Funzioni Generalized APN in caratteristica dispari e curve algebriche

Giovanni Zini

Università degli Studi di Modena e Reggio Emilia

Seminario congiunto
UMI (gruppo Crittografia e Codici) - DeCifris (gruppo MathCifris)

References

- M. Kuroda, S. Tsujie: A generalization of APN functions for odd characteristic, *Finite Fields Appl.* 47, 64–84 (2017).

- M. Kuroda: Monomial generalized almost perfect nonlinear functions, *Internat. J. Found. Comput. Sci.* 31(3), 411–419 (2020).

- Z. Zha, L. Hu, Z. Zhang: Three new classes of generalized almost perfect nonlinear power functions, *Finite Fields Appl.* 53, 254–266 (2018).

- F. Özbudak, A. Sălăgean: New generalized almost perfect nonlinear functions, *Finite Fields Appl.* 70, 101796 (2021).

- D. Bartoli, M. Giulietti, G. Peraro, G.Z.: On monomial generalized almost perfect nonlinear functions, *Finite Fields Appl.* 82, 102050 (2022).

PN functions

$p \geq 2$ prime $\qquad q = p^n \qquad \mathbb{F}_q$: finite field of order q

$$f : \mathbb{F}_q \to \mathbb{F}_q$$

PN functions

$$p \geq 2 \text{ prime} \qquad q = p^n \qquad \mathbb{F}_q : \text{ finite field of order } q$$

$$f : \mathbb{F}_q \to \mathbb{F}_q$$

- perfect nonlinear (PN): for all $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, the equation

$$f(x+a) - f(x) = b \tag{1}$$

has exactly 1 solution $\bar{x} \in \mathbb{F}_q$.

PN functions

$$p \geq 2 \text{ prime} \qquad q = p^n \qquad \mathbb{F}_q : \text{ finite field of order } q$$

$$f : \mathbb{F}_q \to \mathbb{F}_q$$

- perfect nonlinear (PN): for all $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, the equation

$$f(x+a) - f(x) = b \tag{1}$$

  has exactly 1 solution $\bar{x} \in \mathbb{F}_q$.

- If $\bar{x}$ is a solution of (1) and $0 \neq \bar{y} \in \mathbb{F}_q$ satisfies
  $f(\bar{y}+\bar{x}) = f(\bar{y}) + f(\bar{x}), \qquad f(\bar{y}+\bar{x}+a) = f(\bar{y}) + f(\bar{x}+a)$
  $\Longrightarrow \bar{y}+\bar{x}$ is another solution of (1)

PN functions

$$p \geq 2 \text{ prime} \qquad q = p^n \qquad \mathbb{F}_q : \text{ finite field of order } q$$
$$f : \mathbb{F}_q \to \mathbb{F}_q$$

- perfect nonlinear (PN): for all $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, the equation

$$f(x+a) - f(x) = b \tag{1}$$

  has exactly 1 solution $\bar{x} \in \mathbb{F}_q$.

- If $\bar{x}$ is a solution of (1) and $0 \neq \bar{y} \in \mathbb{F}_q$ satisfies
  $f(\bar{y}+\bar{x}) = f(\bar{y}) + f(\bar{x}), \qquad f(\bar{y}+\bar{x}+a) = f(\bar{y}) + f(\bar{x}+a)$
  $\Longrightarrow \bar{y}+\bar{x}$ is another solution of (1)

- PN functions are the most nonlinear functions

APN functions

$$p = 2, \quad f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},$$

$$f(x+a) + f(x) = b \quad (a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n})$$

APN functions

$$p = 2, \qquad f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},$$

$$f(x+a) + f(x) = b \qquad (a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n})$$

- if $\bar{x}$ is a solution, then $\bar{x} + a$ is a solution

APN functions

$$p = 2, \qquad f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},$$

$$f(x+a) + f(x) = b \qquad (a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n})$$

- if $\bar{x}$ is a solution, then $\bar{x} + a$ is a solution $\Longrightarrow$ no PN functions!

APN functions

$$p = 2, \qquad f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},$$

$$f(x+a) + f(x) = b \qquad (a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n})$$

- if $\bar{x}$ is a solution, then $\bar{x} + a$ is a solution $\Longrightarrow$ no PN functions!
- almost perfect nonlinear (APN):

  at most 2 solutions in $\mathbb{F}_{2^n}$ for all $a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$

APN functions

$$p = 2, \quad f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},$$
$$f(x+a) + f(x) = b \quad (a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n})$$

- if $\bar{x}$ is a solution, then $\bar{x} + a$ is a solution $\Longrightarrow$ no PN functions!
- almost perfect nonlinear (APN):

  at most 2 solutions in $\mathbb{F}_{2^n}$ for all $a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$

  $\Longrightarrow$ APN: the most nonlinear functions in characteristic 2

APN functions

$$p = 2, \quad f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},$$
$$f(x+a) + f(x) = b \quad (a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n})$$

- if $\bar{x}$ is a solution, then $\bar{x} + a$ is a solution $\Longrightarrow$ no PN functions!
- almost perfect nonlinear (APN):

  at most 2 solutions in $\mathbb{F}_{2^n}$ for all $a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$

  $\Longrightarrow$ APN: the most nonlinear functions in characteristic 2

  $\Longrightarrow$ S-boxes of block ciphers which are

  resistant against differential cryptanalysis

APN functions

$$p = 2, \quad f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},$$
$$f(x+a) + f(x) = b \quad (a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n})$$

- if $\bar{x}$ is a solution, then $\bar{x} + a$ is a solution $\Longrightarrow$ no PN functions!
- almost perfect nonlinear (APN):

  at most 2 solutions in $\mathbb{F}_{2^n}$ for all $a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$

  $\Longrightarrow$ APN: the most nonlinear functions in characteristic 2

  $\Longrightarrow$ S-boxes of block ciphers which are

  resistant against differential cryptanalysis

- Introduced by Nyberg (EUROCRYPT'93)
- Studied by many authors since then

APN functions: a connection to Finite Geometry

$V = V(m,2)$: m-dimensional $\mathbb{F}_2$-vector space

$\mathcal{S}$: family of $(d+1)$-dimensional vector subspaces of V

APN functions: a connection to Finite Geometry

$V = V(m,2)$: m-dimensional $\mathbb{F}_2$-vector space

$\mathcal{S}$: family of $(d+1)$-dimensional vector subspaces of V

$\mathcal{S}$ is a d-**dimensional dual hyperoval** if

- $\mathcal{S}$ has exactly $q^d + q^{d-1} + \cdots + q + 2$ elements
- the union of the elements of $\mathcal{S}$ generates V
- $\dim(U_1 \cap U_2) = 1$ for all distinct $U_1, U_2 \in \mathcal{S}$
- $U_1 \cap U_2 \cap U_3 = \{0\}$ for all distinct $U_1, U_2, U_3 \in \mathcal{S}$

