLea21, Conjecture 1]
- Cyclotomic mappings outside the known classes? (from *non-quadratic* APN monomial)
- Projective mappings outside the known classes? (with *more* coordinates)

About the naming

Definition (APN function) [NybKnu92]

A function $\boldsymbol{F}$ is APN if: $\forall\, \boldsymbol{\Delta}^{\text{in}} \neq \mathbf{0}, \boldsymbol{\Delta}^{\text{out}}, \quad \delta_{\boldsymbol{F}}(\boldsymbol{\Delta}^{\text{in}}, \boldsymbol{\Delta}^{\text{out}}) \leq \mathbf{2}.$

About the naming

Definition (APN function) [NybKnu92]

A function F is APN if: $\forall \Delta^{\text{in}} \neq 0, \Delta^{\text{out}}, \quad \delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) \leq 2.$

The linear case

F linear.

$$F(x + \Delta^{\text{in}}) + F(x) = F(x) + F(\Delta^{\text{in}}) + F(x) = F(\Delta^{\text{in}})$$

$\Delta^{\text{in}} \neq 0.$ $\quad \delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) = \begin{cases} 2^n & \text{if } \Delta^{\text{out}} = F(\Delta^{\text{in}}) \\ 0 & \text{otherwise.} \end{cases}$

About the naming

Definition (APN function) [NybKnu92]

A function F is APN if: $\forall \Delta^{\text{in}} \neq 0, \Delta^{\text{out}}, \quad \delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) \leq 2.$

The linear case

F linear.

$$F(x + \Delta^{\text{in}}) + F(x) \quad = \quad F(x) + F(\Delta^{\text{in}}) + F(x) \quad = \quad F(\Delta^{\text{in}})$$

$\Delta^{\text{in}} \neq 0.$ $\quad \delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) = \begin{cases} 2^n & \text{if } \Delta^{\text{out}} = F(\Delta^{\text{in}}) \\ 0 & \text{otherwise.} \end{cases}$

The APN case

F APN. Then $\forall \Delta^{\text{in}} \neq 0, \quad \left|\left\{\Delta^{\text{out}},\ \delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) > 0\right\}\right| = 2^{n-1}.$