On vectorial functions mapping strict affine subspaces of their domain into strict affine subspaces of their co-domain, and the strong D-property

Enrico Piccione[1]
(Joint work with Claude Carlet[1,2])

[1]University of Bergen, [2]University of Paris 8

Selmer Seminar
January 22, 2024

Overview

1. Preliminaries and Introduction
2. Restricting vectorial functions to affine spaces
3. Restricting (N, N)-functions over affine hyperplanes and the strong D-property
4. Revisiting two infinite families of differentially 4-uniform $(N-1, N-1)$-permutations
5. Conclusions

Preliminaries and Introduction

$\mathbb{F}_{2^N}$ is the finite field of order 2^N

$\mathbb{F}_2^N$ is a vector space over $\mathbb{F}_2$

$\mathrm{Tr}_N(x) = x + x^2 + \cdots + x^{2^{N-1}}$ is the (absolute) trace function over $\mathbb{F}_{2^N}$.
We also write $\mathrm{Tr} = \mathrm{Tr}_N$

A set $A \subseteq \mathbb{F}_2^N$ is called affine if $x + y + z \in A$ for all $x, y, z \in A$.

The dimension of A is given by the dimension of the vector space $a + A$ for any $a \in A$

Vectorial Boolean functions

$\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$ Vectorial Boolean functions $\mathbb{F}_2^N \to \mathbb{F}_2^M$ (occasionally F, G, H)

If $N = M$, we can represent a function as a polynomial in $\mathbb{F}_{2^N}[x]$ of degree strictly less than 2^N (univariate representation).

$W_{\mathcal{F}}(u, v) = \sum_{x \in \mathbb{F}_2^N} (-1)^{v \cdot \mathcal{F}(x) + u \cdot x}$ Walsh transform evaluated in $u \in \mathbb{F}_2^N$ $v \in \mathbb{F}_2^M$

$\mathrm{nl}(\mathcal{F}) = 2^{N-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^N, v \in \mathbb{F}_2^M \setminus \{0\}} |W_{\mathcal{F}}(u, v)|$ Nonlinearity

$D_a\mathcal{F}(x) = \mathcal{F}(x + a) + \mathcal{F}(x)$ derivative through direction $a \in \mathbb{F}_2^N \setminus \{0\}$.

$\delta_{\mathcal{F}} = \max_{a \in \mathbb{F}_2^N \setminus \{0\}, b \in \mathbb{F}_2^M} \left| \{x \in \mathbb{F}_2^N \mid D_a\mathcal{F}(x) = b\} \right|$ Differential Uniformity.

$\mathcal{F}$ is called δ-uniform if $\delta_{\mathcal{F}} \leq \delta$.

2-uniform functions are called APN.

Vectorial Boolean functions

$\mathcal{F}, \mathcal{G}, \mathcal{H}$ Vectorial Boolean functions $\mathbb{F}_2^N \to \mathbb{F}_2^M$ (occasionally F, G, H)
If $N = M$, we can represent a function as a polynomial in $\mathbb{F}_{2^N}[x]$ of degree strictly less than 2^N (univariate representation).

$W_{\mathcal{F}}(u, v) = \sum_{x \in \mathbb{F}_2^N} (-1)^{v \cdot \mathcal{F}(x) + u \cdot x}$ Walsh transform evaluated in $u \in \mathbb{F}_2^N$ $v \in \mathbb{F}_2^M$
$\mathrm{nl}(\mathcal{F}) = 2^{N-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^N, v \in \mathbb{F}_2^M \setminus \{0\}} |W_{\mathcal{F}}(u, v)|$ Nonlinearity
$D_a\mathcal{F}(x) = \mathcal{F}(x + a) + \mathcal{F}(x)$ derivative through direction $a \in \mathbb{F}_2^N \setminus \{0\}$.
$\delta_{\mathcal{F}} = \max_{a \in \mathbb{F}_2^N \setminus \{0\}, b \in \mathbb{F}_2^M} \left| \{x \in \mathbb{F}_2^N \mid D_a\mathcal{F}(x) = b\} \right|$ Differential Uniformity.
$\mathcal{F}$ is called δ-uniform if $\delta_{\mathcal{F}} \leq \delta$.
2-uniform functions are called APN.

Vectorial Boolean functions

$\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$ Vectorial Boolean functions $\mathbb{F}_2^N \to \mathbb{F}_2^M$ (occasionally F, G, H)
If $N = M$, we can represent a function as a polynomial in $\mathbb{F}_{2^N}[x]$ of degree strictly less than 2^N (univariate representation).

$W_{\mathcal{F}}(u, v) = \sum_{x \in \mathbb{F}_2^N} (-1)^{v \cdot \mathcal{F}(x) + u \cdot x}$ Walsh transform evaluated in $u \in \mathbb{F}_2^N$ $v \in \mathbb{F}_2^M$
$\mathrm{nl}(\mathcal{F}) = 2^{N-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^N, v \in \mathbb{F}_2^M \setminus \{0\}} |W_{\mathcal{F}}(u, v)|$ Nonlinearity
$D_a\mathcal{F}(x) = \mathcal{F}(x + a) + \mathcal{F}(x)$ derivative through direction $a \in \mathbb{F}_2^N \setminus \{0\}$.
$\delta_{\mathcal{F}} = \max_{a \in \mathbb{F}_2^N \setminus \{0\}, b \in \mathbb{F}_2^M} \left| \{x \in \mathbb{F}_2^N \mid D_a\mathcal{F}(x) = b\} \right|$ Differential Uniformity.
$\mathcal{F}$ is called δ-uniform if $\delta_{\mathcal{F}} \leq \delta$.
2-uniform functions are called APN.

Equivalence relations

$\mathbb{1}_{\mathcal{F}}(x, y) = 1$ if $y = \mathcal{F}(x)$ and $\mathbb{1}_{\mathcal{F}}(x, y) = 0$ otherwise.

$\mathcal{F}$ and $\mathcal{F}'$ are

Affine equivalent if $\exists \mathcal{A}_1, \mathcal{A}_2$ affine permutations: $\mathcal{F} = \mathcal{A}_1 \circ \mathcal{F}' \circ \mathcal{A}_2$,
EA equivalent if $\exists \mathcal{A}$ affine: $\mathcal{F} + \mathcal{A}$ and $\mathcal{F}'$ are Affine equivalent,
CCZ equivalent if $\mathbb{1}_{\mathcal{F}}$ and $\mathbb{1}_{\mathcal{F}'}$ are Affine equivalent.

Introduction

Let $\mathcal{F}$ be permutation polynomial over $\mathbb{F}_{2^N}$.

Let $A \subseteq \mathbb{F}_{2^N}$ n-dimensional ($n < N$) affine subspace such that $\mathcal{F}(A) = A'$ is an affine space.

Then we construct a permutation polynomial $F = \mathcal{F}_A$ by identifying A and A' with $\mathbb{F}_{2^n}$.

