

Irene Villa

#### Introduction Vectorial Boolean Eunctions

On anticrookedness

On APN permutations

Sketch of proof

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

## Vectorial Boolean Functions in even dimension

Irene Villa

Università degli Studi di Trento



Irene Villa

Introduction

Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof







Irene Villa

Introduction

ALICE

Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

BOB





Irene Villa

Introduction

Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

#### Communicate a secret message



・ロト・雪・・ヨト ・雪・ ・ロト



Introduction

# SECRET MESSAGE 1001110101001011010010011011110 EVE ▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

ALICE

Communicate a secret message

BOB



Irene Villa

#### Introduction

Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

## Cipher:

・ロト・雪・・ヨト ・雪・ ・ロト



Irene Villa

Introduction

Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

## Cipher:

•  $\mathcal{M} = \mathbb{F}^n$  set of messages over an alphabet  $\mathbb{F}$ 



#### Cipher:

- $\mathcal{M} = \mathbb{F}^n$  set of messages over an alphabet  $\mathbb{F}$
- $\varphi_k : \mathcal{M} \to \mathcal{M}$  encryption function,  $k \in \mathcal{K}$  key-space

Vectorial Boolean Functions in even dimension

Irene Villa

#### Introduction

Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof



Cipher:

- $\mathcal{M} = \mathbb{F}^n$  set of messages over an alphabet  $\mathbb{F}$
- $\varphi_k : \mathcal{M} \to \mathcal{M}$  encryption function,  $k \in \mathcal{K}$  key-space  $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$

Vectorial Boolean Functions in even dimension

Irene Villa

#### Introduction

Vectorial Boolean Functions

On anticrookedness

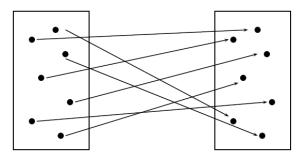
On APN permutations

Sketch of proof



#### Cipher:

- $\mathcal{M} = \mathbb{F}^n$  set of messages over an alphabet  $\mathbb{F}$
- $\varphi_k : \mathcal{M} \to \mathcal{M}$  encryption function,  $k \in \mathcal{K}$  key-space  $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction

Vectorial Boolean Functions

On anticrookedness

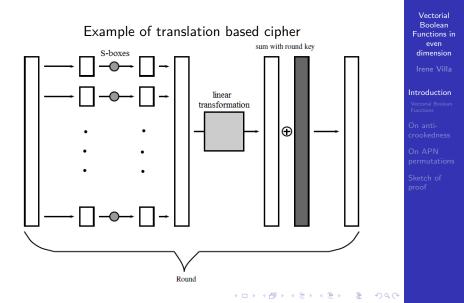
On APN permutations

Sketch of proof

・ロト・日本・日本・日本・日本・日本

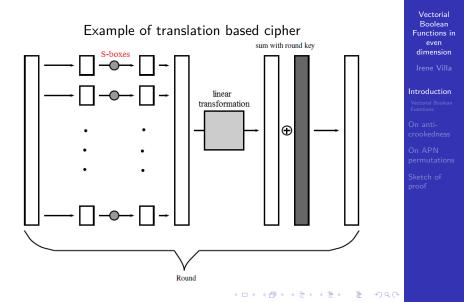
**Block ciphers** 





**Block ciphers** 







A Cipher is considered secure if an attacker cannot understand  $\varphi_k$  (or k) from

## $\{P, \varphi_k(P)\}_{P \in X}$

with X small subset of  $\mathcal{M}$ .

Vectorial Boolean Functions in even dimension

Irene Villa

Introduction

Vectorial Boolean Functions

On anticrookedness

On APN permutations

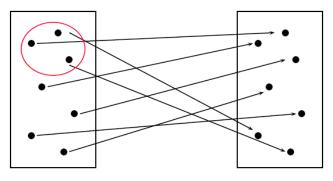
Sketch of proof



A Cipher is considered secure if an attacker cannot understand  $\varphi_k$  (or k) from

 $\{P, \varphi_k(P)\}_{P \in X}$ 

with X small subset of  $\mathcal{M}$ .