APN functions: a connection to Finite Geometry

$V = V(m,2)$: m-dimensional $\mathbb{F}_2$-vector space

$\mathcal{S}$: family of $(d+1)$-dimensional vector subspaces of V

$\mathcal{S}$ is a d-**dimensional dual hyperoval** if

- $\mathcal{S}$ has exactly $q^d + q^{d-1} + \cdots + q + 2$ elements
- the union of the elements of $\mathcal{S}$ generates V
- $\dim(U_1 \cap U_2) = 1$ for all distinct $U_1, U_2 \in \mathcal{S}$
- $U_1 \cap U_2 \cap U_3 = \{0\}$ for all distinct $U_1, U_2, U_3 \in \mathcal{S}$

$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ quadratic function, e.g.: $x \mapsto x^{2^i+1}$

APN functions: a connection to Finite Geometry

$V = V(m, 2)$: m-dimensional $\mathbb{F}_2$-vector space

$\mathcal{S}$: family of $(d+1)$-dimensional vector subspaces of V

$\mathcal{S}$ is a d-**dimensional dual hyperoval** if

- $\mathcal{S}$ has exactly $q^d + q^{d-1} + \cdots + q + 2$ elements
- the union of the elements of $\mathcal{S}$ generates V
- $\dim(U_1 \cap U_2) = 1$ for all distinct $U_1, U_2 \in \mathcal{S}$
- $U_1 \cap U_2 \cap U_3 = \{0\}$ for all distinct $U_1, U_2, U_3 \in \mathcal{S}$

$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ quadratic function, e.g.: $x \mapsto x^{2^i+1}$

$B_f(x, a) := f(x+a) + f(x) + f(a) + f(0)$

APN functions: a connection to Finite Geometry

$V = V(m, 2)$: m-dimensional $\mathbb{F}_2$-vector space

$\mathcal{S}$: family of $(d+1)$-dimensional vector subspaces of V

$\mathcal{S}$ is a d-**dimensional dual hyperoval** if

- $\mathcal{S}$ has exactly $q^d + q^{d-1} + \cdots + q + 2$ elements
- the union of the elements of $\mathcal{S}$ generates V
- $\dim(U_1 \cap U_2) = 1$ for all distinct $U_1, U_2 \in \mathcal{S}$
- $U_1 \cap U_2 \cap U_3 = \{0\}$ for all distinct $U_1, U_2, U_3 \in \mathcal{S}$

$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ quadratic function, e.g.: $x \mapsto x^{2^i+1}$

$B_f(x, a) := f(x+a) + f(x) + f(a) + f(0) \longrightarrow B_f$ is $\mathbb{F}_2$-bilinear

APN functions: a connection to Finite Geometry

$V = V(m,2)$: m-dimensional $\mathbb{F}_2$-vector space

$\mathcal{S}$: family of $(d+1)$-dimensional vector subspaces of V

$\mathcal{S}$ is a d-**dimensional dual hyperoval** if

- $\mathcal{S}$ has exactly $q^d + q^{d-1} + \cdots + q + 2$ elements
- the union of the elements of $\mathcal{S}$ generates V
- $\dim(U_1 \cap U_2) = 1$ for all distinct $U_1, U_2 \in \mathcal{S}$
- $U_1 \cap U_2 \cap U_3 = \{0\}$ for all distinct $U_1, U_2, U_3 \in \mathcal{S}$

$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ quadratic function, e.g.: $x \mapsto x^{2^i+1}$

$B_f(x,a) := f(x+a) + f(x) + f(a) + f(0) \longrightarrow B_f$ is $\mathbb{F}_2$-bilinear

$a \in \mathbb{F}_{2^n}$, $X_f(a) := \{(x, B_f(x,a)) \colon x \in \mathbb{F}_{2^n}\}$, $\qquad \mathcal{S}_f := \{X_f(a) \colon a \in \mathbb{F}_{2^n}\}$

APN functions: a connection to Finite Geometry

$V = V(m,2)$: m-dimensional $\mathbb{F}_2$-vector space

$\mathcal{S}$: family of $(d+1)$-dimensional vector subspaces of V

$\mathcal{S}$ is a d-**dimensional dual hyperoval** if

- $\mathcal{S}$ has exactly $q^d + q^{d-1} + \cdots + q + 2$ elements
- the union of the elements of $\mathcal{S}$ generates V
- $\dim(U_1 \cap U_2) = 1$ for all distinct $U_1, U_2 \in \mathcal{S}$
- $U_1 \cap U_2 \cap U_3 = \{0\}$ for all distinct $U_1, U_2, U_3 \in \mathcal{S}$

$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ quadratic function, e.g.: $x \mapsto x^{2^i+1}$

$B_f(x,a) := f(x+a) + f(x) + f(a) + f(0) \longrightarrow B_f$ is $\mathbb{F}_2$-bilinear

$a \in \mathbb{F}_{2^n}$, $X_f(a) := \{(x, B_f(x,a)) : x \in \mathbb{F}_{2^n}\}$, $\quad \mathcal{S}_f := \{X_f(a) : a \in \mathbb{F}_{2^n}\}$

Theorem

f is APN $\iff$ $\mathcal{S}_f$ is a $(n-1)$-dimensional dual hyperoval in $\mathbb{F}_2^{2n}$

Generalized APN (GAPN) functions

- $q = p^n, \quad f : \mathbb{F}_q \to \mathbb{F}_q$
- $a \in \mathbb{F}_q^*, \quad D_a f : \mathbb{F}_q \to \mathbb{F}_q,\ x \mapsto f(x+a) - f(x)$

Generalized APN (GAPN) functions

- $q = p^n, \quad f : \mathbb{F}_q \to \mathbb{F}_q$
- $a \in \mathbb{F}_q^*, \quad D_a f : \mathbb{F}_q \to \mathbb{F}_q,\ x \mapsto f(x+a) - f(x)$
- $D_a^{(j)} f := D_a D_a^{(j-1)} f$ higher order discrete derivatives in direction a
- $GD_a f := D_a^{(p-1)} f$ **generalized discrete derivative** in direction a

Generalized APN (GAPN) functions

- $q = p^n, \quad f : \mathbb{F}_q \to \mathbb{F}_q$
- $a \in \mathbb{F}_q^*, \quad D_a f : \mathbb{F}_q \to \mathbb{F}_q, \; x \mapsto f(x+a) - f(x)$
- $D_a^{(j)} f := D_a D_a^{(j-1)} f$ higher order discrete derivatives in direction a
- $GD_a f := D_a^{(p-1)} f$ **generalized discrete derivative** in direction a

$$GD_a f(x) = \sum_{i=0}^{p-1} f(x + ia)$$

Generalized APN (GAPN) functions

- $q = p^n, \quad f : \mathbb{F}_q \to \mathbb{F}_q$
- $a \in \mathbb{F}_q^*, \quad D_a f : \mathbb{F}_q \to \mathbb{F}_q,\; x \mapsto f(x+a) - f(x)$
- $D_a^{(j)} f := D_a D_a^{(j-1)} f$ higher order discrete derivatives in direction a
- $GD_a f := D_a^{(p-1)} f$ **generalized discrete derivative** in direction a

$$GD_a f(x) = \sum_{i=0}^{p-1} f(x + ia)$$

- f is APN if $p = 2$ and $GD_a f : \mathbb{F}_q \to \mathbb{F}_q$ is 2-to-1 for every $a \in \mathbb{F}_q^*$

