Exploring the Set of APN Functions in Practice

Jules Baudrin[1], Pierre Galissant[2], Léo Perrin [2]

Université Versailles Saint-Quentin, Versailles, France [1]
Inria, Paris, France [2]

April 3, 2026

European Research Council
Established by the European Commission

informatics mathematics

université PARIS-SACLAY

APN Functions

Almost Perfect Nonlinear Function

A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *Almost Perfect Non-linear* (APN) if $F(x + a) + F(x) = b$ has at most 2 solutions for all $a \neq 0, b$.

APN Functions

Almost Perfect Nonlinear Function

A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *Almost Perfect Non-linear* (APN) if $F(x + a) + F(x) = b$ has at most 2 solutions for all $a \neq 0, b$.

- APN functions are important for **cryptography**

APN Functions

Almost Perfect Nonlinear Function

A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *Almost Perfect Non-linear* (APN) if $F(x+a) + F(x) = b$ has at most 2 solutions for all $a \neq 0, b$.

- APN functions are important for **cryptography**
- **Perfect Nonlinear**: for linear functions, 0 or 2^n solutions $F(x+a) + F(x) = F(a)$

APN Functions

Almost Perfect Nonlinear Function

A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *Almost Perfect Non-linear* (APN) if $F(x+a)+F(x)=b$ has at most 2 solutions for all $a \neq 0, b$.

- APN functions are important for **cryptography**
- **Perfect Nonlinear**: for linear functions, 0 or 2^n solutions $\quad F(x+a)+F(x)=F(a)$
- **Almost**: in characteristic 2, we have an even number of solutions

APN Functions

Almost Perfect Nonlinear Function

A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *Almost Perfect Non-linear* (APN) if $F(x+a) + F(x) = b$ has at most 2 solutions for all $a \neq 0, b$.

- APN functions are important for **cryptography**
- **Perfect Nonlinear**: for linear functions, 0 or 2^n solutions $\quad F(x+a) + F(x) = F(a)$
- **Almost**: in characteristic 2, we have an even number of solutions

- Example: $F(x) = x^3$ is APN for any n $\quad (x+a)^3 + x^3 = ax^2 + a^2x + a^3$

APN Functions

Almost Perfect Nonlinear Function

A function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is *Almost Perfect Non-linear* (APN) if $F(x+a)+F(x)=b$ has at most 2 solutions for all $a \neq 0, b$.

- APN functions are important for **cryptography**
- **Perfect Nonlinear**: for linear functions, 0 or 2^n solutions $\quad F(x+a)+F(x)=F(a)$
- **Almost**: in characteristic 2, we have an even number of solutions

- Example: $F(x)=x^3$ is APN for any n $\quad (x+a)^3+x^3=ax^2+a^2x+a^3$

We need more properties for cryptography

- It is usually better for it to have a **higher degree**

APN Functions

Almost Perfect Nonlinear Function

A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *Almost Perfect Non-linear* (APN) if $F(x+a)+F(x)=b$ has at most 2 solutions for all $a \neq 0, b$.

- APN functions are important for **cryptography**
- **Perfect Nonlinear**: for linear functions, 0 or 2^n solutions $\quad F(x+a)+F(x)=F(a)$
- **Almost**: in characteristic 2, we have an even number of solutions

- Example: $F(x)=x^3$ is APN for any n $\quad (x+a)^3+x^3=ax^2+a^2x+a^3$

We need more properties for cryptography

- It is usually better for it to have a **higher degree**
- Sometimes, it needs to be **bijective**

The Big APN Problem

The Big APN Problem

Are there APN bijections when n is even and $n > 6$?

The Big APN Problem

The Big APN Problem

Are there APN bijections when n is even and $n > 6$?

- In small dimension, we can just check $2^2! = 24$, $2^4! = 2^{44}$

The Big APN Problem

The Big APN Problem

Are there APN bijections when n is even and $n > 6$?

- In small dimension, we can just check $2^2! = 24,\ 2^4! = 2^{44}$
- x^3 is a bijection when n is odd (since $gcd(3, 2^n - 1) = 1$)

The Big APN Problem

The Big APN Problem

Are there APN bijections when n is even and $n > 6$?

- In small dimension, we can just check $2^2! = 24,\ 2^4! = 2^{44}$
- x^3 is a bijection when n is odd (since $gcd(3, 2^n - 1) = 1$)

Dillon Permutation (n = 6)

```
[ 0 54 48 13 15 18 53 35]
[25 63 45 52  3 20 41 33]
[59 36  2 34 10  8 57 37]
[60 19 42 14 50 26 58 24]
[39 27 21 17 16 29  1 62]
[47 40 51 56  7 43 44 38]
[31 11  4 28 61 46  5 49]
[ 9  6 23 32 30 12 55 22]
```

The Big APN Problem

The Big APN Problem

Are there APN bijections when n is even and $n > 6$?

- In small dimension, we can just check $2^2! = 24,\ 2^4! = 2^{44}$
- x^3 is a bijection when n is odd (since $gcd(3, 2^n - 1) = 1$)

Dillon Permutation (n = 6)

0	54	48	13	15	18	53	35
25	63	45	52	3	20	41	33
59	36	2	34	10	8	57	37
60	19	42	14	50	26	58	24
39	27	21	17	16	29	1	62
47	40	51	56	7	43	44	38
31	11	4	28	61	46	5	49
9	6	23	32	30	12	55	22

- It is the only known APN permutation since 2009

The Big APN Problem

The Big APN Problem

Are there APN bijections when n is even and $n > 6$?

- In small dimension, we can just check $2^2! = 24,\ 2^4! = 2^{44}$
- x^3 is a bijection when n is odd (since $gcd(3, 2^n - 1) = 1$)

Dillon Permutation (n = 6)

0	54	48	13	15	18	53	35
25	63	45	52	3	20	41	33
59	36	2	34	10	8	57	37
60	19	42	14	50	26	58	24
39	27	21	17	16	29	1	62
47	40	51	56	7	43	44	38
31	11	4	28	61	46	5	49
9	6	23	32	30	12	55	22

- It is the only known APN permutation since 2009
- It was found **exploring** the set of APN functions starting from the Kim mapping:

$$x^3 + x^{10} + u\,x^{24}, \text{with a special u}$$

The Big APN Problem

The Big APN Problem

Are there APN bijections when n is even and $n > 6$?

- In small dimension, we can just check $2^2! = 24,\ 2^4! = 2^{44}$
- x^3 is a bijection when n is odd (since $gcd(3, 2^n - 1) = 1$)

Dillon Permutation (n = 6)

0	54	48	13	15	18	53	35
25	63	45	52	3	20	41	33
59	36	2	34	10	8	57	37
60	19	42	14	50	26	58	24
39	27	21	17	16	29	1	62
47	40	51	56	7	43	44	38
31	11	4	28	61	46	5	49
9	6	23	32	30	12	55	22

- It is the only known APN permutation since 2009
- It was found **exploring** the set of APN functions starting from the Kim mapping:

$$x^3 + x^{10} + u\,x^{24}, \text{with a special u}$$

- The studied generalizations of the Kim mapping **do not** work

The Big APN Problem

The Big APN Problem

Are there APN bijections when n is even and $n > 6$?

