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

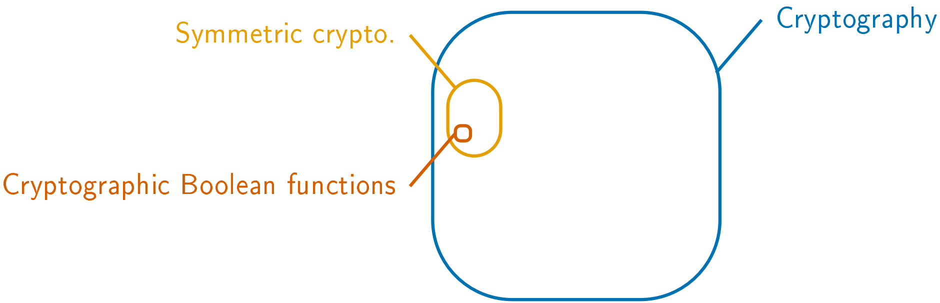
Jules Baudrin

based on joint works with A. Canteaut & L. Perrin

Crypto seminar, UVSQ, February 21th, 2025

Contact: jules.baudrin@uclouvain.be

Searching for ideal components



Using optimal components

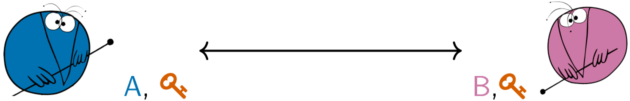
- to reach a high security at *lower costs*
- to achieve ideal properties ***assumed in security proofs***

Outline

- Symmetric encryption schemes
- Block cipher (security and construction)
- Differential cryptanalysis and APN functions
- Vectorial Boolean function study
- APN state of the art
- Our unified point of view on the known APN functions

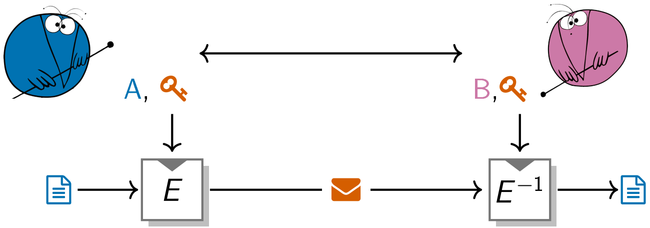
Goal

Ensure *confidentiality* under the assumption of a *shared secret* .



Goal

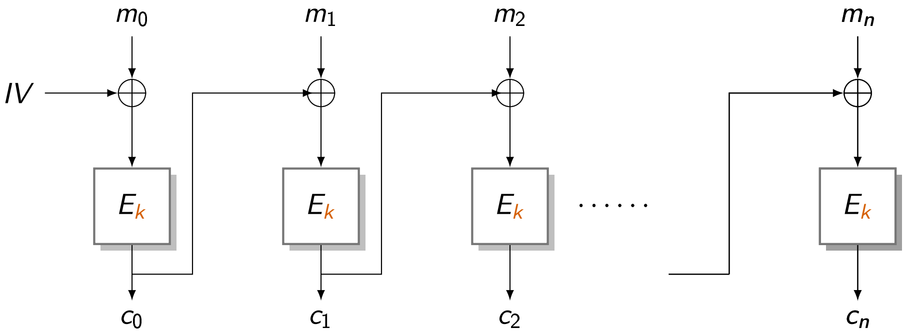
Ensure *confidentiality* under the assumption of a *shared secret* 🔑.



Constraints

- Secure
- Easily implemented
- Arbitrary-long messages

Building a symmetric encryption scheme



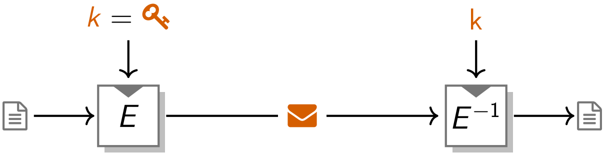
Ingredients

- a key-dependent transformation of n-bit words (*e.g.* $n = 128$). *Block cipher*
- a chaining method to handle arbitrary-long messages *Mode of operation*