Generalized APN (GAPN) functions

- $q = p^n, \quad f : \mathbb{F}_q \to \mathbb{F}_q$
- $a \in \mathbb{F}_q^*, \quad D_a f : \mathbb{F}_q \to \mathbb{F}_q, \; x \mapsto f(x+a) - f(x)$
- $D_a^{(j)} f := D_a D_a^{(j-1)} f$ higher order discrete derivatives in direction a
- $GD_a f := D_a^{(p-1)} f$ **generalized discrete derivative** in direction a

$$GD_a f(x) = \sum_{i=0}^{p-1} f(x + ia)$$

- f is APN if $p = 2$ and $GD_a f : \mathbb{F}_q \to \mathbb{F}_q$ is 2-to-1 for every $a \in \mathbb{F}_q^*$
- f is Generalized APN (**GAPN**) if

  $p \geq 2$ and $GD_a f : \mathbb{F}_q \to \mathbb{F}_q$ is p-to-1 for every $a \in \mathbb{F}_q^*$,

  i.e.: $GD_a f(x) = b$ has either 0 or p solutions for all $a, b \in \mathbb{F}_q$, $a \neq 0$

Generalized APN (GAPN) functions

- $q = p^n, \quad f : \mathbb{F}_q \to \mathbb{F}_q$
- $a \in \mathbb{F}_q^*, \quad D_a f : \mathbb{F}_q \to \mathbb{F}_q, \; x \mapsto f(x+a) - f(x)$
- $D_a^{(j)} f := D_a D_a^{(j-1)} f$ higher order discrete derivatives in direction a
- $GD_a f := D_a^{(p-1)} f$ **generalized discrete derivative** in direction a

$$GD_a f(x) = \sum_{i=0}^{p-1} f(x + ia)$$

- f is APN if $p = 2$ and $GD_a f : \mathbb{F}_q \to \mathbb{F}_q$ is 2-to-1 for every $a \in \mathbb{F}_q^*$
- f is Generalized APN (**GAPN**) if

  $p \geq 2$ and $GD_a f : \mathbb{F}_q \to \mathbb{F}_q$ is p-to-1 for every $a \in \mathbb{F}_q^*$,

  i.e.: $GD_a f(x) = b$ has either 0 or p solutions for all $a, b \in \mathbb{F}_q$, $a \neq 0$
- if $\bar{x}$ is a solution, then $\bar{x}, \; \bar{x} + a, \; \dots, \; \bar{x} + (p-1)a$ are solutions

GAPN functions: connections

GAPN functions in odd characteristic have connections with

- Dual arcs
- Generalized Almost Bent functions
- other mathematical objects??

GAPN functions: examples

- APN Gold function:

$$\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto x^{2^j+1} \qquad \text{with } \gcd(j,n)=1$$

GAPN functions: examples

- APN Gold function:

$$\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto x^{2^j+1} \qquad \text{with} \ \gcd(j, n) = 1$$

- $f : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n}, \ x \mapsto x^{3^j+2} \quad$ with $\gcd(j, n) = 1$

GAPN functions: examples

- APN Gold function:

$$\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto x^{2^j+1} \qquad \text{with } \gcd(j,n)=1$$

- $f : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n}, \; x \mapsto x^{3^j+2} \quad$ with $\gcd(j,n)=1$

$$GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia) = x^{3^j+2} + (x+a)^{3^j+2} + (x+2a)^{3^j+2}$$

GAPN functions: examples

- APN Gold function:

$$\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto x^{2^j+1} \qquad \text{with } \gcd(j,n)=1$$

- $f : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n}, \; x \mapsto x^{3^j+2}$ with $\gcd(j,n)=1$

$$GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia) = x^{3^j+2} + (x+a)^{3^j+2} + (x+2a)^{3^j+2}$$

$$= x^{3^j+2} + (x^{3^j} + a^{3^j})(x+a)^2 + (x^{3^j} + 2a^{3^j})(x+2a)^2$$

GAPN functions: examples

- APN Gold function:

$$\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto x^{2^j+1} \qquad \text{with } \gcd(j,n)=1$$

- $f : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n},\ x \mapsto x^{3^j+2}$ with $\gcd(j,n)=1$

$$GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia) = x^{3^j+2} + (x+a)^{3^j+2} + (x+2a)^{3^j+2}$$

$$= x^{3^j+2} + (x^{3^j} + a^{3^j})(x+a)^2 + (x^{3^j} + 2a^{3^j})(x+2a)^2$$

$$= 2a^2x^{3^j} + a^{3^j+1}x \qquad \mathbb{F}_3\text{-linearized polynomial}$$

GAPN functions: examples

- APN Gold function:

$$\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto x^{2^j+1} \qquad \text{with } \gcd(j,n)=1$$

- $f : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n}, \; x \mapsto x^{3^j+2}$ with $\gcd(j,n)=1$

$GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia) = x^{3^j+2} + (x+a)^{3^j+2} + (x+2a)^{3^j+2}$

$= x^{3^j+2} + (x^{3^j} + a^{3^j})(x+a)^2 + (x^{3^j} + 2a^{3^j})(x+2a)^2$

$= 2a^2x^{3^j} + a^{3^j+1}x$ $\qquad$ $\mathbb{F}_3$-linearized polynomial

Kernel in $\mathbb{F}_{3^n}$: $\; 2a^2x^{3^j} + a^{3^j+1}x = 0$

GAPN functions: examples

- APN Gold function:

$$\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto x^{2^j+1} \qquad \text{with } \gcd(j,n)=1$$

- $f : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n}, \ x \mapsto x^{3^j+2} \quad$ with $\gcd(j,n)=1$

$$GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia) = x^{3^j+2} + (x+a)^{3^j+2} + (x+2a)^{3^j+2}$$

$$= x^{3^j+2} + (x^{3^j} + a^{3^j})(x+a)^2 + (x^{3^j} + 2a^{3^j})(x+2a)^2$$

$$= 2a^2x^{3^j} + a^{3^j+1}x \qquad \mathbb{F}_3\text{-linearized polynomial}$$

Kernel in $\mathbb{F}_{3^n}$: $\ 2a^2x^{3^j} + a^{3^j+1}x = 0 \quad \Rightarrow \quad (x/a)^{3^j} = x/a$