- In small dimension, we can just check $2^2! = 24,\ 2^4! = 2^{44}$
- x^3 is a bijection when n is odd (since $gcd(3, 2^n - 1) = 1$)

Dillon Permutation (n = 6)

0	54	48	13	15	18	53	35
25	63	45	52	3	20	41	33
59	36	2	34	10	8	57	37
60	19	42	14	50	26	58	24
39	27	21	17	16	29	1	62
47	40	51	56	7	43	44	38
31	11	4	28	61	46	5	49
9	6	23	32	30	12	55	22

- It is the only known APN permutation since 2009
- It was found **exploring** the set of APN functions starting from the Kim mapping:

$$x^3 + x^{10} + u\,x^{24}, \text{with a special u}$$

- The studied generalizations of the Kim mapping **do not** work
- Naive search not possible $2^6! = 2^{295}$

Goal

Goal

Can we replicate the results of Dillon in dimension 8 by *exploring* the set of APN functions ?

Goal

Can we replicate the results of Dillon in dimension 8 by *exploring* the set of APN functions ?

Goal

Can we replicate the results of Dillon in dimension 8 by *exploring* the set of APN functions ?

$\hookrightarrow$ What do we mean by exploration :

1. The computation of the **CCZ class**
2. The computation of **Switching Neighbours**

Definitions - 1

$\mathbb{F}_{2^n} = \mathbb{F}_2^n$

We use heavily $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P) = \mathbb{F}_2^n$ with $a = \sum_{i=0}^{n-1} a_i X^i = (a_0, \ldots, a_{n-1})$

Definitions - 1

$\mathbb{F}_{2^n} = \mathbb{F}_2^n$

We use heavily $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P) = \mathbb{F}_2^n$ with $a = \sum_{i=0}^{n-1} a_i X^i = (a_0, \dots, a_{n-1})$

Definition

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

- **Coordinates** f_i: $F = (f_0, \dots, f_{n-1})$

Definitions - 1

$\mathbb{F}_{2^n} = \mathbb{F}_2^n$

We use heavily $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P) = \mathbb{F}_2^n$ with $a = \sum_{i=0}^{n-1} a_i X^i = (a_0, \dots, a_{n-1})$

Definition

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

- **Coordinates** f_i: $F = (f_0, \dots, f_{n-1})$

Example

$F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$, $x \mapsto x^3$

$$F = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{bmatrix} = \begin{bmatrix} x_0x_2 + x_1x_2 + x_1x_3 + x_0 \\ x_0x_1 + x_0x_2 + x_2x_3 + x_3 \\ x_0x_1 + x_0x_2 + x_1x_2 + x_0x_3 + x_1x_3 + x_2x_3 + x_2 \\ x_1x_3 + x_2x_3 + x_1 + x_2 + x_3 \end{bmatrix}$$

Definitions - 2

- **Degree of a Boolean Function** f: The degree of f as a polynomial in $\mathbb{F}_2[x_0, ..., x_{n-1}]/(x_0^2 + x_0, ..., x_{n-1}^2 + x_{n-1})$

Definitions - 2

- **Degree of a Boolean Function** f: The degree of f as a polynomial in $\mathbb{F}_2[x_0, ..., x_{n-1}]/(x_0^2 + x_0, ..., x_{n-1}^2 + x_{n-1})$

The Boolean function $f_0 = x_0x_2 + x_1x_2 + x_1x_3 + x_0$ has degree 2

Definitions - 2

- **Degree of a Boolean Function** f: The degree of f as a polynomial in $\mathbb{F}_2[x_0, ..., x_{n-1}]/(x_0^2 + x_0, ..., x_{n-1}^2 + x_{n-1})$

The Boolean function $f_0 = x_0x_2 + x_1x_2 + x_1x_3 + x_0$ has degree 2

- **Multivariate Degree of** F : The maximum of the degrees of f_i

Definitions - 2

- **Degree of a Boolean Function** f: The degree of f as a polynomial in $\mathbb{F}_2[x_0, ..., x_{n-1}]/(x_0^2 + x_0, ..., x_{n-1}^2 + x_{n-1})$

The Boolean function $f_0 = x_0x_2 + x_1x_2 + x_1x_3 + x_0$ has degree 2

- **Multivariate Degree of** F : The maximum of the degrees of f_i
- F is a **Quadratic Function** if its multivariate degree is 2

Definitions - 2

- **Degree of a Boolean Function** f: The degree of f as a polynomial in $\mathbb{F}_2[x_0, ..., x_{n-1}]/(x_0^2 + x_0, ..., x_{n-1}^2 + x_{n-1})$

The Boolean function $f_0 = x_0x_2 + x_1x_2 + x_1x_3 + x_0$ has degree 2

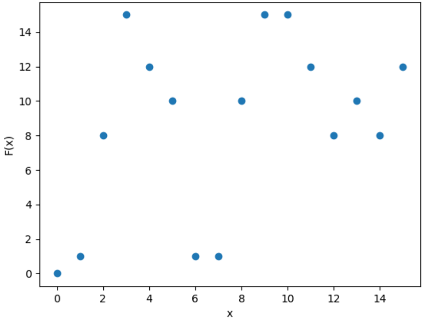
- **Multivariate Degree of** F : The maximum of the degrees of f_i
- F is a **Quadratic Function** if its multivariate degree is 2
- **Univariate Degree of** F: The degree over $\mathbb{F}_{2^n}[X]$

$F(x) = x^3$ has multivariate degree 2 and univariate degree 3

Definitions - 3

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

- **Graph of a Function**: $\Gamma_F = \{(x, F(x)) \mid x \in \mathbb{F}_2^n\}$



Equivalence Relations - 1

Equivalence Relations - 1

The cube for $n = 6$

Are $x^3 + C(x)$ and $x^6 = (x^2)^3$ different from x^3 ? $(a+b)^2 = a^2 + b^2$

Equivalence Relations - 1

The cube for $n = 6$

Are $x^3 + C(x)$ and $x^6 = (x^2)^3$ different from x^3 ? $(a+b)^2 = a^2 + b^2$

Extended-Affine Equivalence

F and G are *EA-equivalent* if there exist A, B affine permutations over $\mathbb{F}_2^n$ and C an affine mapping over $\mathbb{F}_2^n$ such that $G = B \circ F \circ A + C$. In terms of graph:

Equivalence Relations - 1

The cube for $n = 6$

Are $x^3 + C(x)$ and $x^6 = (x^2)^3$ different from x^3 ? $(a+b)^2 = a^2 + b^2$

Extended-Affine Equivalence

F and G are *EA-equivalent* if there exist A, B affine permutations over $\mathbb{F}_2^n$ and C an affine mapping over $\mathbb{F}_2^n$ such that $G = B \circ F \circ A + C$. In terms of graph:

$$\Gamma_G = \begin{bmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{bmatrix} (\Gamma_F)$$

Equivalence Relations - 1

The cube for $n = 6$

Are $x^3 + C(x)$ and $x^6 = (x^2)^3$ different from x^3 ? $(a+b)^2 = a^2 + b^2$

Extended-Affine Equivalence

F and G are *EA-equivalent* if there exist A, B affine permutations over $\mathbb{F}_2^n$ and C an affine mapping over $\mathbb{F}_2^n$ such that $G = B \circ F \circ A + C$. In terms of graph:

$$\Gamma_G = \begin{bmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{bmatrix} (\Gamma_F)$$

Such affine permutation over $\mathbb{F}_2^{2n}$ is called an **EA-mapping**.