Block cipher

A key-dependent transformation of n-bit words. $\rightsquigarrow$ A family of bijections $\mathcal{E}$:

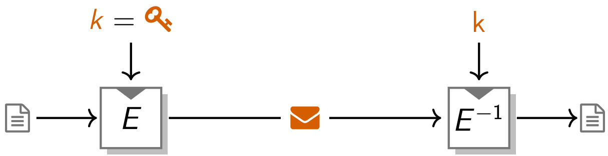
$$\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa} .$$



Block cipher

A key-dependent transformation of n-bit words. $\rightsquigarrow$ A family of bijections $\mathcal{E}$:

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



Ideal block cipher

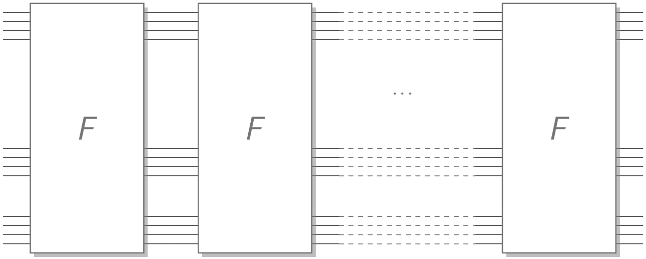
A *random* family of bijections.

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

- to satisfy assumptions of security proofs
- to avoid key recoveries.

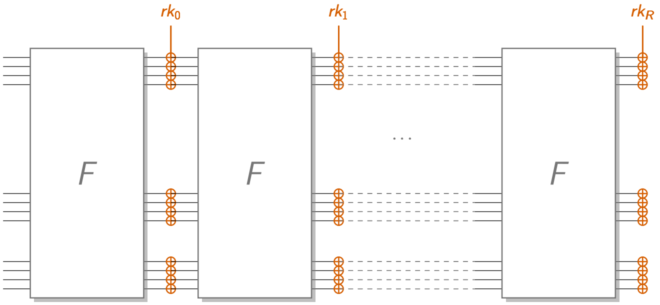
Block cipher

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



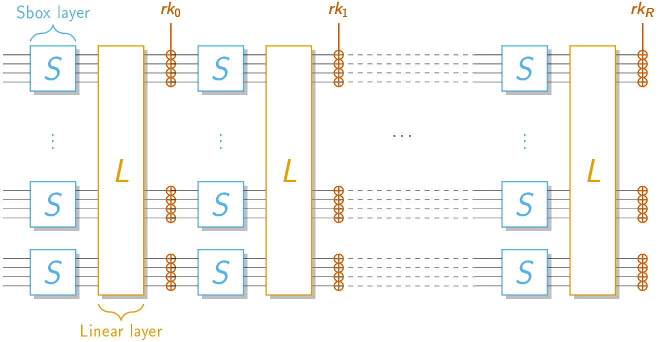
Block cipher

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



Block cipher

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



Differential cryptanalysis

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

Principle

Studies for each input difference $\Delta^{\text{in}} \in \mathbb{F}_2^n$, the *distribution of output differences*:

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

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

Principle

Studies for each input difference $\Delta^{\mathrm{in}} \in \mathbb{F}_2^n$, the *distribution of output differences*:

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

Average over all bijections

$F(x + \Delta^{\mathrm{in}}) + F(x) = \Delta^{\mathrm{out}}$ has 1 solution x on average.

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

Principle

Studies for each input difference $\Delta^{\text{in}} \in \mathbb{F}_2^n$, 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

$F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}$ has 1 solution x on average.

Differential distinguisher [BihSha91]

$\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ s.t for many k, $\quad E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has many solutions x.

Differential distinguisher [BihSha91]

$\Delta^{\mathrm{in}} \neq 0, \Delta^{\mathrm{out}}$ s.t for many k, $\quad E_k(x + \Delta^{\mathrm{in}}) + E_k(x) = \Delta^{\mathrm{out}}$ has many solutions x.

Resisting against differential attacks

Differential distinguisher [BihSha91]

$\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ 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 $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ and all keys k, $E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has ***few*** solutions.

