# Vectorial Boolean Functions in even dimension

Irene Villa

Università degli Studi di Trento

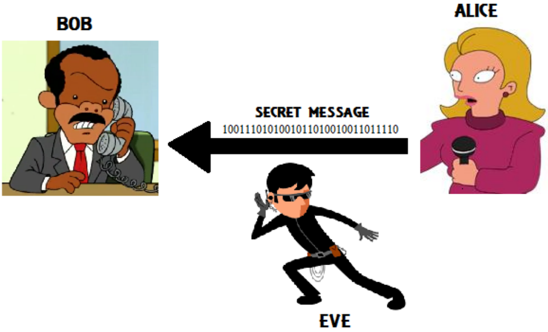

ALICE

BOB

ALICE

Communicate a secret message

Communicate a secret message



Cipher:

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

Cipher:

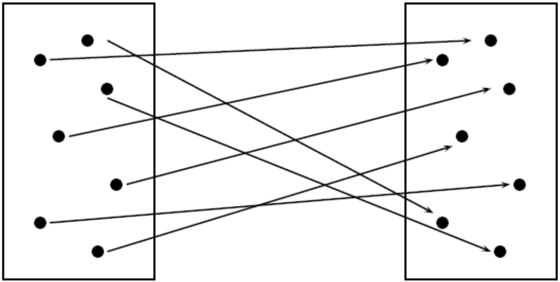
- $\mathcal{M} = \mathbb{F}^n$ set of messages over an alphabet $\mathbb{F}$
- $\varphi_k : \mathcal{M} \to \mathcal{M}$ encryption function, $k \in \mathcal{K}$ key-space

$\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$

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

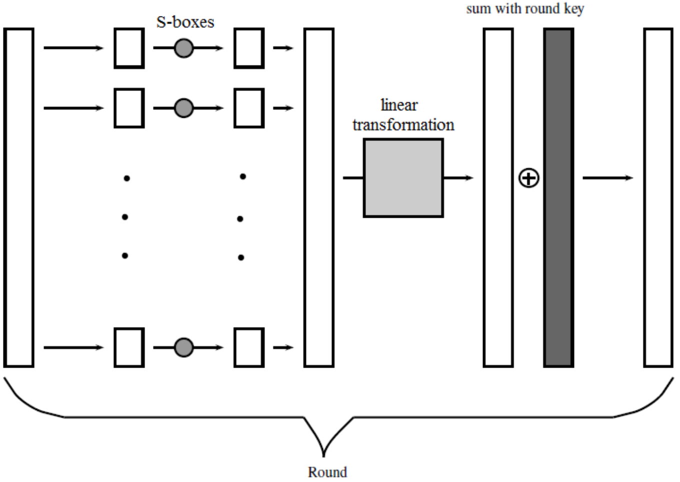
$\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$