Equivalence Relations - 1

The cube for $n = 6$

Are $x^3 + C(x)$ and $x^6 = (x^2)^3$ different from x^3 ? $(a+b)^2 = a^2 + b^2$

Extended-Affine Equivalence

F and G are *EA-equivalent* if there exist A, B affine permutations over $\mathbb{F}_2^n$ and C an affine mapping over $\mathbb{F}_2^n$ such that $G = B \circ F \circ A + C$. In terms of graph:

$$\Gamma_G = \begin{bmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{bmatrix} (\Gamma_F)$$

Such affine permutation over $\mathbb{F}_2^{2n}$ is called an **EA-mapping**.

For all EA-mappings

F is APN $\iff$ $B \circ F \circ A + C$ is APN, F and $B \circ F \circ A + C$ have same multivariate degree

Equivalence Relations - 2

Carlet-Charpin-Zinoviev (CCZ) Equivalence

F and G are *CCZ-equivalent* if there exist an affine bijection $\mathcal{A}$ over $\mathbb{F}_2^{2n}$ such that $\Gamma_G = \mathcal{A}(\Gamma_F)$, i.e :

$$\exists A, B, C, D \text{ affine}, \Gamma_G = \begin{bmatrix} A & D \\ C & B \end{bmatrix} (\Gamma_F)$$

- A mapping $\mathcal{A}$ is said to be **admissible** for F if $\mathcal{A}(\Gamma_F)$ is the graph of a function

Equivalence Relations - 2

Carlet-Charpin-Zinoviev (CCZ) Equivalence

F and G are *CCZ-equivalent* if there exist an affine bijection $\mathcal{A}$ over $\mathbb{F}_2^{2n}$ such that $\Gamma_G = \mathcal{A}(\Gamma_F)$, i.e :

$$\exists A, B, C, D \text{ affine}, \Gamma_G = \begin{bmatrix} A & D \\ C & B \end{bmatrix} (\Gamma_F)$$

- A mapping $\mathcal{A}$ is said to be **admissible** for F if $\mathcal{A}(\Gamma_F)$ is the graph of a function

For all admissible mappings

F is APN $\iff$ $\mathcal{A}(\Gamma_F)$ is the graph of an APN function

Equivalence Relations - 2

Carlet-Charpin-Zinoviev (CCZ) Equivalence

F and G are *CCZ-equivalent* if there exist an affine bijection $\mathcal{A}$ over $\mathbb{F}_2^{2n}$ such that $\Gamma_G = \mathcal{A}(\Gamma_F)$, i.e :

$$\exists A, B, C, D \text{ affine}, \Gamma_G = \begin{bmatrix} A & D \\ C & B \end{bmatrix} (\Gamma_F)$$

- A mapping $\mathcal{A}$ is said to be **admissible** for F if $\mathcal{A}(\Gamma_F)$ is the graph of a function

For all admissible mappings

F is APN $\iff$ $\mathcal{A}(\Gamma_F)$ is the graph of an APN function

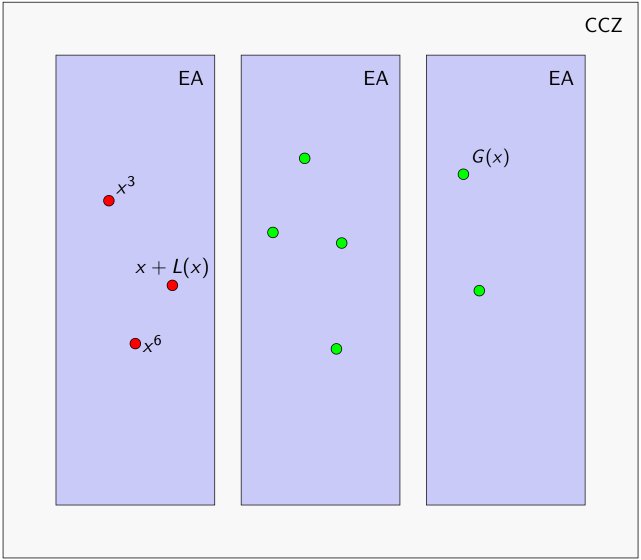
- A function is said to be **CCZ-quadratic** if it is CCZ-equivalent to a quadratic function

Equivalence - Summary

- Red Node: Quadratic function
- Green Node: Other degree
- Not all functions are represented

The cube for $n = 6$

- Exactly 3 EA-classes



Bestiary of APN CCZ-classes in numbers

A first lower bound

The number of CCZ classes of APN functions grows at least **exponentially** in the dimension (Kaspers and Zhou 2020).

Bestiary of APN CCZ-classes in numbers

A first lower bound

The number of CCZ classes of APN functions grows at least **exponentially** in the dimension (Kaspers and Zhou 2020).

Numbers, before 2025

- In dimension 6 : 13 CCZ-quadratic classes, 1 non CCZ-quadratic

Bestiary of APN CCZ-classes in numbers

A first lower bound

The number of CCZ classes of APN functions grows at least **exponentially** in the dimension (Kaspers and Zhou 2020).

Numbers, before 2025

- In dimension 6 : 13 CCZ-quadratic classes, 1 non CCZ-quadratic
- In dimension 7 : 488 CCZ-quadratic classes, 3 non CCZ-quadratic

Bestiary of APN CCZ-classes in numbers

A first lower bound

The number of CCZ classes of APN functions grows at least **exponentially** in the dimension (Kaspers and Zhou 2020).

Numbers, before 2025

- In dimension 6 : 13 CCZ-quadratic classes, 1 non CCZ-quadratic
- In dimension 7 : 488 CCZ-quadratic classes, 3 non CCZ-quadratic
- In dimension 8 : 32,892 CCZ-quadratic classes, 1 non CCZ-quadratic....

Bestiary of APN CCZ-classes in numbers

A first lower bound

The number of CCZ classes of APN functions grows at least **exponentially** in the dimension (Kaspers and Zhou 2020).

Numbers, before 2025

- In dimension 6 : 13 CCZ-quadratic classes, 1 non CCZ-quadratic
- In dimension 7 : 488 CCZ-quadratic classes, 3 non CCZ-quadratic
- In dimension 8 : 32,892 CCZ-quadratic classes, 1 non CCZ-quadratic....

In 2025, in dimension 8

- Beierle et al. found 3.8 millions inequivalent quadratic functions...

Bestiary of APN CCZ-classes in numbers

A first lower bound

The number of CCZ classes of APN functions grows at least **exponentially** in the dimension (Kaspers and Zhou 2020).

Numbers, before 2025

- In dimension 6 : 13 CCZ-quadratic classes, 1 non CCZ-quadratic
- In dimension 7 : 488 CCZ-quadratic classes, 3 non CCZ-quadratic
- In dimension 8 : 32,892 CCZ-quadratic classes, 1 non CCZ-quadratic....