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction

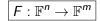
Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?





Vectorial Boolean Functions in even dimension

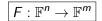
Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof



#### coordinate function



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

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

## coordinate function $F(x) = (f_1(x), \dots, f_m(x))$



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

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

coordinate function  $F(x) = (f_1(x), \dots, f_m(x))$ 

component function



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

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

coordinate function  $F(x) = (f_1(x), \dots, f_m(x))$ 

component function  $\lambda \in \mathbb{F}^m$   $f_{\lambda}(x) = F(x) \cdot \lambda$ 



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

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

coordinate function  $F(x) = (f_1(x), \dots, f_m(x))$ 

 $\begin{array}{c} \text{component function} \\ \lambda \in \mathbb{F}^m \quad f_{\lambda}(x) = F(x) \cdot \lambda \end{array}$ 

#### degree



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

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

coordinate function  $F(x) = (f_1(x), \dots, f_m(x))$ 

component function  $\lambda \in \mathbb{F}^m \quad f_{\lambda}(x) = F(x) \cdot \lambda$ 

 $\frac{\mathsf{degree}}{\mathsf{deg}(F) = \mathsf{max}_{\lambda} \mathsf{deg}(f_{\lambda})}$ 



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

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

coordinate function  $F(x) = (f_1(x), \dots, f_m(x))$ 

component function  $\lambda \in \mathbb{F}^m \quad f_{\lambda}(x) = F(x) \cdot \lambda$ 

 $\frac{\mathsf{degree}}{\mathsf{deg}(F) = \mathsf{max}_{\lambda} \mathsf{deg}(f_{\lambda})}$ 

permutation



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

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

coordinate function  $F(x) = (f_1(x), \dots, f_m(x))$ 

component function  $\lambda \in \mathbb{F}^m \quad f_{\lambda}(x) = F(x) \cdot \lambda$ 

## $\frac{\mathsf{degree}}{\mathsf{deg}(F) = \mathsf{max}_{\lambda} \mathsf{deg}(f_{\lambda})}$

permutation  $\deg(F) \le n-1$ 



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

◆□▶ ◆□▶ ◆三▶ ◆三▶ ○ ● ●

#### Derivative



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

 $a \in \mathbb{F}^n \smallsetminus \{0\}$ 

#### Derivative

$$D_aF(x) = F(x) + F(x+a)$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

#### Derivative

$$a \in \mathbb{F}^n \setminus \{0\}$$
  $D_a F(x) = F(x) + F(x+a)$ 

Uniform differentiability



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

#### Derivative

$$a \in \mathbb{F}^n \setminus \{0\}$$
  $D_a F(x) = F(x) + F(x+a)$ 

#### Uniform differentiability

$$\delta = \max_{a,b} |\{x \in \mathbb{F}^n : D_a F(x) = b\}|$$



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

#### Derivative

$$a \in \mathbb{F}^n \setminus \{0\}$$
  $D_a F(x) = F(x) + F(x+a)$ 

Uniform differentiability

$$\delta = \max_{a,b} |\{x \in \mathbb{F}^n : D_a F(x) = b\}|$$

Weakly uniform differentiability



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

#### Derivative

$$a \in \mathbb{F}^n \setminus \{0\}$$
  $D_a F(x) = F(x) + F(x+a)$ 

#### Uniform differentiability

$$\delta = \max_{a,b} |\{x \in \mathbb{F}^n : D_a F(x) = b\}|$$

Weakly uniform differentiability

$$\forall a \in \mathbb{F}^n \setminus \{0\} \quad |\mathrm{Im}(D_a F)| > \frac{2^{n-1}}{\delta}$$



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

#### Derivative

$$a \in \mathbb{F}^n \setminus \{0\}$$
  $D_a F(x) = F(x) + F(x+a)$ 

Uniform differentiability

$$\delta = \max_{a,b} |\{x \in \mathbb{F}^n : D_a F(x) = b\}|$$

Weakly uniform differentiability

$$\forall a \in \mathbb{F}^n \setminus \{0\} \quad |\mathrm{Im}(D_a F)| > \frac{2^{n-1}}{\delta}$$