Resisting against differential attacks

Differential distinguisher

[BihSha91]

$\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ 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 $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ 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 $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) := \left|\{x,\ S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\}\right|$ *as low as possible*.

Resisting against differential attacks

Differential distinguisher [BihSha91]

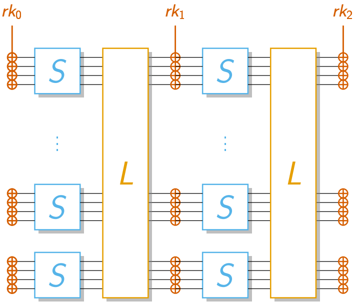
$\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ s.t for many k, $E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ has many solutions x.

Differential resistance

For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ 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 $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) := \left|\{x,\ S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\}\right|$ *as low as possible*.



On average over all (rk_0, rk_1, rk_2)

$$\mathbb{P}[\Delta^{\text{in}}, \Delta^{(1)}, \Delta^{\text{out}}] \leq \left(\frac{\max_{a \neq 0, b} \delta_S(a,b)}{2^m}\right)^{d(L)}$$

How to achieve this

For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) := \left|\{x,\ S(x+\Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\}\right|$ *as low as possible*.

How to achieve this

For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) := \left|\{x,\ S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\}\right|$ *as low as possible*.

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

How to achieve this

For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) := \left|\left\{x,\ S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\right\}\right|$ *as low as possible*.

- 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. $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}})$ is even.

How to achieve this

For all $\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}}) := \left|\{x,\ S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}}\}\right|$ *as low as possible*.

- 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. $\delta_S(\Delta^{\text{in}}, \Delta^{\text{out}})$ is even.

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

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

Almost perfect non-linear (APN) function

Definition (APN function) [NybKnu92]

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

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: $\forall\ \Delta^{\mathrm{in}} \neq 0, \Delta^{\mathrm{out}}, \quad \delta_F(\Delta^{\mathrm{in}}, \Delta^{\mathrm{out}}) \leq 2.$

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 $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ which is APN, bijective for an even n.

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

Boolean function study

Representing a vectorial Boolean function

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

Each $F_i : \mathbb{F}_2^n \to \mathbb{F}_2$ is a ***coordinate***.

Representing a vectorial Boolean function

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

Each $F_i : \mathbb{F}_2^n \to \mathbb{F}_2$ is a ***coordinate***.

A ***component*** of F is a linear combination of coordinate: $\alpha \cdot F := \sum_{i=0}^{n-1} \alpha_i F_i$.

Representing a vectorial Boolean function

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

Each $F_i : \mathbb{F}_2^n \to \mathbb{F}_2$ is a ***coordinate***.

A ***component*** of F is a linear combination of coordinate: $\alpha \cdot F := \sum_{i=0}^{n-1} \alpha_i F_i$.

Representations we won't look at

- Truth table / ***graph*** of F: $\mathcal{G}_F = \{(x, F(x)), x \in \mathbb{F}_2^n\}$
- ***Walsh transform***: Fourier transform of all components $\alpha \cdot F : \mathbb{F}_2^n \to \mathbb{F}_2 \subset \mathbb{C}$

Theorem (Lagrange multivariate interpolation)

$f\colon (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a unique 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 unique 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 $\mathbb{F}_2[X_1, \ldots, X_n]/(X_1^2 + X_1, \ldots, X_n^2 + X_n)$

Theorem (Lagrange multivariate interpolation)

$f : (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a unique 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 (1/2)

Theorem (Lagrange multivariate interpolation)

$f : (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a unique 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 $\mathbb{F}_2[X_1, \ldots, X_n]/(X_1^2 + X_1, \ldots, X_n^2 + X_n)$

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

Algebraic degree : $\deg_a(F) := \max_{1 \leq i \leq n} \deg(F_i)$. Here $\deg_a(F) = 2$

Polynomial representations (2/2)

Theorem (Lagrange multivariate interpolation)

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

Theorem (Lagrange multivariate interpolation)

$f : (\mathbb{F}_q)^m \rightarrow \mathbb{F}_q$ admits a unique 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

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

Theorem (Lagrange multivariate interpolation)

$f : (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a unique 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

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

Up to a choice of bases, we get:

Univariate representation

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be seen as $\widetilde{F} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.
$(q = 2^n, m = 1)$

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

Polynomial representations (2/2)

Theorem (Lagrange multivariate interpolation)

$f\colon (\mathbb{F}_q)^m \to \mathbb{F}_q$ admits a unique 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

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

Up to a choice of bases, we get:

Univariate representation

$F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be seen as $\widetilde{F}\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.
$(q = 2^n, m = 1)$

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

Multivariate representation(s)

$F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be seen as $\widetilde{F}\colon \mathbb{F}_{2^k}^{\ell} \to \mathbb{F}_{2^k}^{\ell}$.
$(q = 2^k, m = \ell)$

$$\widetilde{F}\colon \mathbb{F}_{2^2}^2 \to \mathbb{F}_{2^2}^2$$

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \mapsto \begin{pmatrix} \alpha_0 x_0^3 + x_0^2 x_1 + \alpha_1 x_0 x_1^2 + \alpha_2 x_1^3 \\ \alpha_3 x_0^3 + \alpha_4 x_0^2 x_1 + \alpha_5 x_0 x_1^2 \end{pmatrix}$$

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

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

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

Polynomial representations and APN functions

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

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

$$A \circ F \circ B(x +_V \Delta^{\text{in}}) \quad +_U \quad A \circ F \circ B(x) \quad = \quad \Delta^{\text{out}}$$

Polynomial representations and APN functions

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

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

$$\begin{array}{ccccc} A \circ F \circ B(x +_V \Delta^{\text{in}}) & +_U & A \circ F \circ B(x) & = & \Delta^{\text{out}} \\ F \circ B(x +_V \Delta^{\text{in}}) & + & F \circ B(x) & = & A^{-1}(\Delta^{\text{out}}) \end{array}$$

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

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

$$\begin{array}{ccccc} A \circ F \circ B(x +_V \Delta^{\text{in}}) & +_U & A \circ F \circ B(x) & = & \Delta^{\text{out}} \\ F \circ B(x +_V \Delta^{\text{in}}) & + & F \circ B(x) & = & A^{-1}(\Delta^{\text{out}}) \\ F(B(x) + B(\Delta^{\text{in}})) & + & F \circ B(x) & = & A^{-1}(\Delta^{\text{out}}) \end{array}$$

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

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

$$\begin{array}{ccccc} A \circ F \circ B(x +_V \Delta^{\mathrm{in}}) & +_U & A \circ F \circ B(x) & = & \Delta^{\mathrm{out}} \\ F \circ B(x +_V \Delta^{\mathrm{in}}) & + & F \circ B(x) & = & A^{-1}(\Delta^{\mathrm{out}}) \\ F(B(x) + B(\Delta^{\mathrm{in}})) & + & F \circ B(x) & = & A^{-1}(\Delta^{\mathrm{out}}) \end{array}$$

Proposition (Linear equivalence)

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

Linear equivalence

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

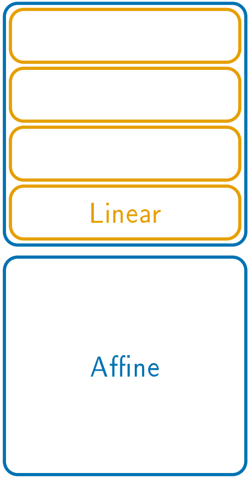
Equivalence relations

Linear equivalence

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

Affine equivalence

$F_1 \sim_{\mathrm{aff}} F_2$ if $\exists\ A, B,$ bijective *affine* s.t. $A \circ F_1 \circ B = F_2$.



Equivalence relations

Linear equivalence

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

Affine equivalence

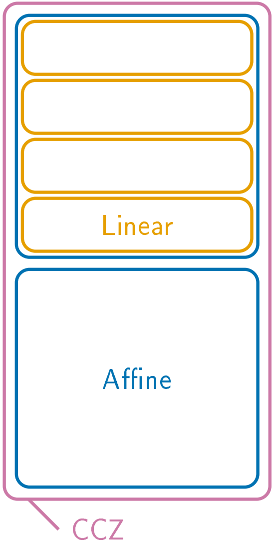
$F_1 \sim_{\text{aff}} F_2$ if $\exists\ A, B$, bijective *affine* s.t. $A \circ F_1 \circ B = F_2$.