- If $\mathcal{F}$ belongs to an infinite family of functions, we could construct an infinite family of functions F.
- Cryptographic properties of F depends on $\mathcal{F}$.

This is possible because we are restricting over an affine space.
We can have more flexibility:

- $\mathcal{F}$ being an (N, M)-function
- $\mathcal{F}(A) \subseteq A'$
- $A' \subseteq \mathbb{F}_2^M$ being m-dimensional ($m < M$)

Introduction

Let $\mathcal{F}$ be permutation polynomial over $\mathbb{F}_{2^N}$.

Let $A \subseteq \mathbb{F}_{2^N}$ n-dimensional ($n < N$) affine subspace such that $\mathcal{F}(A) = A'$ is an affine space.

Then we construct a permutation polynomial $F = \mathcal{F}_A$ by identifying A and A' with $\mathbb{F}_{2^n}$.

- If $\mathcal{F}$ belongs to an infinite family of functions, we could construct an infinite family of functions F.
- Cryptographic properties of F depends on $\mathcal{F}$.

This is possible because we are restricting over an affine space.
We can have more flexibility:

- $\mathcal{F}$ being an (N, M)-function
- $\mathcal{F}(A) \subseteq A'$
- $A' \subseteq \mathbb{F}_2^M$ being m-dimensional ($m < M$)

Introduction

Let $\mathcal{F}$ be permutation polynomial over $\mathbb{F}_{2^N}$.

Let $A \subseteq \mathbb{F}_{2^N}$ n-dimensional $(n < N)$ affine subspace such that $\mathcal{F}(A) = A'$ is an affine space.

Then we construct a permutation polynomial $F = \mathcal{F}_A$ by identifying A and A' with $\mathbb{F}_{2^n}$.

- If $\mathcal{F}$ belongs to an infinite family of functions, we could construct an infinite family of functions F.
- Cryptographic properties of F depends on $\mathcal{F}$.

This is possible because we are restricting over an affine space.
We can have more flexibility:

- $\mathcal{F}$ being an (N, M)-function
- $\mathcal{F}(A) \subseteq A'$
- $A' \subseteq \mathbb{F}_2^M$ being m-dimensional $(m < M)$

Introduction

Let $\mathcal{F}$ be permutation polynomial over $\mathbb{F}_{2^N}$.

Let $A \subseteq \mathbb{F}_{2^N}$ n-dimensional ($n < N$) affine subspace such that $\mathcal{F}(A) = A'$ is an affine space.

Then we construct a permutation polynomial $F = \mathcal{F}_A$ by identifying A and A' with $\mathbb{F}_{2^n}$.

- If $\mathcal{F}$ belongs to an infinite family of functions, we could construct an infinite family of functions F.
- Cryptographic properties of F depends on $\mathcal{F}$.

This is possible because we are restricting over an affine space.
We can have more flexibility:

- $\mathcal{F}$ being an (N, M)-function
- $\mathcal{F}(A) \subseteq A'$
- $A' \subseteq \mathbb{F}_2^M$ being m-dimensional ($m < M$)

Introduction

Let $\mathcal{F}$ be permutation polynomial over $\mathbb{F}_{2^N}$.

Let $A \subseteq \mathbb{F}_{2^N}$ n-dimensional ($n < N$) affine subspace such that $\mathcal{F}(A) = A'$ is an affine space.

Then we construct a permutation polynomial $F = \mathcal{F}_A$ by identifying A and A' with $\mathbb{F}_{2^n}$.

- If $\mathcal{F}$ belongs to an infinite family of functions, we could construct an infinite family of functions F.
- Cryptographic properties of F depends on $\mathcal{F}$.

This is possible because we are restricting over an affine space.
We can have more flexibility:

- $\mathcal{F}$ being an (N, M)-function
- $\mathcal{F}(A) \subseteq A'$
- $A' \subseteq \mathbb{F}_2^M$ being m-dimensional ($m < M$)

Introduction

Let $\mathcal{F}$ be permutation polynomial over $\mathbb{F}_{2^N}$.

Let $A \subseteq \mathbb{F}_{2^N}$ n-dimensional ($n < N$) affine subspace such that $\mathcal{F}(A) = A'$ is an affine space.

Then we construct a permutation polynomial $F = \mathcal{F}_A$ by identifying A and A' with $\mathbb{F}_{2^n}$.

- If $\mathcal{F}$ belongs to an infinite family of functions, we could construct an infinite family of functions F.
- Cryptographic properties of F depends on $\mathcal{F}$.

This is possible because we are restricting over an affine space.

We can have more flexibility:

- $\mathcal{F}$ being an (N, M)-function
- $\mathcal{F}(A) \subseteq A'$
- $A' \subseteq \mathbb{F}_2^M$ being m-dimensional $(m < M)$

Introduction

Let $\mathcal{F}$ be permutation polynomial over $\mathbb{F}_{2^N}$.

Let $A \subseteq \mathbb{F}_{2^N}$ n-dimensional ($n < N$) affine subspace such that $\mathcal{F}(A) = A'$ is an affine space.

Then we construct a permutation polynomial $F = \mathcal{F}_A$ by identifying A and A' with $\mathbb{F}_{2^n}$.

- If $\mathcal{F}$ belongs to an infinite family of functions, we could construct an infinite family of functions F.
- Cryptographic properties of F depends on $\mathcal{F}$.

This is possible because we are restricting over an affine space.
We can have more flexibility:

- $\mathcal{F}$ being an (N, M)-function
- $\mathcal{F}(A) \subseteq A'$
- $A' \subseteq \mathbb{F}_2^M$ being m-dimensional ($m < M$)

Aim of the paper

- Study the cryptographic properties of functions mapping affine spaces to affine spaces
- Construct new "good" functions (and families)
- Study the D-property further

Aim of the paper

- Study the cryptographic properties of functions mapping affine spaces to affine spaces
- Construct new "good" functions (and families)
- Study the D-property further

Aim of the paper

- Study the cryptographic properties of functions mapping affine spaces to affine spaces
- Construct new "good" functions (and families)
- Study the D-property further

Previous works on the topic

- 1st and 2nd Poisson's summation formula[1]
- Trimming of APN functions[2]
- Taniguchi's introduction of the D-property[3]
- Two infinite families of 4-uniform permutations[4][5]

---

[1] Claude Carlet. "Boolean functions for cryptography and coding theory". In: (2021).

[2] Christof Beierle, Gregor Leander, and Léo Perrin. "Trims and extensions of quadratic APN functions". In: *Designs, Codes and Cryptography* 90.4 (2022), pp. 1009–1036.

[3] Hiroaki Taniguchi. "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$". In: *Cryptography and Communications* (2023), pp. 1–21.

[4] Claude Carlet. "On known and new differentially uniform functions". In: *Australasian Conference on Information Security and Privacy*. Springer. 2011, pp. 1–15.

[5] Yongqiang Li and Mingsheng Wang. "Constructing differentially 4-uniform permutations over $GF(2^{2m})$ from quadratic APN permutations over $GF(2^{2m+1})$". In: *Designs, codes and cryptography* 72.2 (2014), pp. 249–264.