(日)

Anti-crookedness (AC)



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

#### Derivative

$$a \in \mathbb{F}^n \setminus \{0\}$$
  $D_a F(x) = F(x) + F(x+a)$ 

Uniform differentiability

$$\delta = \max_{a,b} |\{x \in \mathbb{F}^n : D_a F(x) = b\}|$$

Weakly uniform differentiability

$$\forall a \in \mathbb{F}^n \setminus \{0\} \quad |\mathrm{Im}(D_a F)| > \frac{2^{n-1}}{\delta}$$

Anti-crookedness (AC)

 $\forall a \in \mathbb{F}^n \setminus \{0\} \quad \mathrm{Im}(D_a F) \text{ not affine subspace of } \mathbb{F}^n$ 

<ロト < 同ト < 回ト < 回ト = 三日 = 三日



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

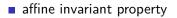
On anticrookedness

On APN permutations

Sketch of proof

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

affine invariant property



• sufficient condition:  $\hat{n} = 0$ 



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

- affine invariant property
- sufficient condition:  $\hat{n} = 0$

$$\hat{n} = \max_{a \neq 0} |\{\lambda \neq 0 : \deg(D_a F \cdot \lambda) = 0\}|$$



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

## Our results on 4-bit permutations

 $F: \mathbb{F}^4 \to \mathbb{F}^4$ , permutation



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

# Our results on 4-bit permutations



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

 $F: \mathbb{F}^4 \to \mathbb{F}^4$ , permutation

#### $\hat{n} > 3 \longrightarrow \text{not AC}$

# Our results on 4-bit permutations



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

$${\sf F}:\mathbb{F}^4 o\mathbb{F}^4$$
, permutation

$$\hat{n} > 3 \longrightarrow \text{not AC}$$
general:  $\hat{n} > 2^{n-2} - 1$ 

# Our results on 4-bit permutations



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

$$F: \mathbb{F}^4 \to \mathbb{F}^4$$
, permutation

$$\hat{n} > 3 \longrightarrow \text{not AC}$$
general:  $\hat{n} > 2^{n-2} - 1$ 

$$\delta > 8 \longrightarrow \text{not AC}$$



Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

$$F: \mathbb{F}^4 \to \mathbb{F}^4$$
, permutation

$$\hat{n} > 3 \longrightarrow \text{not AC}$$
general:  $\hat{n} > 2^{n-2} - 1$ 

 $\bullet \ \delta > 8 \ \longrightarrow \text{not AC}$ 

• AC and 
$$\hat{n} = 3 \longrightarrow \delta = 8$$



Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

$$\overline{F}: \mathbb{F}^4 \to \mathbb{F}^4$$
, permutation

• 
$$\hat{n} > 3 \longrightarrow \text{not AC}$$
  
general:  $\hat{n} > 2^{n-2} - 1$   
•  $\delta > 8 \longrightarrow \text{not AC}$ 

• AC and 
$$\hat{n} = 3 \longrightarrow \delta = 8$$

 $\blacksquare \ \textit{n}_1 > 1 \ \longrightarrow \ \textit{not} \ \mathsf{AC}$ 



Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

・ロト・日本・モン・モン・モー うへぐ

$$F: \mathbb{F}^4 \to \mathbb{F}^4$$
, permutation

$$\hat{n} > 3 \longrightarrow \text{not AC} \\
 general: \quad \hat{n} > 2^{n-2} - 1$$
 $\delta > 8 \longrightarrow \text{not AC}$ 
 $AC \text{ and } \hat{n} = 3 \longrightarrow \delta = 8$ 
 $n_1 > 1 \longrightarrow \text{not AC}$ 
 $n_i = |\{\lambda : \deg(F \cdot \lambda) = i\}$ 

# Almost Perfect Nonlinear (APN)



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean

On anticrookedness

On APN permutations

Sketch of proof

# Almost Perfect Nonlinear (APN)



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean

On anticrookedness

On APN permutations

Sketch of proof

◆□▶ ◆□▶ ◆三▶ ◆三▶ ○ ● ●

## $\forall a, b \in \mathbb{F}^n, a \neq 0, |\{x \in \mathbb{F}^n : D_a F(x) = b\}| \le 2$

# Almost Perfect Nonlinear (APN)

$$\forall a, b \in \mathbb{F}^n, a \neq 0, |\{x \in \mathbb{F}^n : D_a F(x) = b\}| \leq 2$$