In 2025, in dimension 8

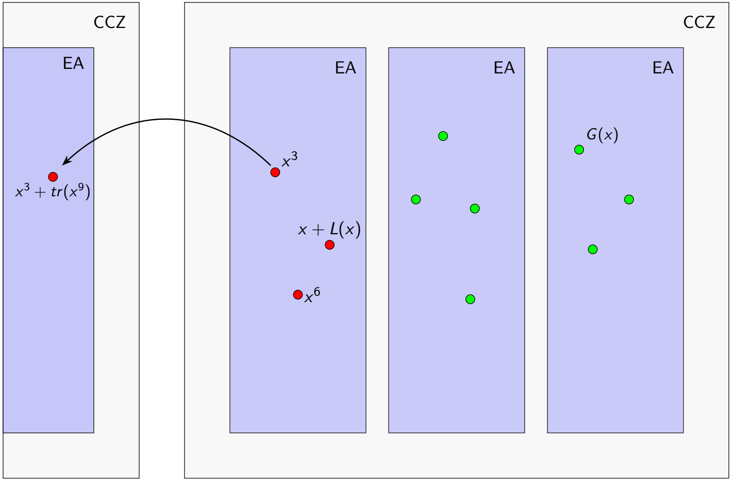
- Beierle et al. found 3.8 millions inequivalent quadratic functions...
- And they conjecture there are more !

What is a new function ?

- Red Node: Quadratic function
- Green Node: Other degree
- Not all functions are represented

A new function ?

With $tr(x) = \sum_{i=0}^{n-1} x^{2^i}$: $x^3 + tr(x^9)$ is not CCZ to x^3



Switching Neighbours

Switching Neighbours (Edel and Pott 2009)

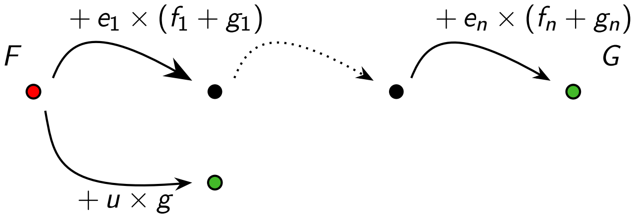
$u \in \mathbb{F}_2^n$, g a Boolean function, $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ APN, the function $F + u \times g$ is called an APN Switching Neighbour of F if it is an APN function.

Switching Neighbours

Switching Neighbours (Edel and Pott 2009)

$u \in \mathbb{F}_2^n$, g a Boolean function, $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ APN, the function $F + u \times g$ is called an APN Switching Neighbour of F if it is an APN function.

Since $F + G = \sum_{i=1}^{n} e_i \times (f_i + g_i)$:

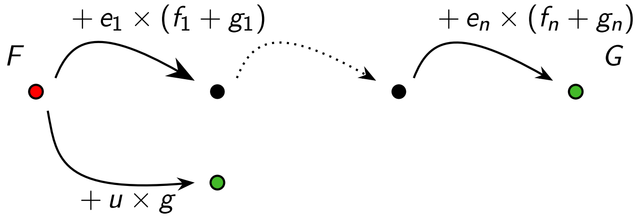


Switching Neighbours

Switching Neighbours (Edel and Pott 2009)

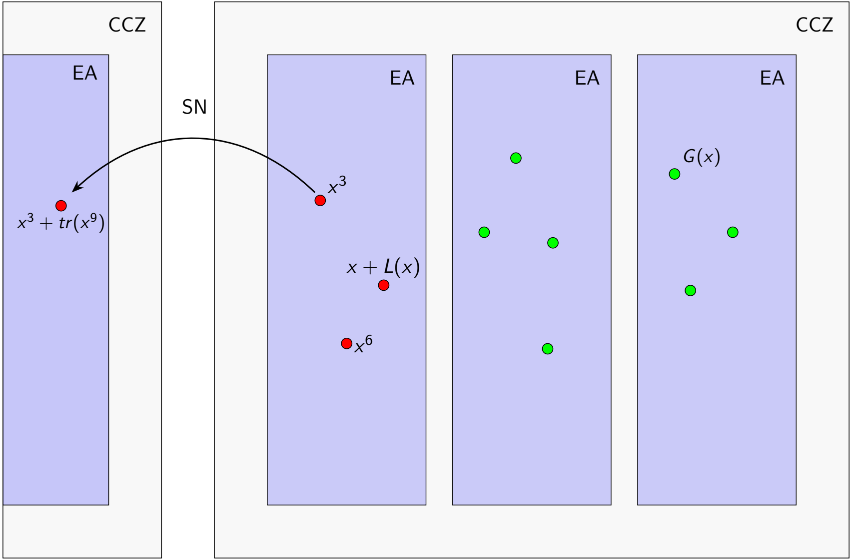
$u \in \mathbb{F}_2^n$, g a Boolean function, $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ APN, the function $F + u \times g$ is called an APN Switching Neighbour of F if it is an APN function.

Since $F + G = \sum_{i=1}^{n} e_i \times (f_i + g_i)$:



- Used to find the only known non-CCZ-quadratic APN in dimension 6 [EP09].
- Example: $x^3 + 1 \times tr(x^9)$, since $tr(x) = \sum_{i=0}^{n-1} x^{2^i}$ is a Boolean function

Exploration - Summary



Can we do it starting from the 3.8 millions function in dimension 8 ?

Could it be feasible ?

Problems

- Too many CCZ equivalent functions

Could it be feasible ?

Problems

- Too many CCZ equivalent functions
- Too many Switching Neighbours

Could it be feasible ?

Problems

- Too many CCZ equivalent functions
- Too many Switching Neighbours
- Bad performances with off-the-shelf implementations

Could it be feasible ?

Problems

- Too many CCZ equivalent functions
- Too many Switching Neighbours
- Bad performances with off-the-shelf implementations

Our contributions

- We provide algorithms to efficiently explore CCZ-classes

Could it be feasible ?

Problems

- Too many CCZ equivalent functions
- Too many Switching Neighbours
- Bad performances with off-the-shelf implementations

Our contributions

- We provide algorithms to efficiently explore CCZ-classes
- We provide theoretic improvements and algorithms to compute Switching Neighbours

Could it be feasible ?

Problems

- Too many CCZ equivalent functions
- Too many Switching Neighbours
- Bad performances with off-the-shelf implementations

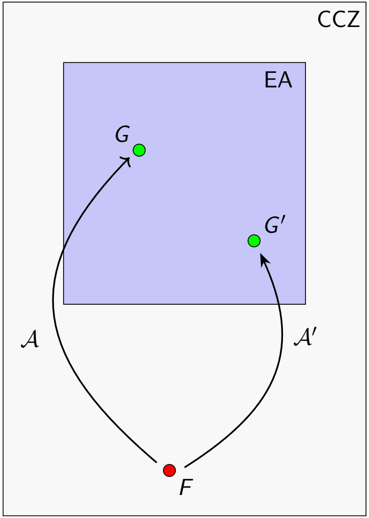
Our contributions

- We provide algorithms to efficiently explore CCZ-classes
- We provide theoretic improvements and algorithms to compute Switching Neighbours
- We provide public C++ implementations with SAGE bindings for all these algorithms

sboxU

- Library for S-box analysis, with all the implementations of this talk
- Available here: https://github.com/lpp-crypto/sboxU/

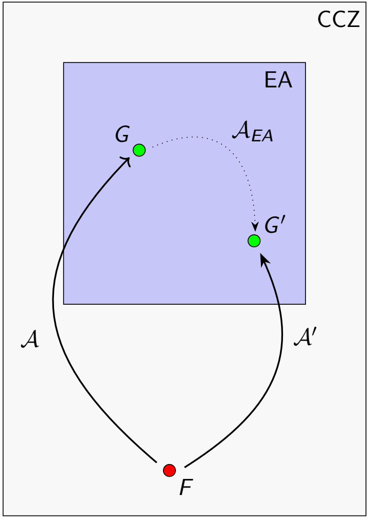
CCZ Class : What is the Problem ?