GAPN functions: examples

- APN Gold function:

$$\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto x^{2^j+1} \qquad \text{with } \gcd(j,n)=1$$

- $f : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n}, \ x \mapsto x^{3^j+2} \quad$ with $\gcd(j,n)=1$

$$GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia) = x^{3^j+2} + (x+a)^{3^j+2} + (x+2a)^{3^j+2}$$

$$= x^{3^j+2} + (x^{3^j} + a^{3^j})(x+a)^2 + (x^{3^j} + 2a^{3^j})(x+2a)^2$$

$$= 2a^2x^{3^j} + a^{3^j+1}x \qquad \mathbb{F}_3\text{-linearized polynomial}$$

Kernel in $\mathbb{F}_{3^n}$: $\ 2a^2x^{3^j} + a^{3^j+1}x = 0 \quad \Rightarrow \quad (x/a)^{3^j} = x/a$

$$\gcd(j,n)=1 \quad \Rightarrow \quad x/a \in \mathbb{F}_{3^n} \cap \mathbb{F}_{3^j} = \mathbb{F}_3$$

GAPN functions: examples

- APN Gold function:

$$\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto x^{2^j+1} \qquad \text{with } \gcd(j,n)=1$$

- $f : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n},\ x \mapsto x^{3^j+2}$ with $\gcd(j,n)=1$

$$GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia) = x^{3^j+2} + (x+a)^{3^j+2} + (x+2a)^{3^j+2}$$

$$= x^{3^j+2} + (x^{3^j} + a^{3^j})(x+a)^2 + (x^{3^j} + 2a^{3^j})(x+2a)^2$$

$$= 2a^2x^{3^j} + a^{3^j+1}x \qquad \mathbb{F}_3\text{-linearized polynomial}$$

Kernel in $\mathbb{F}_{3^n}$: $2a^2x^{3^j} + a^{3^j+1}x = 0 \quad \Rightarrow \quad (x/a)^{3^j} = x/a$

$$\gcd(j,n)=1 \quad \Rightarrow \quad x/a \in \mathbb{F}_{3^n} \cap \mathbb{F}_{3^j} = \mathbb{F}_3$$

Kernel $= \{0, a, 2a\}$ $\Rightarrow$ if $GD_a f(x) = b$ has a solution $\bar{x} \in \mathbb{F}_{3^n}$,

$\{\bar{x}, \bar{x}+a, \bar{x}+2a\}$ are all the solutions in $\mathbb{F}_{3^n}$

GAPN generalized Gold functions

Özbudak-Sălăgean: monomial $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \; x \mapsto x^d$

- $d = k_2 p^{\ell_2} + k_1 p^{\ell_1}$
- $\ell_2 > \ell_1 \geq 0, \quad 0 \leq k_1, k_2 \leq p-1, \quad p-1 < k_1 + k_2 < 2(p-1)$
- $u = k_1 + k_2 - (p-1)$

GAPN generalized Gold functions

Özbudak-Sălăgean: monomial $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $x \mapsto x^d$

- $d = k_2 p^{\ell_2} + k_1 p^{\ell_1}$
- $\ell_2 > \ell_1 \geq 0, \quad 0 \leq k_1, k_2 \leq p-1, \quad p-1 < k_1 + k_2 < 2(p-1)$
- $u = k_1 + k_2 - (p-1)$

If $\gcd(\ell_2 - \ell_1, n) = 1$ and $\gcd(u, p^n - 1) = 1$

$\implies$ f is **GAPN** over $\mathbb{F}_{p^n}$

GAPN generalized Gold functions

Özbudak-Sălăgean: monomial $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $x \mapsto x^d$

- $d = k_2 p^{\ell_2} + k_1 p^{\ell_1}$
- $\ell_2 > \ell_1 \geq 0$, $\quad 0 \leq k_1, k_2 \leq p-1$, $\quad p-1 < k_1 + k_2 < 2(p-1)$
- $u = k_1 + k_2 - (p-1)$

If $\gcd(\ell_2 - \ell_1, n) = 1$ and $\gcd(u, p^n - 1) = 1$

$\implies$ f is **GAPN** over $\mathbb{F}_{p^n}$

Then: $\gcd(\ell_2 - \ell_1, nm) = 1$ and $\gcd(u, p^{nm} - 1) = 1$ for infinitely many m

$\implies$ f is **GAPN** over infinitely many extensions $\mathbb{F}_{p^{nm}}$ of $\mathbb{F}_{p^n}$

GAPN generalized Gold functions

Özbudak-Sălăgean: monomial $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $x \mapsto x^d$

- $d = k_2 p^{\ell_2} + k_1 p^{\ell_1}$
- $\ell_2 > \ell_1 \geq 0, \quad 0 \leq k_1, k_2 \leq p-1, \quad p-1 < k_1 + k_2 < 2(p-1)$
- $u = k_1 + k_2 - (p-1)$

If $\gcd(\ell_2 - \ell_1, n) = 1$ and $\gcd(u, p^n - 1) = 1$

$\implies$ f is **GAPN** over $\mathbb{F}_{p^n}$

Then: $\gcd(\ell_2 - \ell_1, nm) = 1$ and $\gcd(u, p^{nm} - 1) = 1$ for infinitely many m

$\implies$ f is **GAPN** over infinitely many extensions $\mathbb{F}_{p^{nm}}$ of $\mathbb{F}_{p^n}$

f is **exceptional GAPN** over $\mathbb{F}_{p^n}$ $\qquad$ d is a p-**exceptional exponent**

GAPN functions in odd characteristic

Kuroda (2020), Zha-Hu-Zhang (2018), Özbudak-Sălăgean (2021):
families of GAPN functions over $\mathbb{F}_{p^n}$ with p **odd**

GAPN functions in odd characteristic

Kuroda (2020), Zha-Hu-Zhang (2018), Özbudak-Sălăgean (2021):
families of GAPN functions over $\mathbb{F}_{p^n}$ with p **odd**

Monomials $x \mapsto x^d$

- $d = p^n - 2$ inverse function
- $d = tp^{n-1} - 1$
- $d = k_2 p^{\ell_2} + k_1 p^{\ell_1}$ generalized Gold functions, p-exceptional exponent
- $d = 1 + p^{i_2} + \cdots + p^{i_p}$ p-exceptional exponent

GAPN functions in odd characteristic

Kuroda (2020), Zha-Hu-Zhang (2018), Özbudak-Sălăgean (2021):
families of GAPN functions over $\mathbb{F}_{p^n}$ with p **odd**

Monomials $x \mapsto x^d$

- $d = p^n - 2$ inverse function
- $d = tp^{n-1} - 1$
- $d = k_2 p^{\ell_2} + k_1 p^{\ell_1}$ generalized Gold functions, p-exceptional exponent
- $d = 1 + p^{i_2} + \cdots + p^{i_p}$ p-exceptional exponent

Multinomials

- very involved
- Room for new families?