CCZ equivalence [CCZ98]

$F_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n \sim_{\text{CCZ}} F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ if: $\exists\ \mathcal{A} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$ bijective *affine* s.t.

$$\mathcal{A}\left(\mathcal{G}_{F_1}\right) = \mathcal{G}_{F_2},$$

where $\mathcal{G}_F := \{(x, F(x), x \in \mathbb{F}_2^n)\}$.



Linear equivalence

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

Affine equivalence

$F_1 \sim_{\text{aff}} F_2$ if $\exists$ A, B, bijective *affine* s.t. $A \circ F_1 \circ B = F_2$.

CCZ equivalence [CCZ98]

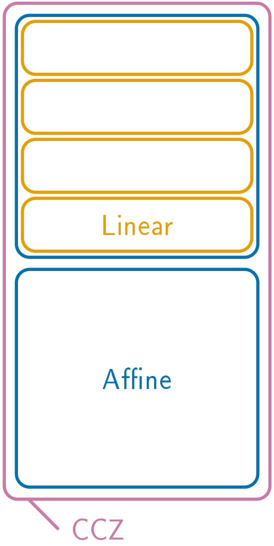
$F_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n \sim_{\text{CCZ}} F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ if: $\exists$ $\mathcal{A} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$ bijective *affine* s.t.

$$\mathcal{A}(\mathcal{G}_{F_1}) = \mathcal{G}_{F_2},$$

where $\mathcal{G}_F := \{(x, F(x), x \in \mathbb{F}_2^n)\}$.

Proposition

If $F_1 \sim_{\text{CCZ}} F_2$, then F_1 APN $\iff$ F_2 APN.



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 representation for easier proofs

4 linearly-equivalent functions

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

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

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

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

4 linearly-equivalent functions

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

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

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

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

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

4 linearly-equivalent functions

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

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

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

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

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

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

Proper representation for easier proofs

4 linearly-equivalent functions

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

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

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

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

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

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

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

Proper representation for easier proofs

4 linearly-equivalent functions

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

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

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

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

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

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

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

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

The APN family tree

A common descent [Nyberg93]

The function $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, X \mapsto X^3$ is APN.

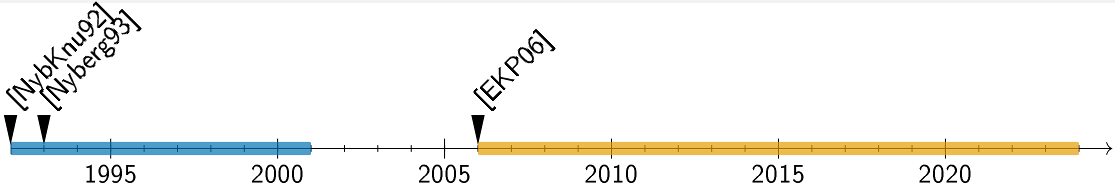
- F is a power mapping
- F is quadratic: $\deg_a(F) = \mathrm{wt}(3) = 2$

A common descent

[Nyberg93]

The function $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, X \mapsto X^3$ is APN.

- F is a power mapping
- F is quadratic: $\deg_a(F) = \mathrm{wt}(3) = 2$



Descendants

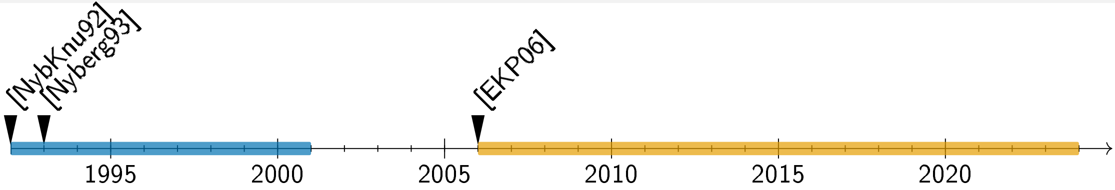
- 6 infinite families of APN power mappings, some are ***not quadratic***.
- About 20 infinite families of quadratic APN mappings.