Fact

We know how to build admissible mappings, $\mathcal{A}, \mathcal{A}'$

CCZ Class : What is the Problem ?

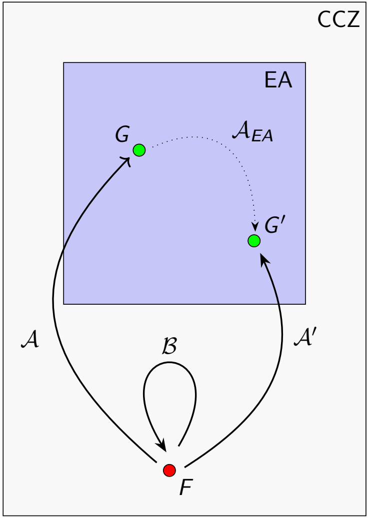


Fact

We know how to build admissible mappings, $\mathcal{A}, \mathcal{A}'$

- Naively: $\mathcal{A}_{EA} = \mathcal{A} \circ \mathcal{A}'^{-1}$

CCZ Class : What is the Problem ?



Fact

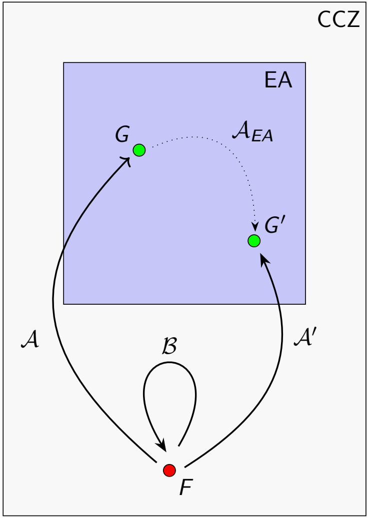
We know how to build admissible mappings, $\mathcal{A}, \mathcal{A}'$

- Naively: $\mathcal{A}_{EA} = \mathcal{A} \circ \mathcal{A}'^{-1}$

$\mathrm{Aut}(F)$

$\mathcal{B} \in \mathrm{Aut}(F) \iff \mathcal{B}(\Gamma_F) = \Gamma_F$

CCZ Class : What is the Problem ?



Fact

We know how to build admissible mappings, $\mathcal{A}, \mathcal{A}'$

- Naively: $\mathcal{A}_{EA} = \mathcal{A} \circ \mathcal{A}'^{-1}$

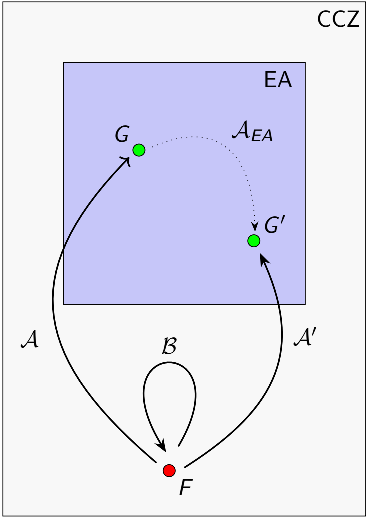
$\mathrm{Aut}(F)$

$\mathcal{B} \in \mathrm{Aut}(F) \iff \mathcal{B}(\Gamma_F) = \Gamma_F$

- Hence, the EA-mappings are:

$$\mathcal{A} \circ \mathcal{B} \circ \mathcal{A}'^{-1}$$

CCZ Class : What is the Problem ?



Fact

We know how to build admissible mappings, $\mathcal{A}, \mathcal{A}'$

- Naively: $\mathcal{A}_{EA} = \mathcal{A} \circ \mathcal{A}'^{-1}$

$\mathrm{Aut}(F)$

$\mathcal{B} \in \mathrm{Aut}(F) \iff \mathcal{B}(\Gamma_F) = \Gamma_F$

- Hence, the EA-mappings are:

$$\mathcal{A} \circ \mathcal{B} \circ \mathcal{A}'^{-1}$$

We have to compute $\mathrm{Aut}(F)$ to quotient, but can we do it efficiently ?

CCZ class: Solutions

A lot of technical details

- Tailored for quadratic functions, using an auxiliary function called ortho-derivative.

CCZ class: Solutions

A lot of technical details

- Tailored for quadratic functions, using an auxiliary function called ortho-derivative.
- The recovery involves spectral analysis with discrete Fourier transform

Takeaway

- We can compute efficiently $\mathrm{Aut}(F)$ for F quadratic
- We can compute one EA representative per EA class

Switching Neighbours: What is the Problem ?

Way to many uninteresting functions !

- If f is affine, $F + u \times f$ is EA-equivalent to F

Switching Neighbours: What is the Problem ?

Way to many uninteresting functions !

- If f is affine, $F + u \times f$ is EA-equivalent to F
- Another example : $F + e_0 \times f_0 = (f_0 + f_1, f_1, .., f_{n-1})$

Switching Neighbours: What is the Problem ?

Way to many uninteresting functions !

- If f is affine, $F + u \times f$ is EA-equivalent to F
- Another example : $F + e_0 \times f_0 = (f_0 + f_1, f_1, .., f_{n-1})$

Algorithmic problems

- Off-the-shelf algorithms are not efficient
- No filters for the uninteresting functions

Switching Neighbours: Solutions

A lot of technical details

- We characterize the affine space of uninteresting functions

Switching Neighbours: Solutions

A lot of technical details

- We characterize the affine space of uninteresting functions
- We propose a simple way to filter them

Switching Neighbours: Solutions

A lot of technical details

- We characterize the affine space of uninteresting functions
- We propose a simple way to filter them
- We propose a new algorithm to compute switching neighbours based on random sampling

Switching Neighbours: Solutions

A lot of technical details

- We characterize the affine space of uninteresting functions
- We propose a simple way to filter them
- We propose a new algorithm to compute switching neighbours based on random sampling

Takeaway

- We gain a factor 2^{3n} on the number of switching neighbours that we need to check **per function**

Switching Neighbours: Solutions

A lot of technical details

- We characterize the affine space of uninteresting functions
- We propose a simple way to filter them
- We propose a new algorithm to compute switching neighbours based on random sampling

Takeaway

- We gain a factor 2^{3n} on the number of switching neighbours that we need to check **per function**
- The new algorithm is 2^n times faster than the state of the art

CCZ classes for $\mathbb{F}_2^6$ and $\mathbb{F}_2^7$

$\mathbb{F}_2^6$

- We found all the 716 EA-classes in the union of the 14 known CCZ-equivalence classes (same as Calderini in 2020)

CCZ classes for $\mathbb{F}_2^6$ and $\mathbb{F}_2^7$

$\mathbb{F}_2^6$

- We found all the 716 EA-classes in the union of the 14 known CCZ-equivalence classes (same as Calderini in 2020)
- It is very important: reproductibility in experiments is key

CCZ classes for $\mathbb{F}_2^6$ and $\mathbb{F}_2^7$

$\mathbb{F}_2^6$

- We found all the 716 EA-classes in the union of the 14 known CCZ-equivalence classes (same as Calderini in 2020)
- It is very important: reproductibility in experiments is key

$\mathbb{F}_2^7$

- 488 EA-classes of quadratic APN functions.