Algebraic degree of a GAPN function, p odd

- $m \geq 0, \quad m = \sum_{i \geq 0} m_i p^i \quad$ p-adic expansion of m
- $w_p(m) := \sum_{i \geq 0} m_i \quad$ p-weight of m

Algebraic degree of a GAPN function, p odd

- $m \geq 0, \quad m = \sum_{i \geq 0} m_i p^i$ p-adic expansion of m
- $w_p(m) := \sum_{i \geq 0} m_i$ p-weight of m
- $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad f(x) = \sum_{j=1}^{p^n-1} a_j x^j$

  $d^0(f) := \max\{w_p(j) \colon a_j \neq 0\} \leq n(p-1)$ **algebraic degree** of f

Algebraic degree of a GAPN function, p odd

- $m \geq 0, \quad m = \sum_{i \geq 0} m_i p^i \quad$ p-adic expansion of m
- $w_p(m) := \sum_{i \geq 0} m_i \quad$ p-weight of m
- $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad f(x) = \sum_{j=1}^{p^n-1} a_j x^j$

  $d^0(f) := \max\{w_p(j) \colon a_j \neq 0\} \leq n(p-1)$ **algebraic degree** of f
- $d^0(f) = 1 \Rightarrow$ **affine** function
- $d^0(f) = 1$ and no constant term $\Rightarrow$ **linear** function

Algebraic degree of a GAPN function, p odd

- $m \geq 0, \quad m = \sum_{i \geq 0} m_i p^i$ $\quad$ p-adic expansion of m
- $w_p(m) := \sum_{i \geq 0} m_i$ $\quad$ p-weight of m
- $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad f(x) = \sum_{j=1}^{p^n-1} a_j x^j$

  $d^0(f) := \max\{w_p(j) \colon a_j \neq 0\} \leq n(p-1)$ $\quad$ **algebraic degree** of f
- $d^0(f) = 1 \Rightarrow$ **affine** function
- $d^0(f) = 1$ and no constant term $\Rightarrow$ **linear** function

Kuroda (2020): monomials $f_d : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \ x \mapsto x^d$

- if $d^0(f_d)$ is even or $d^0(f_d) < p \implies f_d$ is not GAPN
- classification of exceptional GAPN f_d

  for $d^0(f_d) = p$ or $d^0(f_d) = n(p-1) - 1$

Equivalence of GAPN functions

$f_1, f_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

Definition

f and g are generalized extended affine equivalent (**GEA-equivalent**) if

$$f_1 = A_1 \circ f_2 \circ A_2 + g$$

where $A_1, A_2, g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$,

A_1, A_2 are invertible and affine, $\quad d^0(g) \leq p-1$

Theorem

if f_1, f_2 are GEA-equivalent, then f_1 is GAPN $\iff$ f_2 is GAPN

Equivalence of GAPN functions

$f_1, f_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

Definition

f and g are generalized extended affine equivalent (**GEA-equivalent**) if

$$f_1 = A_1 \circ f_2 \circ A_2 + g$$

where $A_1, A_2, g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$,

A_1, A_2 are invertible and affine, $\quad d^0(g) \leq p - 1$

Theorem

if f_1, f_2 are GEA-equivalent, then f_1 is GAPN $\iff$ f_2 is GAPN

CCZ-equivalence: affine equivalence of the graphs (more general)

Equivalence of GAPN functions

$f_1, f_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

Definition

f and g are generalized extended affine equivalent (**GEA-equivalent**) if

$$f_1 = A_1 \circ f_2 \circ A_2 + g$$

where $A_1, A_2, g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$,

A_1, A_2 are invertible and affine, $\quad d^0(g) \leq p - 1$

Theorem

if f_1, f_2 are GEA-equivalent, then f_1 is GAPN $\iff$ f_2 is GAPN

CCZ-equivalence: affine equivalence of the graphs (more general)

CCZ-equivalence preserves the APN property (Budaghyan-Carlet-Pott 2006), but does not preserve the GAPN property when p is odd!

GAPN monomials and permutation polynomials

$f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $GD_a f(x) = \sum_{i=0}^{p-1} f(x + ia)$

GAPN monomials and permutation polynomials

$f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia)$

- $GD_a f(x) = GD_a f(x+ja)$ for all $j \in \mathbb{F}_p$

  $\Rightarrow$ $GD_a f(x)$ is a function in $\prod_{i=0}^{p-1}(x+ja) = x^p - a^{p-1}x$

  $\Rightarrow$ $GD_a f(x) \in \mathbb{F}_{p^n}[x^p - a^{p-1}x]$

GAPN monomials and permutation polynomials

$f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia)$

- $GD_a f(x) = GD_a f(x+ja)$ for all $j \in \mathbb{F}_p$
  $\Rightarrow$ $GD_a f(x)$ is a function in $\prod_{i=0}^{p-1}(x+ja) = x^p - a^{p-1}x$
  $\Rightarrow$ $GD_a f(x) \in \mathbb{F}_{p^n}[x^p - a^{p-1}x]$

- from now on: $f(x) = x^d$ $\Rightarrow$ $GD_a f(x) = a^d GD_1 f(x/a)$
  $GD_a f(x)$ is p-to-1 iff $GDf(x) := GD_1 f(x)$ is p-to-1

GAPN monomials and permutation polynomials

$f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia)$

- $GD_a f(x) = GD_a f(x+ja)$ for all $j \in \mathbb{F}_p$

  $\Rightarrow$ $GD_a f(x)$ is a function in $\prod_{i=0}^{p-1}(x+ja) = x^p - a^{p-1}x$

  $\Rightarrow$ $GD_a f(x) \in \mathbb{F}_{p^n}[x^p - a^{p-1}x]$

- from now on: $f(x) = x^d \Rightarrow GD_a f(x) = a^d GD_1 f(x/a)$

  $GD_a f(x)$ is p-to-1 iff $GDf(x) := GD_1 f(x)$ is p-to-1

  $\Rightarrow$ we can assume $a = 1$ $\Rightarrow$ $GDx^d \in \mathbb{F}_{p^n}[x^p - x]$

$$GDx^d = g(x^p - x), \quad g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$$

GAPN monomials and permutation polynomials

$f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $GD_a f(x) = \sum_{i=0}^{p-1} f(x + ia)$

- $GD_a f(x) = GD_a f(x + ja)$ for all $j \in \mathbb{F}_p$

  $\Rightarrow$ $GD_a f(x)$ is a function in $\prod_{i=0}^{p-1}(x + ja) = x^p - a^{p-1}x$