#### Proposition

Let  $F : \mathbb{F}^n \to \mathbb{F}^n$  be an APN permutation. Then F is AC iif  $\hat{n} = 0.$ 



even dimension

On APN permutations

◆□▶ ◆□▶ ◆三▶ ◆三▶ ○ ● ●



Irene Villa

Introduction Vectorial Boolean

On anticrookedness

On APN permutations

Sketch of proof

◆□▶ ◆□▶ ◆ □▶ ◆ □ ● ● ● ●

## ODD CASE



Irene Villa

Introduction Vectorial Boolean

On anticrookedness

On APN permutations

Sketch of proof

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

#### ODD CASE

There exist many family of APN permutation such as:

$$F(x) = x^{2^n - 2}$$



Irene Villa

Introduction Vectorial Boolean

On anticrookedness

On APN permutations

Sketch of proof

## EVEN CASE

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

There exist many family of APN permutation such as:

ODD CASE

$$F(x) = x^{2^n - 2}$$



Irene Villa

Introduction Vectorial Boolean

On anticrookedness

On APN permutations

Sketch of proof

#### ODD CASE

There exist many family of APN permutation such as:

EVEN CASE

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

n = 4

$$F(x) = x^{2^n - 2}$$



There exist many family of APN permutation such as:

## EVEN CASE

$$n = 4$$

no APN permutations (computational proof by X. Hou in 2006)

◆□ → ◆□ → ◆ □ → ◆ □ → □ □ □

Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Eunctions

On anticrookedness

On APN permutations

$$F(x) = x^{2^n - 2}$$



There exist many family of APN permutation such as:

 $\frac{\text{EVEN CASE}}{n = 4}$  no APN permutations (computational proof by X. Hou in 2006)

◆□▶ ◆□▶ ◆三▶ ◆三▶ ○ ● ●

Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Eunctions

On anticrookedness

On APN permutations

Sketch of proof

$$F(x) = x^{2^n - 2}$$

*n* = 6



There exist many family of APN permutation such as:

#### EVEN CASE

*n* = 4

no APN permutations (computational proof by X. Hou in 2006)

n = 6 (J. F. Dillon in 2010)

Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

$$F(x) = x^{2^n - 2}$$



There exist many family of APN permutation such as:

## EVEN CASE

n = 4 no Al

no APN permutations (computational proof by X. Hou in 2006)

n = 6 (J. F. Dillon in 2010)

$$n_3 = 7, n_4 = 56, \hat{n} = 1$$

Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

$$F(x) = x^{2^n - 2}$$



There exist many family of APN permutation such as:

 $F(x) = x^{2^n - 2}$ 

<u>n = 4</u> no APN permutations (computational proof by X. Hou in 2006)

$$n = 6$$
 (J. F. Dillon in 2010)

$$n_3 = 7, n_4 = 56, \hat{n} = 1$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

$$n \ge 8$$



There exist many family of APN permutation such as:

 $F(x) = x^{2^n - 2}$ 

EVEN CASE
$$n = 4$$
no APN permutations  
(computational proof by  
X. Hou in 2006) $n = 6$ (J. F. Dillon in 2010) $n_3 = 7, n_4 = 56, \hat{n} = 1$ 

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

*n* ≥ 8

Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

## Even case



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean

On anticrookedness

On APN permutations

Sketch of proof

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 - つへぐ





Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

#### Proposition

#### Let *F* be an APN permutation with *n* even. Then $n_2 = 0$ .





Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

#### Proposition

Let *F* be an APN permutation with *n* even. Then  $n_2 = 0$ .

#### Proposition

No partially-bent components.





Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

#### Proposition

Let *F* be an APN permutation with *n* even. Then  $n_2 = 0$ .

#### Proposition

No partially-bent components.