Previous works on the topic

- 1st and 2nd Poisson's summation formula[1]
- Trimming of APN functions[2]
- Taniguchi's introduction of the D-property[3]
- Two infinite families of 4-uniform permutations[4][5]

[1] Claude Carlet. "Boolean functions for cryptography and coding theory". In: (2021).

[2] Christof Beierle, Gregor Leander, and Léo Perrin. "Trims and extensions of quadratic APN functions". In: *Designs, Codes and Cryptography* 90.4 (2022), pp. 1009–1036.

[3] Hiroaki Taniguchi. "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$". In: *Cryptography and Communications* (2023), pp. 1–21.

[4] Claude Carlet. "On known and new differentially uniform functions". In: *Australasian Conference on Information Security and Privacy*. Springer. 2011, pp. 1–15.

[5] Yongqiang Li and Mingsheng Wang. "Constructing differentially 4-uniform permutations over $GF(2^{2m})$ from quadratic APN permutations over $GF(2^{2m+1})$". In: *Designs, codes and cryptography* 72.2 (2014), pp. 249–264.

Previous works on the topic

- 1st and 2nd Poisson's summation formula[1]
- Trimming of APN functions[2]
- Taniguchi's introduction of the D-property[3]
- Two infinite families of 4-uniform permutations[4][5]

[1] Claude Carlet. "Boolean functions for cryptography and coding theory". In: (2021).
[2] Christof Beierle, Gregor Leander, and Léo Perrin. "Trims and extensions of quadratic APN functions". In: *Designs, Codes and Cryptography* 90.4 (2022), pp. 1009–1036.
[3] Hiroaki Taniguchi. "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$". In: *Cryptography and Communications* (2023), pp. 1–21.
[4] Claude Carlet. "On known and new differentially uniform functions". In: *Australasian Conference on Information Security and Privacy*. Springer. 2011, pp. 1–15.
[5] Yongqiang Li and Mingsheng Wang. "Constructing differentially 4-uniform permutations over $GF(2^{2m})$ from quadratic APN permutations over $GF(2^{2m+1})$". In: *Designs, codes and cryptography* 72.2 (2014), pp. 249–264.

Previous works on the topic

- 1st and 2nd Poisson's summation formula[1]
- Trimming of APN functions[2]
- Taniguchi's introduction of the D-property[3]
- Two infinite families of 4-uniform permutations[4][5]

[1] Claude Carlet. "Boolean functions for cryptography and coding theory". In: (2021).
[2] Christof Beierle, Gregor Leander, and Léo Perrin. "Trims and extensions of quadratic APN functions". In: *Designs, Codes and Cryptography* 90.4 (2022), pp. 1009–1036.
[3] Hiroaki Taniguchi. "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$". In: *Cryptography and Communications* (2023), pp. 1–21.
[4] Claude Carlet. "On known and new differentially uniform functions". In: *Australasian Conference on Information Security and Privacy*. Springer. 2011, pp. 1–15.
[5] Yongqiang Li and Mingsheng Wang. "Constructing differentially 4-uniform permutations over $GF(2^{2m})$ from quadratic APN permutations over $GF(2^{2m+1})$". In: *Designs, codes and cryptography* 72.2 (2014), pp. 249–264.

Restricting vectorial functions to affine spaces

Restriction of a vectorial Boolean function

$$A = a + E \subseteq \mathbb{F}_2^N \text{ affine space of dimension } n.$$
$$A' = a' + E' \subseteq \mathbb{F}_2^M \text{ affine space of dimension } m.$$
$$\mathcal{F}(A) \subseteq A'$$

We say that the tuple (ϕ, a, ϕ', a') is a representation of $\mathcal{F}_A$ if

$$\mathcal{F}_A(x) = \phi'\left(\mathcal{F}(\phi(x) + a) + a'\right)$$

$\phi\colon \mathbb{F}_2^n \to E$ linear bijective
$\phi'\colon \mathbb{F}_2^M \to \mathbb{F}_2^m$ linear and such that $\phi'(E') = \mathbb{F}_2^m$

Beierle et al.[6] use a more general definition where ϕ' is just surjective.

[6] Christof Beierle, Gregor Leander, and Léo Perrin. "Trims and extensions of quadratic APN functions". In: *Designs, Codes and Cryptography* 90.4 (2022), pp. 1009–1036.

Restriction of a vectorial Boolean function

$$A = a + E \subseteq \mathbb{F}_2^N \text{ affine space of dimension } n.$$
$$A' = a' + E' \subseteq \mathbb{F}_2^M \text{ affine space of dimension } m.$$
$$\mathcal{F}(A) \subseteq A'$$

We say that the tuple (ϕ, a, ϕ', a') is a representation of $\mathcal{F}_A$ if

$$\mathcal{F}_A(x) = \phi'\left(\mathcal{F}(\phi(x) + a) + a'\right)$$

$\phi\colon \mathbb{F}_2^n \to E$ linear bijective
$\phi'\colon \mathbb{F}_2^M \to \mathbb{F}_2^m$ linear and such that $\phi'(E') = \mathbb{F}_2^m$

Beierle et al.[6] use a more general definition where ϕ' is just surjective.

[6] Christof Beierle, Gregor Leander, and Léo Perrin. "Trims and extensions of quadratic APN functions". In: *Designs, Codes and Cryptography* 90.4 (2022), pp. 1009–1036.

Cryptographic Properties

$$\delta_{\mathcal{F}_A} = \max_{\alpha \in E\setminus\{0\}, \beta \in E'} \left| \{x \in \mathbb{F}_2^N \mid D_\alpha \mathcal{F}(x) = \beta\} \right|$$

$u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^m$, $u' = (\phi^{-1})^*(u)$, $v' = \psi^*(v)$

$W_{\mathcal{F}_A}(u,v) = 2^{-(N-n)}(-1)^\epsilon \sum_{z \in E^\perp} (-1)^{z\cdot a} W_{\mathcal{F}}(u'+z, v')$ where $\epsilon = v' \cdot a' + a \cdot u'$.

$$\mathrm{nl}(\mathcal{F}_A) = 2^{n-1} - \frac{1}{2^{N-n+1}} \max_{u' \in E_1,\, v' \in (E_2\setminus\{0\})} \left| \sum_{z \in E^\perp} (-1)^{z\cdot a} W_{\mathcal{F}}(u'+z, v') \right|,$$

where $E^\perp \oplus E_1 = \mathbb{F}_2^N$ and $(E')^\perp \oplus E_2 = \mathbb{F}_2^M$.