  $\Rightarrow$ $GD_a f(x) \in \mathbb{F}_{p^n}[x^p - a^{p-1}x]$

- from now on: $f(x) = x^d$ $\Rightarrow$ $GD_a f(x) = a^d GD_1 f(x/a)$

  $GD_a f(x)$ is p-to-1 iff $GDf(x) := GD_1 f(x)$ is p-to-1

  $\Rightarrow$ we can assume $a = 1$ $\Rightarrow$ $GDx^d \in \mathbb{F}_{p^n}[x^p - x]$

$$GDx^d = g(x^p - x), \quad g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$$

  if $g(\bar{y}) = b \Rightarrow GDf(x) = b$ has zero or p solutions $\bar{y} + j$, $j \in \mathbb{F}_p$

GAPN monomials and permutation polynomials

$f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $GD_a f(x) = \sum_{i=0}^{p-1} f(x+ia)$

- $GD_a f(x) = GD_a f(x+ja)$ for all $j \in \mathbb{F}_p$
  $\Rightarrow$ $GD_a f(x)$ is a function in $\prod_{i=0}^{p-1}(x+ja) = x^p - a^{p-1}x$
  $\Rightarrow$ $GD_a f(x) \in \mathbb{F}_{p^n}[x^p - a^{p-1}x]$

- from now on: $f(x) = x^d$ $\Rightarrow$ $GD_a f(x) = a^d GD_1 f(x/a)$
  $GD_a f(x)$ is p-to-1 iff $GDf(x) := GD_1 f(x)$ is p-to-1
  $\Rightarrow$ we can assume $a = 1$ $\Rightarrow$ $GDx^d \in \mathbb{F}_{p^n}[x^p - x]$

$$GDx^d = g(x^p - x), \quad g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$$

if $g(\bar{y}) = b \Rightarrow GDf(x) = b$ has zero or p solutions $\bar{y} + j$, $j \in \mathbb{F}_p$

Theorem

*if g is a **permutation polynomial** of $\mathbb{F}_{p^n} \Longrightarrow x^d$ is **GAPN** over $\mathbb{F}_{p^n}$*

GAPN monomials and algebraic curves

$f(x) = x^d$ is GAPN iff GDf is p-to-1, $\qquad GDf(x) = g(x^p - x)$

GAPN monomials and algebraic curves

$f(x) = x^d$ is GAPN iff GDf is p-to-1, $\quad GDf(x) = g(x^p - x)$

- $g(x^p - x) = g(y^p - y)$ is satisfied for $x - y = \alpha \in \mathbb{F}_p$

GAPN monomials and algebraic curves

$f(x) = x^d$ is GAPN iff GDf is p-to-1, $\quad GDf(x) = g(x^p - x)$

- $g(x^p - x) = g(y^p - y)$ is satisfied for $x - y = \alpha \in \mathbb{F}_p$

  $\Rightarrow$ $X - Y - \alpha$ is a factor of $g(X^p - X) - g(Y^p - Y) \in \mathbb{F}_{p^n}[X, Y]$

GAPN monomials and algebraic curves

$f(x) = x^d$ is GAPN iff GDf is p-to-1, $\quad GDf(x) = g(x^p - x)$

- $g(x^p - x) = g(y^p - y)$ is satisfied for $x - y = \alpha \in \mathbb{F}_p$

  $\Rightarrow$ $X - Y - \alpha$ is a factor of $g(X^p - X) - g(Y^p - Y) \in \mathbb{F}_{p^n}[X, Y]$

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X - Y)^p - (X - Y)} = 0$$

GAPN monomials and algebraic curves

$f(x) = x^d$ is GAPN iff GDf is p-to-1, $\qquad GDf(x) = g(x^p - x)$

- $g(x^p - x) = g(y^p - y)$ is satisfied for $x - y = \alpha \in \mathbb{F}_p$

  $\Rightarrow$ $X - Y - \alpha$ is a factor of $g(X^p - X) - g(Y^p - Y) \in \mathbb{F}_{p^n}[X, Y]$

$$\mathcal{C} : \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X - Y)^p - (X - Y)} = 0$$

- GAPN: if $\bar{x}, \bar{y} \in \mathbb{F}_{p^n}$, $g(\bar{x}^p - \bar{x}) = g(\bar{y}^p - \bar{y}) \Rightarrow \bar{x} - \bar{y} \in \mathbb{F}_p$

GAPN monomials and algebraic curves

$f(x) = x^d$ is GAPN iff GDf is p-to-1, $\quad GDf(x) = g(x^p - x)$

- $g(x^p - x) = g(y^p - y)$ is satisfied for $x - y = \alpha \in \mathbb{F}_p$

  $\Rightarrow$ $X - Y - \alpha$ is a factor of $g(X^p - X) - g(Y^p - Y) \in \mathbb{F}_{p^n}[X, Y]$

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X - Y)^p - (X - Y)} = 0$$

- GAPN: if $\bar{x}, \bar{y} \in \mathbb{F}_{p^n}$, $g(\bar{x}^p - \bar{x}) = g(\bar{y}^p - \bar{y}) \Rightarrow \bar{x} - \bar{y} \in \mathbb{F}_p$

Theorem

$f(x) = x^d$ is GAPN over $\mathbb{F}_{p^n}$ $\iff$ every affine $\mathbb{F}_{p^n}$-rational point $(\bar{x}, \bar{y})$ of the curve $\mathcal{C}$ lies on the line $X - Y = \alpha$ for some $\alpha \in \mathbb{F}_p$

GAPN monomials and algebraic curves curves

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X-Y)^p - (X-Y)} = 0$$

Theorem

$f(x) = x^d$ is GAPN over $\mathbb{F}_{p^n}$ $\iff$ every affine $\mathbb{F}_{p^n}$-rational point $(\bar{x}, \bar{y})$ of the curve $\mathcal{C}$ lies on the line $X - Y = \alpha$ for some $\alpha \in \mathbb{F}_p$

GAPN monomials and algebraic curves curves

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X-Y)^p - (X-Y)} = 0$$

Theorem

$f(x) = x^d$ is GAPN over $\mathbb{F}_{p^n}$ $\iff$ every affine $\mathbb{F}_{p^n}$-rational point $(\bar{x}, \bar{y})$ of the curve $\mathcal{C}$ lies on the line $X - Y = \alpha$ for some $\alpha \in \mathbb{F}_p$

Find necessary conditions for GAPN monomials:

GAPN monomials and algebraic curves curves

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X-Y)^p - (X-Y)} = 0$$

Theorem

$f(x) = x^d$ is GAPN over $\mathbb{F}_{p^n}$ $\iff$ every affine $\mathbb{F}_{p^n}$-rational point $(\bar{x}, \bar{y})$ of the curve $\mathcal{C}$ lies on the line $X - Y = \alpha$ for some $\alpha \in \mathbb{F}_p$