The APN family tree

A common descent [Nyberg93]

The function $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, X \mapsto X^3$ is APN.

- F is a power mapping
- F is quadratic: $\deg_a(F) = \mathrm{wt}(3) = 2$



Descendants

- 6 infinite families of APN power mappings, some are ***not quadratic***.
- About 20 infinite families of quadratic APN mappings.

A single counter-example [BriLea08,EdePot09]

A single APN function ***inequivalent*** to a power mapping or a quadratic mapping is known.

Infinite families of quadratic APN mappings

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

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

Where to look for a new function ?

How to prove that a new F is actually new ?

Intersection between families ?

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

One of the first non-power functions

An APN binomial [BudCarLea08]

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

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

One of the first non-power functions

An APN binomial [BudCarLea08]

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

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

$\mathbb{F}_{2^4}^* \subset \mathbb{F}_{2^{12}}^*$. $\quad \mathbb{F}_{2^{12}}^* = \bigsqcup_{\gamma \in \Gamma} \gamma \mathbb{F}_{2^4}^*$ for some system of representatives Γ.

One of the first non-power functions

An APN binomial [BudCarLea08]

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

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

$\mathbb{F}_{2^4}^* \subset \mathbb{F}_{2^{12}}^*$. $\mathbb{F}_{2^{12}}^* = \bigsqcup_{\gamma \in \Gamma} \gamma \mathbb{F}_{2^4}^*$ for some system of representatives Γ.

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

One of the first non-power functions

An APN binomial [BudCarLea08]

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

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

$\mathbb{F}_{2^4}^* \subset \mathbb{F}_{2^{12}}^*$. $\quad \mathbb{F}_{2^{12}}^* = \bigsqcup_{\gamma\in\Gamma} \gamma \mathbb{F}_{2^4}^*$ for some system of representatives Γ.

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

Proposition

The restriction of F to each *multiplicative coset* $\gamma\mathbb{F}_{2^4}^*$ acts *as a power mapping*.

Recap

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

Recap

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

Multivariate point-of-view

F is linearly equivalent to $\widetilde{F} : (\mathbb{F}_{2^4})^3 \to (\mathbb{F}_{2^4})^3 \ (x_1, x_2, x_3) \mapsto \left(\widetilde{F_1}(x), \widetilde{F_2}(x), \widetilde{F_3}(x)\right)$.

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

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

Recap

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

Multivariate point-of-view

F is linearly equivalent to $\widetilde{F} : (\mathbb{F}_{2^4})^3 \to (\mathbb{F}_{2^4})^3 \; (x_1, x_2, x_3) \mapsto \left(\widetilde{F_1}(x), \widetilde{F_2}(x), \widetilde{F_3}(x)\right)$.

$$\widetilde{F_1}(x) = ?x_1^2x_2 + ?x_1x_2^2 + ?x_2^3 + ?x_1^2x_3 + ?x_2^2x_3 + ?x_1x_3^2 + ?x_2x_3^2 + ?x_3^3.$$

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

An APN bivariate functions [ZhoPot13]

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

F_1 homogeneous of order 2, F_2 homogeneous of order 3

Linear self-equivalence

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

Let $\lambda \in \mathbb{F}_{2^n}$. Then for all x, $F(\lambda x) = \lambda^e x^e = \lambda^e F(x)$.

Linear self-equivalence

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

Let $\lambda \in \mathbb{F}_{2^n}$. Then for all x, $F(\lambda x) = \lambda^e x^e = \lambda^e F(x)$.

Power mapping

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

Linear self-equivalence

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

Let $\lambda \in \mathbb{F}_{2^n}$. Then for all x, $F(\lambda x) = \lambda^e x^e = \lambda^e F(x)$.

Power mapping

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

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

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

Linear self-equivalence

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

Let $\lambda \in \mathbb{F}_{2^n}$. Then for all x, $F(\lambda x) = \lambda^e x^e = \lambda^e F(x)$.