Cryptographic Properties

$$\delta_{\mathcal{F}_A} = \max_{\alpha\in E\setminus\{0\},\beta\in E'} \left|\{x \in \mathbb{F}_2^N \mid D_\alpha \mathcal{F}(x) = \beta\}\right|$$

$u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^m$, $u' = (\phi^{-1})^*(u)$, $v' = \psi^*(v)$

$W_{\mathcal{F}_A}(u,v) = 2^{-(N-n)}(-1)^\epsilon \sum_{z\in E^\perp}(-1)^{z\cdot a} W_{\mathcal{F}}(u'+z, v')$ where $\epsilon = v'\cdot a' + a\cdot u'$.

$$\mathrm{nl}(\mathcal{F}_A) = 2^{n-1} - \frac{1}{2^{N-n+1}} \max_{u'\in E_1,\, v'\in(E_2\setminus\{0\})} \left|\sum_{z\in E^\perp}(-1)^{z\cdot a} W_{\mathcal{F}}(u'+z, v')\right|,$$

where $E^\perp \oplus E_1 = \mathbb{F}_2^N$ and $(E')^\perp \oplus E_2 = \mathbb{F}_2^M$.

How to have $\mathrm{nl}(\mathcal{F}_A) \neq 0$

$$\mathrm{nl}(\mathcal{F}_A) \geq \mathrm{nl}(\mathcal{F}) - (2^{N-1} - 2^{n-1})$$

Proposition

$$\mathrm{nl}(\mathcal{F}) > 2^{N-1} - 2^{n-1} \implies \mathcal{F}(A) \not\subseteq A'$$

for all A with dimension n and all A' of dimension $m < M$.

Proposition

$$\max_{u \in \mathbb{F}_2^N,\, v \in \mathbb{F}_2^M \setminus (E')^\perp} |W_{\mathcal{F}}(u,v)| < 2^n \implies \mathrm{nl}(\mathcal{F}_A) \neq 0$$

How to have $\mathrm{nl}(\mathcal{F}_A) \neq 0$

$$\mathrm{nl}(\mathcal{F}_A) \geq \mathrm{nl}(\mathcal{F}) - (2^{N-1} - 2^{n-1})$$

Proposition

$$\mathrm{nl}(\mathcal{F}) > 2^{N-1} - 2^{n-1} \implies \mathcal{F}(A) \not\subseteq A'$$

for all A with dimension n and all A' of dimension $m < M$.

Proposition

$$\max_{u \in \mathbb{F}_2^N,\, v \in \mathbb{F}_2^M \setminus (E')^\perp} |W_{\mathcal{F}}(u,v)| < 2^n \implies \mathrm{nl}(\mathcal{F}_A) \neq 0$$

How to have $\mathrm{nl}(\mathcal{F}_A) \neq 0$

$$\mathrm{nl}(\mathcal{F}_A) \geq \mathrm{nl}(\mathcal{F}) - (2^{N-1} - 2^{n-1})$$

Proposition

$$\mathrm{nl}(\mathcal{F}) > 2^{N-1} - 2^{n-1} \implies \mathcal{F}(A) \not\subseteq A'$$

for all A with dimension n and all A' of dimension $m < M$.

Proposition

$$\max_{u \in \mathbb{F}_2^N,\, v \in \mathbb{F}_2^M \setminus (E')^\perp} |W_{\mathcal{F}}(u, v)| < 2^n \implies \mathrm{nl}(\mathcal{F}_A) \neq 0$$

Restricting vectorial functions with affine components

ψ is a linear (M, M)-function

$$A' = \operatorname{Im} \psi$$

$$\mathcal{F}(x) = \psi(\mathcal{G}(x))$$

Then $\mathcal{F}(A) \subseteq A'$ for all affine spaces A.

Theorem

1. $\mathrm{nl}(\mathcal{F}_A) \geq \mathrm{nl}(\mathcal{G}) - (2^{N-1} - 2^{n-1})$.
2. $\delta_{\mathcal{G}_A} \leq \delta_{\mathcal{F}_A} \leq 2^{M-m}\delta_{\mathcal{G}_A}$.

where $\mathcal{G}_A$ is the restriction of $\mathcal{G}$ over A with co-domain $\mathbb{F}_2^M$

Restricting vectorial functions with affine components

$$\psi \text{ is a linear } (M, M)\text{-function}$$
$$A' = \operatorname{Im}\psi$$
$$\mathcal{F}(x) = \psi(\mathcal{G}(x))$$

Then $\mathcal{F}(A) \subseteq A'$ for all affine spaces A.

Theorem

1. $\mathrm{nl}(\mathcal{F}_A) \geq \mathrm{nl}(\mathcal{G}) - (2^{N-1} - 2^{n-1})$.
2. $\delta_{\mathcal{G}_A} \leq \delta_{\mathcal{F}_A} \leq 2^{M-m}\delta_{\mathcal{G}_A}$.

where $\mathcal{G}_A$ is the restriction of $\mathcal{G}$ over A with co-domain $\mathbb{F}_2^M$

Observations on the differential uniformity

Suppose $M = N$ and $m = n$.

$$\delta_{\mathcal{G}_A} \leq \delta_{\mathcal{F}_A} \leq 2^{N-n}\delta_{\mathcal{G}_A}.$$

If $\mathcal{G}$ belongs to an infinite family of (N, N)-functions, then computing $\delta_{\mathcal{G}_A}$ could be hard.

If $\mathcal{G}$ is APN, then we have that $\delta_{\mathcal{G}_A} = 2$ and that $2 \leq \delta_{\mathcal{F}_A} \leq 2^{N-n+1}$.

With $n = N - 1$ we have that $\mathcal{F}_A$ is at most 4-uniform.

Restricting (N, N)-functions over affine hyperplanes and the strong D-property

The D(illon)-property of APN (n, n)-functions[7]

$$\Phi_F(x, y, z) = F(x + y + z) + F(x) + F(y) + F(z)$$

Lemma

Let F be an (n, n)-function. Then F is APN if and only if all the solutions (x, y, z) to the equation $\Phi_F(x, y, z) = 0$ are such that $|\{x, y, z, x + y + z\}| \neq 4$.

Lemma

Let F be an APN (n, n)-function, then $\mathrm{nl}(F) \neq 0$.

Theorem (Dillon)

Let F be an APN (n, n)-function, then $\mathrm{Im}\,\Phi_F = \mathbb{F}_2^n$.

[7] Claude Carlet. "Boolean functions for cryptography and coding theory". In: (2021).

Proof of the D-property

Proof.

For simplicity, we consider F in its univariate representation.
Suppose there exists $c \in \mathbb{F}_{2^n}$ not in $\mathrm{Im}\,\Phi_F$. We can assume $c \neq 0$.
Then $F'(x) = F(x) + cf(x)$ is APN for any Boolean function f. Indeed, let (x, y, z) be such that $\Phi_{F'}(x, y, z) = 0$ that we can rewrite as

$$\Phi_F(x, y, z) = c\Phi_f(x, y, z).$$

If $\Phi_f(x, y, z) = 1$, then the equation has no solution
If $\Phi_f(x, y, z) = 0$, then all the solutions (x, y, z) are such that $|\{x, y, z, x + y + z\}| \neq 4$ because F is APN.
Let $c' \in \mathbb{F}_{2^n}$ be such that $\mathrm{Tr}(cc') = 1$ and set $f(x) = \mathrm{Tr}(c'F(x))$. Then

$$\mathrm{Tr}(c'F'(x)) = \mathrm{Tr}(c'F(x)) + \mathrm{Tr}(c'c)\mathrm{Tr}(c'F(x)) = 0$$

and so $\mathrm{nl}(F') = 0$. A contradiction. □

The D-property by Taniguchi

Definition (D-property)

An (n, m)-function F has the D-property if $\Phi_F((\mathbb{F}_2^n)^3) = \mathbb{F}_2^m$.