CCZ classes for $\mathbb{F}_2^6$ and $\mathbb{F}_2^7$

$\mathbb{F}_2^6$

- We found all the 716 EA-classes in the union of the 14 known CCZ-equivalence classes (same as Calderini in 2020)
- It is very important: reproductibility in experiments is key

$\mathbb{F}_2^7$

- 488 EA-classes of quadratic APN functions.
- New : The union of their CCZ-classes contains a total of 82,409 EA-classes

CCZ classes for $\mathbb{F}_2^6$ and $\mathbb{F}_2^7$

$\mathbb{F}_2^6$

- We found all the 716 EA-classes in the union of the 14 known CCZ-equivalence classes (same as Calderini in 2020)
- It is very important: reproductibility in experiments is key

$\mathbb{F}_2^7$

- 488 EA-classes of quadratic APN functions.
- New : The union of their CCZ-classes contains a total of 82,409 EA-classes

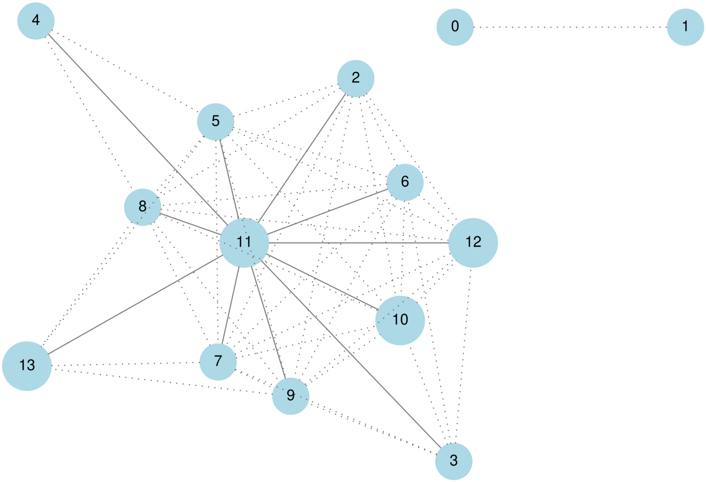
sboxU - For reproducibility

These classes are stored un tinySQL databases in sboxU !

For $\mathbb{F}_2^6$ - CCZ-Switching Neighbours Graph

- Node: CCZ class
- Edge: SN between classes
- Labels: Number in the DB

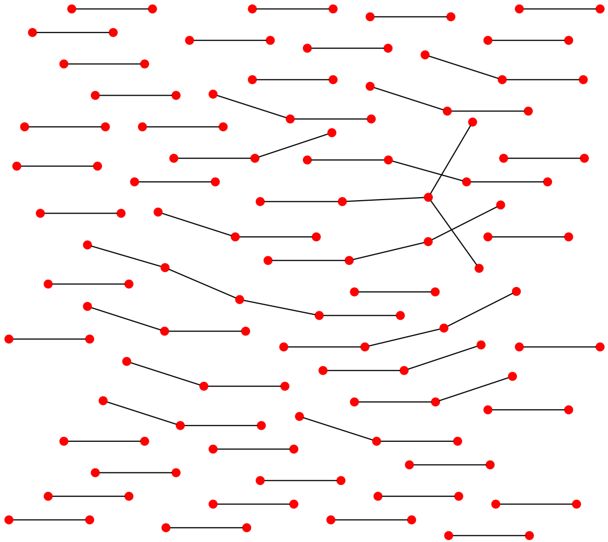
- 0: The cube
- 4: The Kim mapping
- 13: Only non CCZ-quadratic



For $\mathbb{F}_2^7$ - CCZ-Switching Neighbours Graph

- Node: CCZ-Quadratic Class
- Edge: SN between functions

About 10% have switching neighbours



For $\mathbb{F}_2^8$ - Problems

Size Concerns

- We have 3.8 millions new starting-points, but...

For $\mathbb{F}_2^8$ - Problems

Size Concerns

- We have 3.8 millions new starting-points, but...
- The CCZ-classes of these functions contain roughly 300 EA-classes

For $\mathbb{F}_2^8$ - Problems

Size Concerns

- We have 3.8 millions new starting-points, but...
- The CCZ-classes of these functions contain roughly 300 EA-classes
- It takes roughly 0.6s to compute the switching neighbours of a 8-bit function

- $300 \times 0.6 \times 3.8 \times 10^6 \approx 7917$days of computations

For $\mathbb{F}_2^8$ - Experiments on Quadratic Functions

For quadratic functions only

- $0.6 \times 3.8 \times 10^6 \approx 26$ days of computations

For $\mathbb{F}_2^8$ - Experiments on Quadratic Functions

For quadratic functions only

- $0.6 \times 3.8 \times 10^6 \approx 26$ days of computations
- Parallelized on one node of the grid5000 cluster for about a day

For $\mathbb{F}_2^8$ - Experiments on Quadratic Functions

For quadratic functions only

- $0.6 \times 3.8 \times 10^6 \approx 26$ days of computations
- Parallelized on one node of the grid5000 cluster for about a day

We found new functions !

- Among the 3.8 millions, only 1% of them have non trivial switching neighbours

For $\mathbb{F}_2^8$ - Experiments on Quadratic Functions

For quadratic functions only

- $0.6 \times 3.8 \times 10^6 \approx 26$ days of computations
- Parallelized on one node of the grid5000 cluster for about a day

We found new functions !

- Among the 3.8 millions, only 1% of them have non trivial switching neighbours
- Among these switching neighbours, about 10% of them were new

For $\mathbb{F}_2^8$ - Experiments on Quadratic Functions

For quadratic functions only

- $0.6 \times 3.8 \times 10^6 \approx 26$ days of computations
- Parallelized on one node of the grid5000 cluster for about a day

We found new functions !

- Among the 3.8 millions, only 1% of them have non trivial switching neighbours
- Among these switching neighbours, about 10% of them were new

However

These functions are all CCZ-quadratic and none is CCZ-equivalent to a bijection

For $\mathbb{F}_2^8$ - As is the tradition

[0,0,180,132,180,244,96,16,180,188,76,116,118,62,238,150,180,141,196,205,
103,30,119,62,144,161,172,173,53,68,105,40,107,243,216,112,156,68,79,167,
70,214,185,25,199,23,88,184,225,64,150,7,113,144,102,183,92,245,103,254,
186,83,225,56,180,185,152,165,58,119,118,11,148,145,244,193,108,41,108,
25,22,34,254,250,255,139,119,51,166,154,2,14,57,69,253,177,169,60,130,
39,100,177,47,202,16,141,119,218,171,118,172,65,53,153,218,70,159,115,
16,204,28,184,191,43,192,36,3,215,223,156,22,101,115,112,218,233,131,
200,6,125,89,82,188,135,75,49,70,12,128,186,237,231,135,245,198,132,
58,8,27,25,50,233,252,23,221,70,115,216,247,36,117,150,110,253,140,47,
152,122,146,64,16,178,122,232,205,39,139,81,51,153,21,143,66,12,19,109,
212,218,229,219,138,204,151,225,106,108,23,33,192,183,85,18,49,6,196,195,
152,231,65,14,31,32,166,169,217,15,143,105,12,154,58,156,136,86,146,124,
43,181,81,255,101,138,247,40,215,120,37,186,164,67,122,173,96,199,222,73]

sboxU v2 advert

- C++ optimized code
- Databases in tinySQL available for $n = 6$ and $n = 7$
- All the code needed to replicate our experiments
- Many more for S-box analysis

https://github.com/lpp-crypto/sboxU

- A lot of people involved from COSMIQ: Léo, Merlin, Guilhem, me
- And from faraway: Jules, Xavier, Baptiste G.
- Improved structure: it will be easier to contribute, help !
- What do YOU want to see implemented ?