Power mapping

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

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

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

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

Let $\varphi \in \mathbb{F}_{2^k}$, $B(x) := \varphi x$, $A(x) := \varphi^{-e} x$. Then: $A \circ F \circ B = F$.

Linear self-equivalence

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

Let $\lambda \in \mathbb{F}_{2^n}$. Then for all x, $F(\lambda x) = \lambda^e x^e = \lambda^e F(x)$.

Power mapping

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

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

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

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

Let $\varphi \in \mathbb{F}_{2^k}$, $B(x) := \varphi x$, $A(x) := \varphi^{-e} x$. Then: $A \circ F \circ B = F$.

ℓ-projective mapping [BCP24,Göloğlu22]

$$F : \mathbb{F}_{2^k}^{\ell} \to \mathbb{F}_{2^k}^{\ell}\ (x_1, \ldots, x_\ell) \mapsto (F_1(x), \ldots, F_\ell(x)),$$

$\forall\ i$, F_i is homogeneous of order e_i.

$A \circ F \circ B = F$ 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
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$	$\sim_{\mathrm{lin}}$ biprojective
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$	cyclotomic/($\sim_{\mathrm{lin}}$) frob.
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$	cyclotomic/($\sim_{\mathrm{lin}}$) frob.
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$	cyclotomic/($\sim_{\mathrm{lin}}$) 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
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$	$\sim_{\mathrm{lin}}$ biprojective
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$	$\sim_{\mathrm{lin}}$ 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

Sketch of proof

Linear self-equivalence & conjugacy

Let F be linearly self-equivalent: $F = A \circ F \circ B$.
Let G be linearly equivalent to F: $G = P \circ F \circ Q$.

Then G is linearly self-equivalent:

$$G = (P \circ A \circ P)^{-1} \circ G \circ (Q^{-1} \circ B \circ Q)$$

Sketch of proof

Linear self-equivalence & conjugacy

Let F be linearly self-equivalent: $F = A \circ F \circ B$.
Let G be linearly equivalent to F: $G = P \circ F \circ Q$.

Then G is linearly self-equivalent:

$$G = (P \circ A \circ P)^{-1} \circ G \circ (Q^{-1} \circ B \circ Q)$$

Furthermore, A and $P \circ A \circ P^{-1}$ are *similar* and thus share the same *elementary divisors*.

Linear self-equivalence & conjugacy

Let F be linearly self-equivalent: $F = A \circ F \circ B$.
Let G be linearly equivalent to F: $G = P \circ F \circ Q$.

Then G is linearly self-equivalent:

$$G = (P \circ A \circ P)^{-1} \circ G \circ (Q^{-1} \circ B \circ Q)$$

Furthermore, A and $P \circ A \circ P^{-1}$ are ***similar*** and thus share the same ***elementary divisors***.

$$G = P \circ F \circ Q = P \circ A \circ F \circ B \circ Q = P \circ A \circ P^{-1} \circ G \circ Q^{-1} \circ B \circ Q$$

Linear self-equivalence & conjugacy

Let F be linearly self-equivalent: $F = A \circ F \circ B$.
Let G be linearly equivalent to F: $G = P \circ F \circ Q$.

Then G is linearly self-equivalent:

$$G = (P \circ A \circ P)^{-1} \circ G \circ (Q^{-1} \circ B \circ Q)$$

Furthermore, A and $P \circ A \circ P^{-1}$ are *similar* and thus share the same *elementary divisors*.

$$G = P \circ F \circ Q = P \circ A \circ F \circ B \circ Q = P \circ A \circ P^{-1} \circ G \circ Q^{-1} \circ B \circ Q$$

Theorem (Alternative formulation)

Most of the known infinite APN families are made of *linearly self-equivalent mappings* with *very specific* mappings A, B. This can be detected independently of the representation.