# Block ciphers

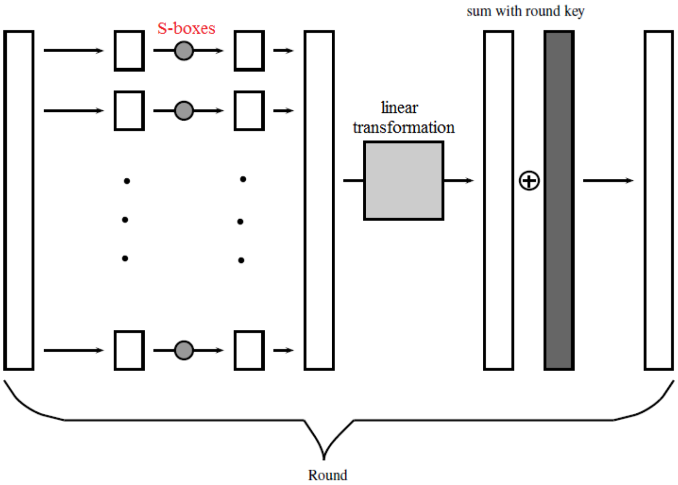


Example of translation based cipher



# Block ciphers

Example of translation based cipher



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

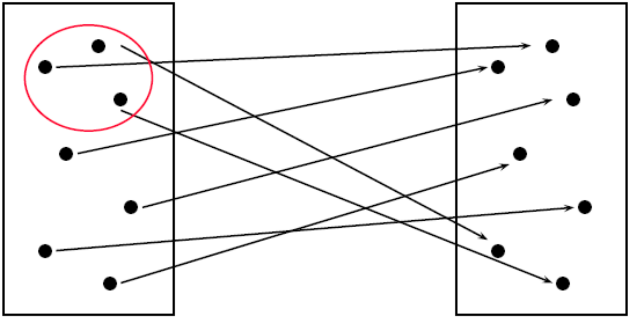
$$\{P, \varphi_k(P)\}_{P \in X}$$

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

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 function

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

# Vectorial Boolean function

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

coordinate function

# Vectorial Boolean function

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

coordinate function

$$F(x) = (f_1(x), \ldots, f_m(x))$$

# Vectorial Boolean function

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

coordinate function

$$F(x) = (f_1(x), \ldots, f_m(x))$$

component function

# Vectorial Boolean function

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

coordinate function

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

component function

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

# Vectorial Boolean function

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

coordinate function

$$F(x) = (f_1(x), \ldots, f_m(x))$$

component function

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

degree

# Vectorial Boolean function

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

coordinate function

$$F(x) = (f_1(x), \ldots, f_m(x))$$

component function

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

degree

$$\deg(F) = \max_\lambda \deg(f_\lambda)$$

# Vectorial Boolean function

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

coordinate function

$$F(x) = (f_1(x), \ldots, f_m(x))$$

component function

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

degree

$$\deg(F) = \max_\lambda \deg(f_\lambda)$$

permutation

# Vectorial Boolean function

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

coordinate function

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

component function

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

degree

$$\deg(F) = \max_\lambda \deg(f_\lambda)$$

permutation $\qquad \deg(F) \leq n - 1$

# Some definitions of “non-linearity”

Derivative

# Some definitions of “non-linearity”

## Derivative

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

$$\boxed{D_aF(x) = F(x) + F(x+a)}$$

# Some definitions of "non-linearity"

Derivative

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

Uniform differentiability

# Some definitions of "non-linearity"

Derivative

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

Uniform differentiability

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

# Some definitions of "non-linearity"

Derivative

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

Uniform differentiability

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

Weakly uniform differentiability

# Some definitions of “non-linearity”



Derivative

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

Uniform differentiability

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

Weakly uniform differentiability

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

# Some definitions of "non-linearity"

Derivative

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

Uniform differentiability

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

Weakly uniform differentiability

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

Anti-crookedness (AC)

# Some definitions of “non-linearity”



Derivative

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

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)

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

# On anti-crookedness

# On anti-crookedness

- affine invariant property

# On anti-crookedness

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

# On anti-crookedness

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

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

# Our results on 4-bit permutations

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

# Our results on 4-bit permutations

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

- $\hat{n} > 3 \longrightarrow$ not AC

# Our results on 4-bit permutations

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

- $\hat{n} > 3 \longrightarrow$ not AC

  general: $\boxed{\hat{n} > 2^{n-2} - 1}$

# Our results on 4-bit permutations

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

- $\hat{n} > 3 \longrightarrow$ not AC

  general: $\boxed{\hat{n} > 2^{n-2} - 1}$

- $\delta > 8 \longrightarrow$ not AC

# Our results on 4-bit permutations

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

- $\hat{n} > 3 \longrightarrow$ not AC

  general: $\boxed{\hat{n} > 2^{n-2} - 1}$
- $\delta > 8 \longrightarrow$ not AC
- AC and $\hat{n} = 3 \longrightarrow \delta = 8$

# Our results on 4-bit permutations

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

- $\hat{n} > 3 \longrightarrow$ not AC

  general: $\boxed{\hat{n} > 2^{n-2} - 1}$
- $\delta > 8 \longrightarrow$ not AC
- AC and $\hat{n} = 3 \longrightarrow \delta = 8$
- $n_1 > 1 \longrightarrow$ not AC

# Our results on 4-bit permutations

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

- $\hat{n} > 3 \longrightarrow$ not AC

  general: $\boxed{\hat{n} > 2^{n-2} - 1}$
- $\delta > 8 \longrightarrow$ not AC
- AC and $\hat{n} = 3 \longrightarrow \delta = 8$
- $n_1 > 1 \longrightarrow$ not AC

$$n_i = |\{\lambda : \deg(F \cdot \lambda) = i\}|$$

# Almost Perfect Nonlinear (APN)

# Almost Perfect Nonlinear (APN)

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

# Almost Perfect Nonlinear (APN)

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

## Proposition

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

ODD CASE

ODD CASE

There exist many family of APN permutation such as:

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

ODD CASE

There exist many family of APN permutation such as:

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

EVEN CASE

ODD CASE

There exist many family of APN permutation such as:

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

EVEN CASE

$\boxed{n = 4}$

ODD CASE

There exist many family of APN permutation such as:

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

EVEN CASE

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

ODD CASE

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)

$n = 6$

ODD CASE

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)

ODD CASE

There exist many family of APN permutation such as:

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

EVEN CASE

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

$\boxed{n = 6}$ (J. F. Dillon in 2010)

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

ODD CASE

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)

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

$n \geq 8$

ODD CASE

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)

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

$n \geq 8$

# Even case

# Even case

**Proposition**

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

# Even case

**Proposition**

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

**Proposition**

No partially-bent components.

# Even case

**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).

# Formal proof for the case $n = 4$

# Formal proof for the case $n = 4$

**Definition**

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

# Formal proof for the case $n = 4$

**Definition**

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

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

# Formal proof for the case $n = 4$

**Definition**

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

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

$$n_1 = n_2 = 0$$

# Formal proof for the case $n = 4$

**Definition**

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

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

$$n_1 = n_2 = 0$$

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

# Formal proof for the case $n = 4$

**Definition**

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

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

$$n_1 = n_2 = 0$$

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

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

# Formal proof for the case $n = 4$

## Definition

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

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

$$n_1 = n_2 = 0$$

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

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

## Proposition

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

## Proposition

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

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

**Proposition**

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

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

**Theorem**

No 4-bit permutation can be APN.

Thank you for your attention