In[8], there is a focus on the case $m = n + 1$ and $F = \mathcal{G}_{E_0}$ where

- $\mathcal{G}$ is an APN $(n + 1, n + 1)$-function
- $E_0 = \{x \in \mathbb{F}_{2^{n+1}} : \mathrm{Tr}(x) = 0\}$

A recent paper[9], investigates this property further.

We consider it in relation to the problem of constructing APN $(N - 1, N - 1)$-functions

[8] Hiroaki Taniguchi. "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$". In: *Cryptography and Communications* (2023), pp. 1–21.

[9] Matteo Abbondati, Marco Calderini, and Irene Villa. "On Dillon's property of (n, m)-functions". In: *arXiv preprint arXiv:2302.13922* (2023).

The D-property by Taniguchi

Definition (D-property)

An (n, m)-function F has the D-property if $\Phi_F((\mathbb{F}_2^n)^3) = \mathbb{F}_2^m$.

In[8], there is a focus on the case $m = n + 1$ and $F = \mathcal{G}_{E_0}$ where

- $\mathcal{G}$ is an APN $(n + 1, n + 1)$-function
- $E_0 = \{x \in \mathbb{F}_{2^{n+1}} : \mathrm{Tr}(x) = 0\}$

A recent paper[9], investigates this property further.

We consider it in relation to the problem of constructing APN $(N - 1, N - 1)$-functions

[8] Hiroaki Taniguchi. "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$". In: *Cryptography and Communications* (2023), pp. 1–21.

[9] Matteo Abbondati, Marco Calderini, and Irene Villa. "On Dillon's property of (n, m)-functions". In: *arXiv preprint arXiv:2302.13922* (2023).

The D-property by Taniguchi

Definition (D-property)

An (n, m)-function F has the D-property if $\Phi_F((\mathbb{F}_2^n)^3) = \mathbb{F}_2^m$.

In[8], there is a focus on the case $m = n + 1$ and $F = \mathcal{G}_{E_0}$ where

- $\mathcal{G}$ is an APN $(n+1, n+1)$-function
- $E_0 = \{x \in \mathbb{F}_{2^{n+1}} : \mathrm{Tr}(x) = 0\}$

A recent paper[9], investigates this property further.

We consider it in relation to the problem of constructing APN $(N-1, N-1)$-functions

---

[8] Hiroaki Taniguchi. "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$". In: *Cryptography and Communications* (2023), pp. 1–21.

[9] Matteo Abbondati, Marco Calderini, and Irene Villa. "On Dillon's property of (n, m)-functions". In: *arXiv preprint arXiv:2302.13922* (2023).

Constructing APN $(N-1, N-1)$-functions as restrictions

Let $\mathcal{G}$ be an APN (N, N)-function.
Let ψ be a linear (N, N)-function with $\ker \psi = \langle c \rangle$.
Let $A \subseteq \mathbb{F}_2^N$ be an affine hyperplane.
Let $\mathcal{F}(x) = \psi(\mathcal{G}(x))$.

Lemma

$\mathcal{F}_A$ is APN if and only if $\Phi_{\mathcal{G}}(x, y, z) \neq c \ \forall x, y, z \in A$.

Proof.

Suppose that there exists $x, y, z \in A$ such that $\Phi_{\mathcal{G}}(x, y, z) = c$.
Since $\Phi_{\mathcal{G}}(x, y, z) \neq 0$, then $|\{x, y, z, x + y + z\}| = 4$.
So we have that $0 = \psi(c) = \psi(\Phi_{\mathcal{G}}(x, y, z)) = \Phi_{\mathcal{F}}(x, y, z)$ and therefore $\mathcal{F}_A$ is not APN.
Suppose that $\mathcal{F}_A$ is not APN, then there exists $x, y, z \in A$ such that $\Phi_{\mathcal{F}}(x, y, z) = 0$ and $|\{x, y, z, x + y + z\}| = 4$.
So we have that $\Phi_{\mathcal{G}}(x, y, z) \in \ker \psi = \langle c \rangle$ and since $\mathcal{G}$ is APN, then $\Phi_{\mathcal{G}}(x, y, z) = c$. □

Constructing APN $(N-1, N-1)$-functions as restrictions

Let $\mathcal{G}$ be an APN (N, N)-function.
Let ψ be a linear (N, N)-function with $\ker \psi = \langle c \rangle$.
Let $A \subseteq \mathbb{F}_2^N$ be an affine hyperplane.
Let $\mathcal{F}(x) = \psi(\mathcal{G}(x))$.

Lemma

$\mathcal{F}_A$ is APN if and only if $\Phi_{\mathcal{G}}(x, y, z) \neq c \ \forall x, y, z \in A$.

Proof.

Suppose that there exists $x, y, z \in A$ such that $\Phi_{\mathcal{G}}(x, y, z) = c$.
Since $\Phi_{\mathcal{G}}(x, y, z) \neq 0$, then $|\{x, y, z, x + y + z\}| = 4$.
So we have that $0 = \psi(c) = \psi(\Phi_{\mathcal{G}}(x, y, z)) = \Phi_{\mathcal{F}}(x, y, z)$ and therefore $\mathcal{F}_A$ is not APN.
Suppose that $\mathcal{F}_A$ is not APN, then there exists $x, y, z \in A$ such that $\Phi_{\mathcal{F}}(x, y, z) = 0$ and $|\{x, y, z, x + y + z\}| = 4$.
So we have that $\Phi_{\mathcal{G}}(x, y, z) \in \ker \psi = \langle c \rangle$ and since $\mathcal{G}$ is APN, then $\Phi_{\mathcal{G}}(x, y, z) = c$. □

Constructing APN $(N-1, N-1)$-functions as restrictions

Let $\mathcal{G}$ be an APN (N, N)-function.
Let ψ be a linear (N, N)-function with $\ker \psi = \langle c \rangle$.
Let $A \subseteq \mathbb{F}_2^N$ be an affine hyperplane.
Let $\mathcal{F}(x) = \psi(\mathcal{G}(x))$.

Lemma

$\mathcal{F}_A$ is APN if and only if $\Phi_{\mathcal{G}}(x, y, z) \neq c \ \forall x, y, z \in A$.

Proof.