Find necessary conditions for GAPN monomials: **if**

- $\mathcal{C}$ has an absolutely irreducible component $\mathcal{A}$ defined over $\mathbb{F}_{p^n}$ and not contained in the lines $X - Y = \alpha \in \mathbb{F}_p$
- $\mathcal{A}$ has small genus g with respect to p^n (true when $d << p^n$)

GAPN monomials and algebraic curves curves

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X-Y)^p - (X-Y)} = 0$$

Theorem

$f(x) = x^d$ is GAPN over $\mathbb{F}_{p^n}$ $\iff$ every affine $\mathbb{F}_{p^n}$-rational point $(\bar{x}, \bar{y})$ of the curve $\mathcal{C}$ lies on the line $X - Y = \alpha$ for some $\alpha \in \mathbb{F}_p$

Find necessary conditions for GAPN monomials: **if**

- $\mathcal{C}$ has an absolutely irreducible component $\mathcal{A}$ defined over $\mathbb{F}_{p^n}$ and not contained in the lines $X - Y = \alpha \in \mathbb{F}_p$
- $\mathcal{A}$ has small genus g with respect to p^n (true when $d << p^n$)

Then by **Hasse-Weil** bound on N = number of $\mathbb{F}_{p^n}$-rat. points of $\mathcal{A} \subseteq \mathcal{C}$

$$N \geq p^n + 1 - 2 \cdot g \cdot \sqrt{p^n} >> 0$$

$\Rightarrow \mathcal{C}$ has affine $\mathbb{F}_{p^n}$-rational points $(\bar{x}, \bar{y})$ off the lines $X - Y \in \mathbb{F}_p$

GAPN monomials and algebraic curves curves

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X-Y)^p - (X-Y)} = 0$$

Theorem

$f(x) = x^d$ is GAPN over $\mathbb{F}_{p^n}$ $\iff$ every affine $\mathbb{F}_{p^n}$-rational point $(\bar{x}, \bar{y})$ of the curve $\mathcal{C}$ lies on the line $X - Y = \alpha$ for some $\alpha \in \mathbb{F}_p$

Find necessary conditions for GAPN monomials: **if**

- $\mathcal{C}$ has an absolutely irreducible component $\mathcal{A}$ defined over $\mathbb{F}_{p^n}$ and not contained in the lines $X - Y = \alpha \in \mathbb{F}_p$
- $\mathcal{A}$ has small genus g with respect to p^n (true when $d << p^n$)

Then by **Hasse-Weil** bound on N = number of $\mathbb{F}_{p^n}$-rat. points of $\mathcal{A} \subseteq \mathcal{C}$

$$N \geq p^n + 1 - 2 \cdot g \cdot \sqrt{p^n} >> 0$$

$\Rightarrow \mathcal{C}$ has affine $\mathbb{F}_{p^n}$-rational points $(\bar{x}, \bar{y})$ off the lines $X - Y \in \mathbb{F}_p$

$\Longrightarrow f(x) = x^d$ is **not** GAPN over $\mathbb{F}_{p^n}$

A double Artin-Schreier extension on an easier curve

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X^p - X) - (Y^p - Y)} = 0$$

A double Artin-Schreier extension on an easier curve

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X^p - X) - (Y^p - Y)} = 0 \qquad \mathcal{E}: \quad E(U, V) = \frac{g(U) - g(V)}{U - V} = 0$$

A double Artin-Schreier extension on an easier curve

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X^p - X) - (Y^p - Y)} = 0 \qquad \mathcal{E}: \quad E(U,V) = \frac{g(U) - g(V)}{U - V} = 0$$

$$\mathcal{C}: \begin{cases} Y^p - Y = V \\ X^p - X = U \\ E(U,V) = 0 \end{cases}$$

A double Artin-Schreier extension on an easier curve

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X^p - X) - (Y^p - Y)} = 0 \qquad \mathcal{E}: \quad E(U,V) = \frac{g(U) - g(V)}{U - V} = 0$$

$$\mathcal{C}: \begin{cases} Y^p - Y = V \\ X^p - X = U \\ E(U,V) = 0 \end{cases}$$

(Bartoli-Giulietti-Peraro-Z.) If

- $p \nmid \deg(g)$
- $\mathcal{E}$ has an absolutely irreducible component $\mathcal{Z}$ such that
  - $\mathcal{Z}$ is defined over $\mathbb{F}_{p^n}$
  - $\mathcal{Z}$ has at least one point at infinity P_∞ not $\mathbb{F}_p$-rational

Then $\mathcal{C}$ has an absolutely irreducible component
defined over $\mathbb{F}_{p^n}$ and not contained in the lines $X - Y \in \mathbb{F}_p$

A double Artin-Schreier extension on an easier curve

$$\mathcal{C}: \quad \frac{g(X^p - X) - g(Y^p - Y)}{(X^p - X) - (Y^p - Y)} = 0 \qquad \mathcal{E}: \quad E(U,V) = \frac{g(U) - g(V)}{U - V} = 0$$

$$\mathcal{C}: \begin{cases} Y^p - Y = V \\ X^p - X = U \\ E(U,V) = 0 \end{cases}$$

(Bartoli-Giulietti-Peraro-Z.) If

- $p \nmid \deg(g)$
- $\mathcal{E}$ has an absolutely irreducible component $\mathcal{Z}$ such that
  - $\mathcal{Z}$ is defined over $\mathbb{F}_{p^n}$
  - $\mathcal{Z}$ has at least one point at infinity P_∞ not $\mathbb{F}_p$-rational

Then $\mathcal{C}$ has an absolutely irreducible component defined over $\mathbb{F}_{p^n}$ and not contained in the lines $X - Y \in \mathbb{F}_p$

(Tools: Artin-Schreier extensions of function fields)

Necessary conditions for GAPN monomials

$\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^d, \qquad GDx^d = g(x^p - x)$

Özbudak-Sălăgean: g permutation of $\mathbb{F}_{p^n} \implies x^d$ GAPN over $\mathbb{F}_{p^n}$

Necessary conditions for GAPN monomials

$\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^d, \qquad GDx^d = g(x^p - x)$

Özbudak-Sălăgean: $\qquad g$ permutation of $\mathbb{F}_{p^n} \implies x^d$ GAPN over $\mathbb{F}_{p^n}$

Conversely, using the previous result:

Theorem

If $\quad p \nmid \deg(g), \qquad \gcd(\deg(g), p-1) = 1, \qquad \deg(g) \leq p^{n/4-1},$

Then: $\qquad x^d$ *GAPN over* $\mathbb{F}_{p^n} \implies g$ *permutation of* $\mathbb{F}_{p^n}$

Necessary conditions for GAPN monomials

$\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^d, \qquad GDx^d = g(x^p - x)$

Özbudak-Sălăgean: $\qquad g$ permutation of $\mathbb{F}_{p^n} \implies x^d$ GAPN over $\mathbb{F}_{p^n}$