Admissible Mapping and LAT

Linear Approximation Table (LAT)

The LAT is the table of the values $W_F(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot F(x)}$, where $\cdot$ is the usual scalar product over $\mathbb{F}_2^n$.

Admissible Mapping and LAT

Linear Approximation Table (LAT)

The LAT is the table of the values $W_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot F(x)}$, where $\cdot$ is the usual scalar product over $\mathbb{F}_2^n$.

- $\mathcal{V} := \{(x,0), x \in \mathbb{F}_2^n\}$
- The set of Walsh Zeroes $\mathcal{Z}_F := \{(\alpha,\beta) \mid W_F(\alpha,\beta) = 0\} \cup \{(0,0)\}$
- $\mathcal{V} \subset \mathcal{Z}_F$

Admissible Mapping and LAT

Linear Approximation Table (LAT)

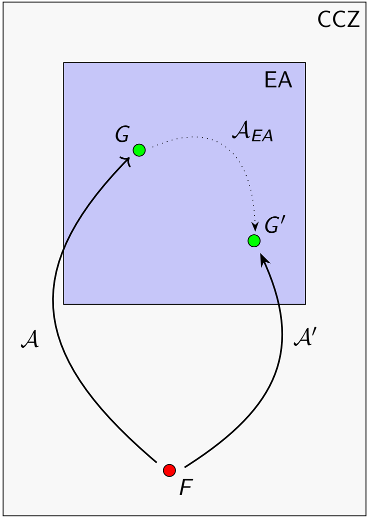
The LAT is the table of the values $W_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot F(x)}$, where $\cdot$ is the usual scalar product over $\mathbb{F}_2^n$.

- $\mathcal{V} := \{(x,0), x \in \mathbb{F}_2^n\}$
- The set of Walsh Zeroes $\mathcal{Z}_F := \{(\alpha,\beta) \mid W_F(\alpha,\beta) = 0\} \cup \{(0,0)\}$
- $\mathcal{V} \subset \mathcal{Z}_F$

Admissibility Criterion [CP19]

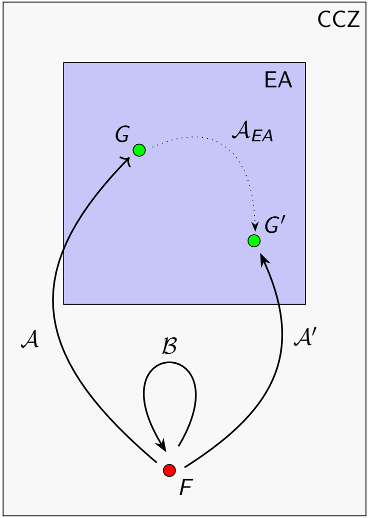
The mapping $\mathcal{A}$ is admissible for F if and only if $\mathcal{A}^\top(\mathcal{V}) \subset \mathcal{Z}_F$.

Filtering with Walsh Zeroes



- Admissible: $\mathcal{A}^\top(\mathcal{V}) \subset \mathcal{Z}_F$
- For G: $\mathcal{A}^\top(\mathcal{V}) = V$
- For G': $\mathcal{A}'^\top(\mathcal{V}) = V'$

Filtering with Walsh Zeroes

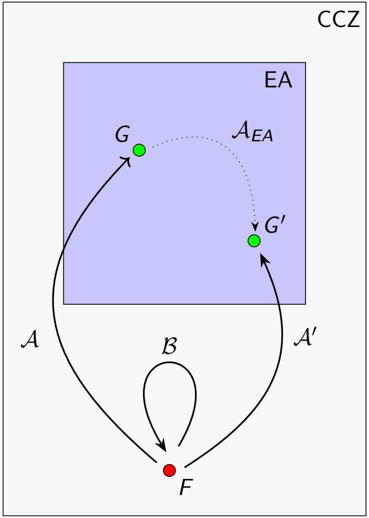


- Admissible: $\mathcal{A}^\top(\mathcal{V}) \subset \mathcal{Z}_F$
- For G: $\mathcal{A}^\top(\mathcal{V}) = V$
- For G': $\mathcal{A}'^\top(\mathcal{V}) = V'$

Proposition (refined from [CP19])

G and G' are EA-equivalent if and only if there exists $\mathcal{B} \in \mathrm{Aut}(F)$ such that $\mathcal{B}^\top(V) = V'$.

Filtering with Walsh Zeroes



- Admissible: $\mathcal{A}^\top(\mathcal{V}) \subset \mathcal{Z}_F$
- For G: $\mathcal{A}^\top(\mathcal{V}) = V$
- For G': ${\mathcal{A}'}^\top(\mathcal{V}) = V'$

Proposition (refined from [CP19])

G and G' are EA-equivalent if and only if there exists $\mathcal{B} \in \mathrm{Aut}(F)$ such that $\mathcal{B}^\top(V) = V'$.

Advantages

- Easier to test
- We already have an algorithm to search for the V [BPT19]

Filtering EA-equivalent functions

Filtering Algorithm

1. Compute all the vector spaces V_i of dimension n in $\mathcal{Z}_F$ (using [BPT19])

Filtering EA-equivalent functions

Filtering Algorithm

1. Compute all the vector spaces V_i of dimension n in $\mathcal{Z}_F$ (using [BPT19])
2. For all V_i and for all $\mathcal{B} \in \mathrm{Aut}(F)$, check if there exists k such that $\mathcal{B}^T(V_i) = V_k$. If it is the case, then remove V_k from the list of vector spaces.

Filtering EA-equivalent functions

Filtering Algorithm

1. Compute all the vector spaces V_i of dimension n in $\mathcal{Z}_F$ (using [BPT19])
2. For all V_i and for all $\mathcal{B} \in \mathrm{Aut}(F)$, check if there exists k such that $\mathcal{B}^T(V_i) = V_k$. If it is the case, then remove V_k from the list of vector spaces.
3. Loop over all remaining spaces V_i, build a corresponding admissible mapping, *i.e.* satisfying $\mathcal{A}^\top(\mathcal{V}) = V_i$.

Filtering EA-equivalent functions

Filtering Algorithm

1. Compute all the vector spaces V_i of dimension n in $\mathcal{Z}_F$ (using [BPT19])
2. For all V_i and for all $\mathcal{B} \in \mathrm{Aut}(F)$, check if there exists k such that $\mathcal{B}^T(V_i) = V_k$. If it is the case, then remove V_k from the list of vector spaces.
3. Loop over all remaining spaces V_i, build a corresponding admissible mapping, *i.e.* satisfying $\mathcal{A}^\top(\mathcal{V}) = V_i$.

Since we have almost only quadratic functions

How to compute the automorphism group Aut of quadratic functions ?