Suppose that there exists $x, y, z \in A$ such that $\Phi_{\mathcal{G}}(x, y, z) = c$.
Since $\Phi_{\mathcal{G}}(x, y, z) \neq 0$, then $|\{x, y, z, x + y + z\}| = 4$.
So we have that $0 = \psi(c) = \psi(\Phi_{\mathcal{G}}(x, y, z)) = \Phi_{\mathcal{F}}(x, y, z)$ and therefore $\mathcal{F}_A$ is not APN.
Suppose that $\mathcal{F}_A$ is not APN, then there exists $x, y, z \in A$ such that $\Phi_{\mathcal{F}}(x, y, z) = 0$ and $|\{x, y, z, x + y + z\}| = 4$.
So we have that $\Phi_{\mathcal{G}}(x, y, z) \in \ker \psi = \langle c \rangle$ and since $\mathcal{G}$ is APN, then $\Phi_{\mathcal{G}}(x, y, z) = c$. □

The strong D-property

Let $\mathcal{G}$ be an (N, N)-function.

Definition (strong D-property)

$\mathcal{G}$ has the strong D-property if the $(N-1, N)$-function $\mathcal{G}_A$ has the D-property for any affine hyperplane A.

Proposition

If $\mathcal{G}$ is APN, then

$\mathcal{G}$ has the strong D-property if and only if $\mathcal{F}_A$ is not APN ($\delta_{\mathcal{F}_A} = 4$) where $\mathcal{F}(x) = \psi(\mathcal{G}(x))$

for all ψ linear function with kernel of dimension 1
for all affine hyperplane A.

The strong D-property

Let $\mathcal{G}$ be an (N, N)-function.

Definition (strong D-property)

$\mathcal{G}$ has the strong D-property if the $(N-1, N)$-function $\mathcal{G}_A$ has the D-property for any affine hyperplane A.

Proposition

If $\mathcal{G}$ is APN, then

$$\mathcal{G} \text{ has the strong D-property if and only if } \mathcal{F}_A \text{ is not APN } (\delta_{\mathcal{F}_A} = 4) \text{ where } \mathcal{F}(x) = \psi(\mathcal{G}(x))$$

for all ψ linear function with kernel of dimension 1
for all affine hyperplane A.

Open problems/questions

Open Question

Do all APN power functions in dimension big enough have the strong D-property?

Open Problem

Find an infinite class of APN functions that do not have the strong D-property.

Proposition

Let $\mathcal{G}$ be a quadratic APN (N, N)-function with N even.
If $\mathcal{G}$ has the strong D-property, then $\mathrm{nl}(\mathcal{G}) > 2^{N-2}$.

The minimum known nonlinearity is 2^{N-2} for an N-variable APN function, achieved by some quadratic APN functions in dimension 6 and 8.

Open Problem

Find non-quadratic APN functions with nonlinearity 2^{N-2}, or less, if possible an infinite class.

Open problems/questions

Open Question

Do all APN power functions in dimension big enough have the strong D-property?

Open Problem

Find an infinite class of APN functions that do not have the strong D-property.

Proposition

Let $\mathcal{G}$ be a quadratic APN (N, N)-function with N even.
If $\mathcal{G}$ has the strong D-property, then $\mathrm{nl}(\mathcal{G}) > 2^{N-2}$.

The minimum known nonlinearity is 2^{N-2} for an N-variable APN function, achieved by some quadratic APN functions in dimension 6 and 8.

Open Problem

Find non-quadratic APN functions with nonlinearity 2^{N-2}, or less, if possible an infinite class.

Open problems/questions

Open Question

Do all APN power functions in dimension big enough have the strong D-property?

Open Problem

Find an infinite class of APN functions that do not have the strong D-property.

Proposition

Let $\mathcal{G}$ be a quadratic APN (N, N)-function with N even.
If $\mathcal{G}$ has the strong D-property, then $\mathrm{nl}(\mathcal{G}) > 2^{N-2}$.

The minimum known nonlinearity is 2^{N-2} for an N-variable APN function, achieved by some quadratic APN functions in dimension 6 and 8.

Open Problem

Find non-quadratic APN functions with nonlinearity 2^{N-2}, or less, if possible an infinite class.

Open problems/questions

Open Question

Do all APN power functions in dimension big enough have the strong D-property?

Open Problem

Find an infinite class of APN functions that do not have the strong D-property.

Proposition

Let $\mathcal{G}$ be a quadratic APN (N, N)-function with N even.
If $\mathcal{G}$ has the strong D-property, then $\mathrm{nl}(\mathcal{G}) > 2^{N-2}$.

The minimum known nonlinearity is 2^{N-2} for an N-variable APN function, achieved by some quadratic APN functions in dimension 6 and 8.

Open Problem

Find non-quadratic APN functions with nonlinearity 2^{N-2}, or less, if possible an infinite class.

Open problems/questions

Open Question

Do all APN power functions in dimension big enough have the strong D-property?

Open Problem

Find an infinite class of APN functions that do not have the strong D-property.

Proposition

Let $\mathcal{G}$ be a quadratic APN (N, N)-function with N even.
If $\mathcal{G}$ has the strong D-property, then $\mathrm{nl}(\mathcal{G}) > 2^{N-2}$.

The minimum known nonlinearity is 2^{N-2} for an N-variable APN function, achieved by some quadratic APN functions in dimension 6 and 8.

Open Problem

Find non-quadratic APN functions with nonlinearity 2^{N-2}, or less, if possible an infinite class.

The case of crooked functions[10]

Definition (Crooked function)

An (N, N)-function $\mathcal{G}$ is crooked if $\mathrm{Im}\,(D_a\mathcal{G})$ is an affine hyperplane for all $a \in \mathbb{F}_2^N \setminus \{0\}$.

Conjecture

$\mathcal{G}$ is a crooked function if and only if $\mathcal{G}$ is a quadratic APN function.

$$\varphi_{\mathcal{G}}(a, b) = \mathcal{G}(a + b) + \mathcal{G}(a) + \mathcal{G}(b) + \mathcal{G}(0)$$

The ortho-derivative of $\mathcal{G}$ is the (N, N)-function $\pi_{\mathcal{G}}$ such that $\pi_{\mathcal{G}}(0) = 0$ and that $\pi_{\mathcal{G}}(a) \cdot \varphi_{\mathcal{G}}(a, b) = 0 \ \forall a, b \in \mathbb{F}_2^N \setminus \{0\}$.

[10] Gohar M Kyureghyan. "Crooked maps in $\mathbb{F}_2^n$". In: *Finite Fields and their applications* 13.3 (2007), pp. 713–726.

The case of crooked functions[10]

Definition (Crooked function)

An (N, N)-function $\mathcal{G}$ is crooked if $\mathrm{Im}\,(D_a\mathcal{G})$ is an affine hyperplane for all $a \in \mathbb{F}_2^N \setminus \{0\}$.

Conjecture

$\mathcal{G}$ is a crooked function if and only if $\mathcal{G}$ is a quadratic APN function.

$$\varphi_{\mathcal{G}}(a, b) = \mathcal{G}(a + b) + \mathcal{G}(a) + \mathcal{G}(b) + \mathcal{G}(0)$$

The ortho-derivative of $\mathcal{G}$ is the (N, N)-function $\pi_{\mathcal{G}}$ such that $\pi_{\mathcal{G}}(0) = 0$ and that $\pi_{\mathcal{G}}(a) \cdot \varphi_{\mathcal{G}}(a, b) = 0 \ \forall a, b \in \mathbb{F}_2^N \setminus \{0\}$.