Conversely, using the previous result:

Theorem

If $\qquad p \nmid \deg(g), \qquad \gcd(\deg(g), p-1) = 1, \qquad \deg(g) \leq p^{n/4-1},$

Then: $\qquad x^d$ *GAPN over* $\mathbb{F}_{p^n} \implies g$ *permutation of* $\mathbb{F}_{p^n}$

Proof: g not a permutation

Necessary conditions for GAPN monomials

$\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^d, \qquad GDx^d = g(x^p - x)$

Özbudak-Sălăgean: $\qquad g$ permutation of $\mathbb{F}_{p^n} \implies x^d$ GAPN over $\mathbb{F}_{p^n}$

Conversely, using the previous result:

Theorem

If $\quad p \nmid \deg(g), \qquad \gcd(\deg(g), p-1) = 1, \qquad \deg(g) \leq p^{n/4-1}$,

Then: $\quad x^d$ *GAPN over* $\mathbb{F}_{p^n} \implies g$ *permutation of* $\mathbb{F}_{p^n}$

Proof: g not a permutation $\implies \mathcal{E} : \frac{g(U)-g(V)}{U-V} = 0$ has an abs. irreducible $\mathbb{F}_{p^n}$-rational component $\mathcal{Z}$ with a simple non-$\mathbb{F}_p$-rational point at infinity

Necessary conditions for GAPN monomials

$\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^d, \qquad GDx^d = g(x^p - x)$

Özbudak-Sălăgean: g permutation of $\mathbb{F}_{p^n} \implies x^d$ GAPN over $\mathbb{F}_{p^n}$

Conversely, using the previous result:

Theorem

If $p \nmid \deg(g), \qquad \gcd(\deg(g), p-1) = 1, \qquad \deg(g) \leq p^{n/4-1}$,

Then: x^d *GAPN over* $\mathbb{F}_{p^n} \implies g$ *permutation of* $\mathbb{F}_{p^n}$

Proof: g not a permutation $\implies \mathcal{E} : \frac{g(U)-g(V)}{U-V} = 0$ has an abs. irreducible $\mathbb{F}_{p^n}$-rational component $\mathcal{Z}$ with a simple non-$\mathbb{F}_p$-rational point at infinity

$\implies \mathcal{C} : \frac{g(X^p-X)-g(Y^p-Y)}{(X^p-X)-(Y^p-Y)} = 0$ has an abs. irred. $\mathbb{F}_{p^n}$-rational component with $\mathbb{F}_{p^n}$-rational points off the lines $X - Y \in \mathbb{F}_p$

Necessary conditions for GAPN monomials

$\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^d, \qquad GDx^d = g(x^p - x)$

Özbudak-Sălăgean: $\quad g$ permutation of $\mathbb{F}_{p^n} \implies x^d$ GAPN over $\mathbb{F}_{p^n}$

Conversely, using the previous result:

Theorem

If $\quad p \nmid \deg(g), \qquad \gcd(\deg(g), p-1) = 1, \qquad \deg(g) \leq p^{n/4-1},$

Then: $\quad x^d$ *GAPN over* $\mathbb{F}_{p^n} \implies g$ *permutation of* $\mathbb{F}_{p^n}$

Proof: g not a permutation $\implies \mathcal{E} : \frac{g(U)-g(V)}{U-V} = 0$ has an abs. irreducible $\mathbb{F}_{p^n}$-rational component $\mathcal{Z}$ with a simple non-$\mathbb{F}_p$-rational point at infinity $\implies \mathcal{C} : \frac{g(X^p-X)-g(Y^p-Y)}{(X^p-X)-(Y^p-Y)} = 0$ has an abs. irred. $\mathbb{F}_{p^n}$-rational component with $\mathbb{F}_{p^n}$-rational points off the lines $X - Y \in \mathbb{F}_p \implies x^d$ is not GAPN

Necessary conditions for GAPN monomials

$\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^d, \qquad GDx^d = g(x^p - x)$

Özbudak-Sălăgean: $\qquad g$ permutation of $\mathbb{F}_{p^n} \implies x^d$ GAPN over $\mathbb{F}_{p^n}$

Conversely, using the previous result:

Theorem *If* $\quad p \nmid \deg(g), \qquad \deg(g) \leq p^{n/4-1},$

Then: x^d *GAPN over* $\mathbb{F}_{p^n} \implies \gcd(\deg(g), p^n - 1) = \gcd(\deg(g), p - 1)$

Necessary conditions for GAPN monomials

$\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^d, \qquad GDx^d = g(x^p - x)$

Özbudak-Sălăgean: $\qquad g$ permutation of $\mathbb{F}_{p^n} \implies x^d$ GAPN over $\mathbb{F}_{p^n}$

Conversely, using the previous result:

Theorem $\qquad$ *If* $\quad p \nmid \deg(g), \qquad \deg(g) \le p^{n/4-1},$

Then: x^d *GAPN over* $\mathbb{F}_{p^n} \implies \gcd(\deg(g), p^n - 1) = \gcd(\deg(g), p - 1)$

Sketch of the **proof:** $\qquad$ if $\gcd(\deg(g), p^n - 1) > \gcd(\deg(g), p - 1)$

$\implies \mathcal{E} : \frac{g(U)-g(V)}{U-V} = 0$ has a simple $\mathbb{F}_{p^n} \setminus \mathbb{F}_p$-rational point P

Necessary conditions for GAPN monomials

$\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^d, \qquad GDx^d = g(x^p - x)$

Özbudak-Sălăgean: g permutation of $\mathbb{F}_{p^n} \implies x^d$ GAPN over $\mathbb{F}_{p^n}$

Conversely, using the previous result:

Theorem

If $\quad p \nmid \deg(g), \qquad \deg(g) \leq p^{n/4-1},$

Then: x^d *GAPN over* $\mathbb{F}_{p^n} \implies \gcd(\deg(g), p^n - 1) = \gcd(\deg(g), p - 1)$

Sketch of the **proof:** if $\gcd(\deg(g), p^n - 1) > \gcd(\deg(g), p - 1)$

$\implies \mathcal{E} : \frac{g(U)-g(V)}{U-V} = 0$ has a simple $\mathbb{F}_{p^n} \setminus \mathbb{F}_p$-rational point P

$\implies \mathcal{E}$ has an abs. irreducible $\mathbb{F}_{p^n}$-rational component through P

not in the line $U - V = 0$

GAPN: an open field

GAPN functions: much more is unkown than for APN functions!

GAPN: an open field

GAPN functions: much more is unkown than for APN functions!

- classify exceptional GAPN monomials
- $GDx^d = g(x^{p^i} - x)$

  $d \longleftrightarrow$ permutation properties of $g \quad \Longrightarrow \quad$ GAPN monomials
- likely room for new GAPN multinomials
- use algebraic curves

Thank you for your attention!