$\mathrm{Aut}(F) = \mathrm{Aut}_{\mathrm{EA}}(F)$

$\mathrm{Aut}_{\mathrm{EA}} \subset \mathrm{Aut}$: Automorphisms that are EA-mappings

$\mathrm{Aut}(F) = \mathrm{Aut}_{\mathrm{EA}}(F)$

$\mathrm{Aut}_{\mathrm{EA}} \subset \mathrm{Aut}$: Automorphisms that are EA-mappings

Theorem (CCZ equivalence of quadratic APN)

Let $n \geqslant 4$. Let $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be quadratic APN mappings. Then:

(i) Any automorphism of F is an EA-mapping: $\mathrm{Aut}(F) = \mathrm{Aut}_{\mathrm{EA}}(F)$ [KZ21]

(ii) if $\mathcal{A}$ is an admissible mapping satisfying $\mathcal{A}(\Gamma_F) = \Gamma_G$, then $\mathcal{A}$ is an EA-mapping.

$\mathrm{Aut}(F) = \mathrm{Aut}_{\mathrm{EA}}(F)$

$\mathrm{Aut}_{\mathrm{EA}} \subset \mathrm{Aut}$: Automorphisms that are EA-mappings

Theorem (CCZ equivalence of quadratic APN)

Let $n \geqslant 4$. Let $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be quadratic APN mappings. Then:

(i) Any automorphism of F is an EA-mapping: $\mathrm{Aut}(F) = \mathrm{Aut}_{\mathrm{EA}}(F)$ [KZ21]

(ii) if $\mathcal{A}$ is an admissible mapping satisfying $\mathcal{A}(\Gamma_F) = \Gamma_G$, then $\mathcal{A}$ is an EA-mapping.

There is only one EA-class of quadratic functions in a CCZ-class, like it is for x^3

$\mathrm{Aut}(F)$ and $\mathrm{Aut}(\pi_F)$

Definition (Ortho-derivative)

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic APN function. The *ortho-derivative* of F is the function $\pi_F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ where $\pi_F(0) = 0$ and where for any $a \in (\mathbb{F}_2^n)^*$, $\pi_F(a)$ is the only non-zero element satisfying:

$$\pi_F(a) \cdot \big(F(x+a) + F(x) + F(a) + F(0)\big) \;=\; 0 \quad \forall\, x \in \mathbb{F}_2^n\,. \tag{1}$$

$\mathrm{Aut}(F)$ and $\mathrm{Aut}(\pi_F)$

Definition (Ortho-derivative)

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic APN function. The *ortho-derivative* of F is the function $\pi_F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ where $\pi_F(0) = 0$ and where for any $a \in (\mathbb{F}_2^n)^*$, $\pi_F(a)$ is the only non-zero element satisfying:

$$\pi_F(a) \cdot \big(F(x+a) + F(x) + F(a) + F(0)\big) \;=\; 0 \quad \forall\, x \in \mathbb{F}_2^n\,. \tag{1}$$

$\mathrm{Aut}(F)$ and $\mathrm{Aut}_{\mathrm{LE}}(\pi_F)$ [CCP22]

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic APN function, if $F = B \circ F \circ A + C$, then π_F satisfies $\pi_F = B^T \circ \pi_F \circ A^{-1}$.

LAT of π_f and Computing $\mathrm{Aut}(\pi_F)$

The LAT of π_F looks like the LAT of random functions: they have large and 'rarer' coefficients.

LAT of π_f and Computing $\mathrm{Aut}(\pi_F)$

The LAT of π_F looks like the LAT of random functions: they have large and 'rarer' coefficients.

SboxU demonstration

The LAT of the Kim mapping and its ortho-derivative

Computing $\mathrm{Aut}(\pi_F)$ (as in [HK22])

- Coefficients of the same value are mapped to each other

LAT of π_f and Computing $\mathrm{Aut}(\pi_F)$

The LAT of π_F looks like the LAT of random functions: they have large and 'rarer' coefficients.

SboxU demonstration

The LAT of the Kim mapping and its ortho-derivative

Computing $\mathrm{Aut}(\pi_F)$ (as in [HK22])

- Coefficients of the same value are mapped to each other
- It put constraints on A and B quite fast since the batches of coefficients are small

LAT of π_f and Computing $\mathrm{Aut}(\pi_F)$

The LAT of π_F looks like the LAT of random functions: they have large and 'rarer' coefficients.

SboxU demonstration

The LAT of the Kim mapping and its ortho-derivative

Computing $\mathrm{Aut}(\pi_F)$ (as in [HK22])

- Coefficients of the same value are mapped to each other
- It put constraints on A and B quite fast since the batches of coefficients are small
- Very fast algorithm for ortho-derivatives in our experiments

Computing the Group of Automorphisms

Computing $\mathrm{Aut}(E)$

1. Compute the ortho-derivative π_F of the target function F.

Computing the Group of Automorphisms

Computing $\mathrm{Aut}(E)$

1. Compute the ortho-derivative π_F of the target function F.
2. Find all the pairs of linear permutations B^T and A^{-1} such that $B^T \circ \pi_F \circ A^{-1} = \pi_F$.

Computing the Group of Automorphisms

Computing $\mathrm{Aut}(E)$

1. Compute the ortho-derivative π_F of the target function F.
2. Find all the pairs of linear permutations B^T and A^{-1} such that $B^T \circ \pi_F \circ A^{-1} = \pi_F$.
3. For all $\delta \in \mathbb{F}_2^n$, compute the values of the function C such that $C(x) = F(x + \delta) + B \circ F \circ A(x)$. If C is affine, then we have just deduced an automorphism $\mathcal{A}$ of F.

Computing the Group of Automorphisms

Computing $\mathrm{Aut}(E)$

1. Compute the ortho-derivative π_F of the target function F.
2. Find all the pairs of linear permutations B^T and A^{-1} such that $B^T \circ \pi_F \circ A^{-1} = \pi_F$.
3. For all $\delta \in \mathbb{F}_2^n$, compute the values of the function C such that $C(x) = F(x + \delta) + B \circ F \circ A(x)$. If C is affine, then we have just deduced an automorphism $\mathcal{A}$ of F.

Available in sboxU

`graph_automorphisms_of_apn_quadratic`

Xavier Bonnetain, Léo Perrin, and Shizhu Tian.
Anomalies and vector space search: Tools for S-box analysis.
In *Advances in Cryptology – ASIACRYPT 2019*, Cham, 2019. Springer International Publishing.

Anne Canteaut, Alain Couvreur, and Léo Perrin.
Recovering or testing extended-affine equivalence.
IEEE Transactions on Information Theory, 68(9):6187–6206, 2022.

Anne Canteaut and Léo Perrin.
On CCZ-equivalence, extended-affine equivalence, and function twisting.
Finite Fields and Their Applications, 56:209–246, 2019.

Yves Edel and Alexander Pott.
A new almost perfect nonlinear function which is not quadratic.
Adv. Math. Commun., 3(1):59–81, 2009.

Marie Heggebakk and Nikolay Kaleyski.
Testing linear and affine equivalence.

In *BFA 2022: The 7th International Workshop on Boolean Functions and their Applications*, Balestrand, Norway, September 2022.
https://boolean.w.uib.no/bfa-2022/.

Christian Kaspers and Yue Zhou.
The number of almost perfect nonlinear functions grows exponentially.
J. Cryptol., 34(1):4, 2021.