[10] Gohar M Kyureghyan. "Crooked maps in $\mathbb{F}_2^n$". In: *Finite Fields and their applications* 13.3 (2007), pp. 713–726.

The strong D-property of crooked functions

Let $\mathcal{G}$ be crooked.
Let $\Gamma_{v,c}^{(1)} = \{a \in \mathbb{F}_2^N \mid c \cdot \pi_{\mathcal{G}}(a) = 0,\ v \cdot a = 1\}$ and let $\Lambda_c = \{(a,b) \in (\mathbb{F}_2^N)^2 \mid \varphi_{\mathcal{G}}(a,b) = c\}$

Lemma

$\mathcal{G}$ has the strong D-property if and only if, for all $v, c \in \mathbb{F}_2^N \setminus \{0\}$, we have that

$$|\Gamma_{v,c}^{(1)}| < \frac{|\Lambda_c|}{3}.$$

$$|\Lambda_c| = W_{\pi_{\mathcal{G}}}(0,c) + 2^N - 2$$

$$|\Gamma_{c,v}^{(1)}| = \frac{|\Lambda_c| + 2 - W_{\pi_{\mathcal{G}}}(v,c)}{4}$$

The strong D-property of crooked functions

Let $\mathcal{G}$ be crooked.
Let $\Gamma^{(1)}_{v,c} = \{a \in \mathbb{F}_2^N \mid c \cdot \pi_{\mathcal{G}}(a) = 0,\ v \cdot a = 1\}$ and let $\Lambda_c = \{(a,b) \in (\mathbb{F}_2^N)^2 \mid \varphi_{\mathcal{G}}(a,b) = c\}$

Lemma

$\mathcal{G}$ has the strong D-property if and only if, for all $v, c \in \mathbb{F}_2^N \setminus \{0\}$, we have that

$$|\Gamma^{(1)}_{v,c}| < \frac{|\Lambda_c|}{3}.$$

$$|\Lambda_c| = W_{\pi_{\mathcal{G}}}(0,c) + 2^N - 2$$

$$|\Gamma^{(1)}_{c,v}| = \frac{|\Lambda_c| + 2 - W_{\pi_{\mathcal{G}}}(v,c)}{4}$$

The strong D-property of the Gold APN function

Theorem

Let $\mathcal{G}$ be a crooked (N,N)-function with $N \geq 3$. Let $\lambda^{\min} = \min_{c \in \mathbb{F}_2^N \setminus \{0\}} |\Lambda_c|$.

If $\mathrm{nl}(\pi_{\mathcal{G}}) > 2^{N-1} - \frac{\lambda^{\min}}{6} + 2$, *then $\mathcal{G}$ has the strong D-property.*

Theorem

Let $N \geq 3$ and i be such that $\gcd(i,N) = 1$.

Then the Gold APN function x^{2^i+1} has the strong D-property if and only if $N = 6$ or $N \geq 8$.

$\pi_{\mathcal{G}}(x) = x^{-(2^i+1)}$

We proved the case N odd, while the case N even follows from the work of Taniguchi[11].

[11] Hiroaki Taniguchi. "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$". In: *Cryptography and Communications* (2023), pp. 1–21.

The strong D-property of the Gold APN function

Theorem

Let $\mathcal{G}$ be a crooked (N, N)-function with $N \geq 3$. Let $\lambda^{\min} = \min_{c \in \mathbb{F}_2^N \setminus \{0\}} |\Lambda_c|$.

If $\mathrm{nl}(\pi_{\mathcal{G}}) > 2^{N-1} - \frac{\lambda^{\min}}{6} + 2$, then $\mathcal{G}$ has the strong D-property.

Theorem

Let $N \geq 3$ and i be such that $\gcd(i, N) = 1$.
Then the Gold APN function x^{2^i+1} has the strong D-property if and only if $N = 6$ or $N \geq 8$.

$\pi_{\mathcal{G}}(x) = x^{-(2^i+1)}$

We proved the case N odd, while the case N even follows from the work of Taniguchi[11].

[11] Hiroaki Taniguchi. "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$". In: *Cryptography and Communications* (2023), pp. 1–21.

The (partial) strong D-property of the Dobbertin APN function

Proposition

Let $\mathcal{G}(x) = x^{2^{4t}+2^{3t}+2^{2t}+2^{t}-1}$ *be the Dobbertin APN function over* $\mathbb{F}_{2^{5t}}$*.*
Let $E = \{x \in \mathbb{F}_{2^{5t}} \mid \mathrm{Tr}_{5t}(x) = 0\}$.
Then $\mathcal{G}_E$ *has the D-property if and only if* $t \geq 2$*.*

Conjecture

For $t \geq 2$*, the Dobbertin APN function in dimension* $N = 5t$ *has the strong D-property.*

The (partial) strong D-property of the Dobbertin APN function

Proposition

Let $\mathcal{G}(x) = x^{2^{4t}+2^{3t}+2^{2t}+2^t-1}$ *be the Dobbertin APN function over* $\mathbb{F}_{2^{5t}}$.
Let $E = \{x \in \mathbb{F}_{2^{5t}} \mid \mathrm{Tr}_{5t}(x) = 0\}$.
Then $\mathcal{G}_E$ *has the D-property if and only if* $t \geq 2$.

Conjecture

For $t \geq 2$*, the Dobbertin APN function in dimension* $N = 5t$ *has the strong D-property.*

Sketch of the proof

We use the following Lemma by Taniguchi[12]

Lemma

Let $\mathcal{G}(x) = x^d$ be an APN power function over $\mathbb{F}_{2^{5t}}$.
Let us denote $E_K = \{x \in \mathbb{F}_{2^K} \mid \mathrm{Tr}_K(x) = 0\}$.
If either $\mathcal{G}_{E_t}$ or $\mathcal{G}_{E_5}$ has the D-property, then $\mathcal{G}_{E_{5t}}$ has the D-property.

Let $d = 2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$.
The cases $t \leq 5$ can be verified computationally. Assume $t > 5$. Let us prove the case $t \neq 7$.
Observe that $d = 3 \pmod{2^t - 1}$ and so we can use the strong D-property of x^3.
Assume $t = 7$. In this case, the D-property of $\mathcal{G}_{E_5}$ can be verified computationally.

[12] Hiroaki Taniguchi. "D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$". In: *Cryptography and Communications* (2023), pp. 1–21.

Revisiting two infinite families of differentially 4-uniform $(N-1, N-1)$-permutations

The setting

$\mathcal{G}(x) = x^d$ APN power permutation over $\mathbb{F}_{2^N}$ (N is odd).
ψ linear with kernel of dimension 1 generated by $c \in \mathbb{F}_{2^N} \setminus \{0\}$
$A = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = \epsilon\}$ where $\epsilon \in \mathbb{F}_2$.

$$\mathcal{F}(x) = \psi(\mathcal{G}(x))$$
$$\mathcal{F}'(x) = \psi(\mathcal{G}(x)) + x$$

Either $\mathcal{F}_A$ or $\mathcal{F}'_A$ is a permutation.