Example: Cyclotomic mappings

Recap

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

Univariate: $A \circ F \circ B = F$ with $B(x) = \lambda x$, $A(x) = \lambda^{-e} x$ for any $\lambda \in \mathbb{F}_{2^k}^*$

Multivariate: $\widetilde{A} \circ \widetilde{F} \circ \widetilde{B} = \widetilde{F}$ with $\widetilde{B}(v) = (\lambda v_1, \ldots, \lambda v_\ell)$, $\widetilde{A}(v) = (\lambda^{-e} v_1, \ldots, \lambda^{-e} v_\ell)$

Example: Cyclotomic mappings

Recap

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

Univariate: $A \circ F \circ B = F$ with $B(x) = \lambda x$, $A(x) = \lambda^{-e} x$ for any $\lambda \in \mathbb{F}_{2^k}^*$

Multivariate: $\widetilde{A} \circ \widetilde{F} \circ \widetilde{B} = \widetilde{F}$ with $\widetilde{B}(v) = (\lambda v_1, \ldots, \lambda v_\ell)$, $\widetilde{A}(v) = (\lambda^{-e} v_1, \ldots, \lambda^{-e} v_\ell)$

Proposition (Up to linear equivalence)

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. F is linearly equivalent to a cyclotomic mapping w.r.t a subfield $\mathbb{F}_{2^k}$ iff:

$\exists$ A, B such that $A \circ F \circ B = F$ and:

- $\min(A), \min(B)$ are ***irreducible*** polynomials
- $\mathrm{ord}(B) = 2^k - 1$ and $\mathrm{ord}(A) \mid \mathrm{ord}(B)$

Sum up

- *Pen-and-paper* functions: linearly self-equivalent with *very specific* A, B
- From *computer searches*: most are linearly self-equivalent with *less structured* A, B.

Sum up

- *Pen-and-paper* functions: linearly self-equivalent with *very specific* A, B
- From *computer searches*: most are linearly self-equivalent with *less structured* A, B.

The only solution to the big APN problem

A single bijective APN mapping is known when n is even. It is *CCZ-equivalent* to the "Kim mapping":

$$\kappa \colon \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}, X \mapsto X^3 + X^{10} + uX^{24},$$

for some specific $u \in \mathbb{F}_{2^6}$.

Sum up

- *Pen-and-paper* functions: linearly self-equivalent with *very specific* A, B
- From *computer searches*: most are linearly self-equivalent with *less structured* A, B.

The only solution to the big APN problem

A single bijective APN mapping is known when n is even. It is *CCZ-equivalent* to the "Kim mapping":

$$\kappa : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}, X \mapsto X^3 + X^{10} + uX^{24},$$

for some specific $u \in \mathbb{F}_{2^6}$.

$\kappa(X) = X^3(1 + X^7 + uX^{21}) = X^3 P(X^{2^3-1})$ *cyclotomic w.r.t* $\mathbb{F}_{2^3}$.

A (re)open problem

Question

For an APN function F, does there always exist a *CCZ-equivalent* function G which is linear self-equivalent ($A \circ G \circ B = G$) ?

A (re)open problem

Question

For an APN function F, does there always exist a *CCZ-equivalent* function G which is linear self-equivalent ($A \circ G \circ B = G$) ?

Element of answers

- A *data base* of the known functions (sporadic / infinite families) for small n.
- Some of the properties of A, B are still preserved by *affine and CCZ equivalences*.

More self-equivalent APN functions ?

Previous works

Linearly self-equivalence to ***speed up searches*** [BeiBriLea21,BeiLea22].

More self-equivalent APN functions ?

Previous works

Linearly self-equivalence to *speed up searches* [BeiBriLea21,BeiLea22].

Toward new APN functions ?

- *Non-quadratic* linearly self-equivalent functions for $n = 6$?
- Cyclotomic mappings $F(x) = x^e P\left(x^{2^k-1}\right)$ with *non-quadratic* e ?
- ℓ-projective mappings with $\ell > 4$?

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
- Linearly self-equivalent APN functions from *computer searches* are generally *less structured*. [BeiBriLea21, BeiLea22]

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
- Linearly self-equivalent APN functions from *computer searches* are generally *less structured*. [BeiBriLea21,BeiLea22]

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

About the naming

Definition (APN function) [NybKnu92]

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

The linear case

F linear.

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

$\Delta^{\mathrm{in}} \neq 0.$

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

About the naming

Definition (APN function) [NybKnu92]

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

The linear case

F linear.

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

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

The APN case

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