Extend the results of J. Seberry, X.-M. Zhang, and Y. Zheng (1994) and K. Nyberg (1995).



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Eunctions

On anticrookedness

On APN permutations

Sketch of proof

#### Definition

For 
$$g: \mathbb{F}^n \to \mathbb{F}$$
, let  $\mathcal{F}(g) = \sum_{x} (-1)^{g(x)}$ .



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

・ロト・日本・モン・モン・モー うへぐ

#### Definition

For 
$$g: \mathbb{F}^n \to \mathbb{F}$$
, let  $\mathcal{F}(g) = \sum_{x} (-1)^{g(x)}$ .

 $F: \mathbb{F}^4 \to \mathbb{F}^4$  APN permutation



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Eurctions

On anticrookedness

On APN permutations

Sketch of proof

#### Definition

For 
$$g: \mathbb{F}^n \to \mathbb{F}$$
, let  $\mathcal{F}(g) = \sum_{x} (-1)^{g(x)}$ .

$$F: \mathbb{F}^4 \to \mathbb{F}^4$$
 APN permutation

$$n_1 = n_2 = 0$$



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Eunctions

On anticrookedness

On APN permutations

Sketch of proof

#### Definition

For 
$$g: \mathbb{F}^n \to \mathbb{F}$$
, let  $\mathcal{F}(g) = \sum_{x} (-1)^{g(x)}$ .

$$F: \mathbb{F}^4 \to \mathbb{F}^4$$
 APN permutation

$$n_1 = n_2 = 0$$

$$\forall \lambda \neq 0 \ \deg(f_{\lambda}) = 3$$



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

・ロト・日本・モン・モン・モー うへぐ

#### Definition

For 
$$g: \mathbb{F}^n \to \mathbb{F}$$
, let  $\mathcal{F}(g) = \sum_{x} (-1)^{g(x)}$ .

$$F: \mathbb{F}^4 \to \mathbb{F}^4$$
 APN permutation

$$n_1 = n_2 = 0$$

$$\forall \lambda \neq 0 \ \deg(f_{\lambda}) = 3$$

 $\exists \lambda \text{ s.t. } |\{a: \mathcal{F}(D_a f_{\lambda}) = 0\}| \geq 11$ 



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Eunctions

On anticrookedness

On APN permutations

Sketch of proof

#### Definition

For 
$$g: \mathbb{F}^n \to \mathbb{F}$$
, let  $\mathcal{F}(g) = \sum_{x} (-1)^{g(x)}$ .

$$F: \mathbb{F}^4 \to \mathbb{F}^4$$
 APN permutation

$$n_1 = n_2 = 0$$

$$\forall \lambda \neq 0 \ \deg(f_{\lambda}) = 3$$

$$\exists \ \lambda \text{ s.t. } |\{a: \mathcal{F}(D_a f_{\lambda}) = 0\}| \geq 11$$



Vectorial Boolean Functions in even dimension

Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

#### Proposition

Let *F* be a cubic APN permutation with *n* even. Then  $\exists \lambda$  s.t.  $|\{a : \mathcal{F}(D_a f_{\lambda}) = 0\}| \ge 2^n - 2^{n-2} - 1.$ 



Irene Villa

Introduction Vectorial Boolean Eunctions

On anticrookedness

On APN permutations

Sketch of proof

・ロト・日本・モン・モン・モー うへぐ

#### Proposition

Given  $f: \mathbb{F}^4 \to \mathbb{F}$  balanced and deg(f) = 3, then

 $|\{a:\mathcal{F}(D_af)=0\}|<11$ 



Irene Villa

Introduction Vectorial Boolean Functions

On anticrookedness

On APN permutations

Sketch of proof

・ロト・日本・モン・モン・モー うへぐ

#### Proposition

# Given $f:\mathbb{F}^4 o\mathbb{F}$ balanced and deg(f)= 3, then $|\{a:\mathcal{F}(D_af)=0\}|<11$

#### Theorem

No 4-bit permutation can be APN.



Irene Villa

Introduction Vectorial Boolean Eunctions

On anticrookedness

On APN permutations

Sketch of proof

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

#### Thank you for your attention