If the system

$$\begin{cases} x^d + y^d + z^d + (x+y+z)^d = 0 \\ \mathrm{Tr}(x) = \mathrm{Tr}(y) = \mathrm{Tr}(z) = \epsilon \end{cases} \tag{1}$$

has at least one solution, then $\mathcal{F}_A$ and $\mathcal{F}'_A$ are not APN.

Family of 4-uniform permutations $\mathcal{F}'_A$ by Carlet[13]

$N \geq 5$ odd, $A = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 1\}$, $\mathcal{G}(x) = x^{2^N-2}$.

$\mathcal{F}'(x) = \psi(\mathcal{G}(x)) + x$

Theorem

$\mathcal{F}'_A$ is not APN.

The proof of the theorem uses the Hasse-Weil bound.

Conjecture

For $N \geq 5$ odd, the inverse function has the strong D-property.

[13] Claude Carlet. "On known and new differentially uniform functions". In: *Australasian Conference on Information Security and Privacy*. Springer. 2011, pp. 1–15.

Family of 4-uniform permutations $\mathcal{F}'_A$ by Carlet[13]

$N \geq 5$ odd, $A = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 1\}$, $\mathcal{G}(x) = x^{2^N-2}$.

$\mathcal{F}'(x) = \psi(\mathcal{G}(x)) + x$

Theorem

$\mathcal{F}'_A$ is not APN.

The proof of the theorem uses the Hasse-Weil bound.

Conjecture

For $N \geq 5$ odd, the inverse function has the strong D-property.

[13] Claude Carlet. "On known and new differentially uniform functions". In: *Australasian Conference on Information Security and Privacy*. Springer. 2011, pp. 1–15.

Family of 4-uniform permutations $\mathcal{F}'_A$ by Carlet[13]

$N \geq 5$ odd, $A = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 1\}$, $\mathcal{G}(x) = x^{2^N-2}$.
$\mathcal{F}'(x) = \psi(\mathcal{G}(x)) + x$

Theorem

$\mathcal{F}'_A$ is not APN.

The proof of the theorem uses the Hasse-Weil bound.

Conjecture

For $N \geq 5$ odd, the inverse function has the strong D-property.

[13] Claude Carlet. "On known and new differentially uniform functions". In: *Australasian Conference on Information Security and Privacy*. Springer. 2011, pp. 1–15.

Family of 4-uniform permutations $\mathcal{F}_E$ by Li and Wang[14]

$N \geq 5$ odd, $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$
$c \in \mathbb{F}_{2^N} \setminus \{0\}$, $\psi(x) = cx^{2^i} + c^{2^i}x$, $\mathcal{G}(x) = x^{\frac{1}{2^i+1}}$ with $\gcd(i, N) = 1$
$\mathcal{F}(x) = \psi(\mathcal{G}(x))$

Theorem

$\mathcal{F}_E$ is not APN.

The proof of the theorem uses the ortho-derivative $\pi(x) = x^{-(2^i+1)}$.

Conjecture

For $N \geq 5$ odd, the inverse of the Gold APN function has the strong D-property.

[14] Yongqiang Li and Mingsheng Wang. "Constructing differentially 4-uniform permutations over $GF(2^{2m})$ from quadratic APN permutations over $GF(2^{2m+1})$". In: *Designs, codes and cryptography* 72.2 (2014), pp. 249–264.

Family of 4-uniform permutations $\mathcal{F}_E$ by Li and Wang[14]

$N \geq 5$ odd, $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$

$c \in \mathbb{F}_{2^N} \setminus \{0\}$, $\psi(x) = cx^{2^i} + c^{2^i}x$, $\mathcal{G}(x) = x^{\frac{1}{2^i+1}}$ with $\gcd(i, N) = 1$

$\mathcal{F}(x) = \psi(\mathcal{G}(x))$

Theorem

$\mathcal{F}_E$ is not APN.

The proof of the theorem uses the ortho-derivative $\pi(x) = x^{-(2^i+1)}$.

Conjecture

For $N \geq 5$ odd, the inverse of the Gold APN function has the strong D-property.

[14] Yongqiang Li and Mingsheng Wang. "Constructing differentially 4-uniform permutations over GF(2^{2m}) from quadratic APN permutations over GF(2^{2m+1})". In: *Designs, codes and cryptography* 72.2 (2014), pp. 249–264.

Family of 4-uniform permutations $\mathcal{F}_E$ by Li and Wang[14]

$N \geq 5$ odd, $E = \{x \in \mathbb{F}_{2^N} \mid \mathrm{Tr}(x) = 0\}$
$c \in \mathbb{F}_{2^N} \setminus \{0\}$, $\psi(x) = cx^{2^i} + c^{2^i}x$, $\mathcal{G}(x) = x^{\frac{1}{2^i+1}}$ with $\gcd(i, N) = 1$
$\mathcal{F}(x) = \psi(\mathcal{G}(x))$

Theorem

$\mathcal{F}_E$ is not APN.

The proof of the theorem uses the ortho-derivative $\pi(x) = x^{-(2^i+1)}$.

Conjecture

For $N \geq 5$ odd, the inverse of the Gold APN function has the strong D-property.

[14] Yongqiang Li and Mingsheng Wang. "Constructing differentially 4-uniform permutations over GF(2^{2m}) from quadratic APN permutations over GF(2^{2m+1})". In: *Designs, codes and cryptography* 72.2 (2014), pp. 249–264.

Conclusions

On the construction of cryptographically strong functions

- If $\mathcal{F}$ does not have affine components, mapping affine to affine is rare
- Fairly easy to construct 4-uniform functions with good cryptographic properties
- The revisiting of previously known infinite families

On the construction of cryptographically strong functions

- If $\mathcal{F}$ does not have affine components, mapping affine to affine is rare
- Fairly easy to construct 4-uniform functions with good cryptographic properties
- The revisiting of previously known infinite families

- If $\mathcal{F}$ does not have affine components, mapping affine to affine is rare
- Fairly easy to construct 4-uniform functions with good cryptographic properties
- The revisiting of previously known infinite families

- Constructing APN functions is hard (also) in this setting
- The strong D-property is hard to prove for a family of APN functions
- Several open problems/questions

On the construction of APN functions, and the strong D-property

- Constructing APN functions is hard (also) in this setting
- The strong D-property is hard to prove for a family of APN functions
- Several open problems/questions

On the construction of APN functions, and the strong D-property

- Constructing APN functions is hard (also) in this setting
- The strong D-property is hard to prove for a family of APN functions
- Several open problems/questions

On the construction of APN permutation

- Easier to study
- Less equations than proving the strong D-property

On the construction of APN permutation

- Easier to study
- Less equations than proving the strong D-property

Thanks for your attention!