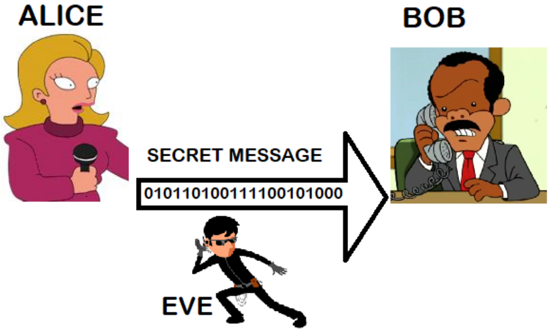
# Optimal Boolean Functions

Irene Villa

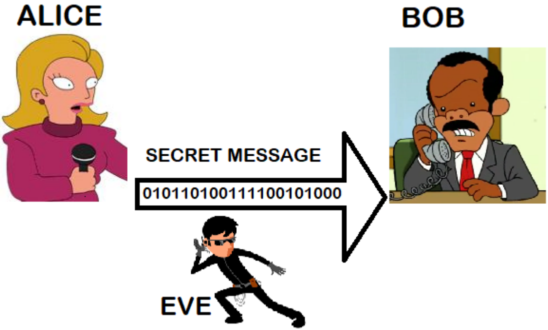
UiB - Universitetet i Bergen
Selmer center

Finse 2018

Communicate a secret message



Communicate a secret message



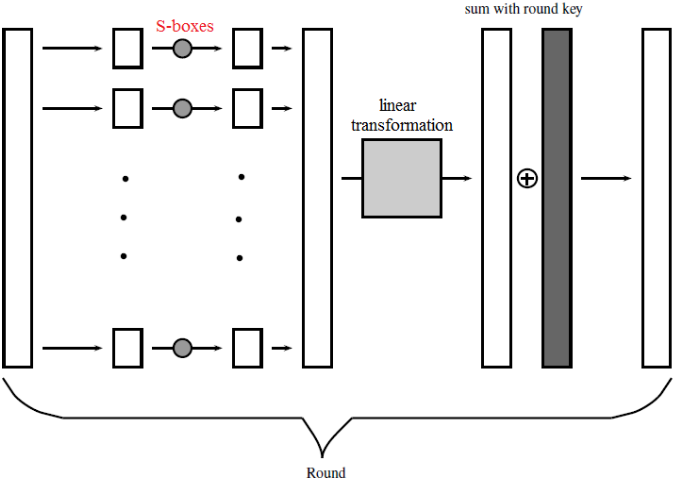

Cipher: $\mathcal{M}$ set of possible messages

$k \in \mathcal{K}$ key-space

$\varphi_k : \mathcal{M} \to \mathcal{M}$ encryption function

# Block ciphers

Example of translation based cipher



## Vectorial Boolean Function

Given $n, m$ integers, an *(n, m)-function* is a function that transform a sequence of $n$ bits into a sequence of $m$ bits,

## Vectorial Boolean Function

Given $n, m$ integers, an *$(n, m)$-function* is a function that transform a sequence of $n$ bits into a sequence of $m$ bits,

$$\boxed{F : \mathbb{F}_2^n \to \mathbb{F}_2^m} \text{ with } \mathbb{F}_2 = \{0, 1\}$$

$$F(x_1, \ldots, x_n) = \begin{pmatrix} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_m(x_1, \ldots, x_n) \end{pmatrix}, \ f_i : \mathbb{F}_2^n \to \mathbb{F}_2$$

## Vectorial Boolean Function

Given $n, m$ integers, an *(n, m)-function* is a function that transform a sequence of $n$ bits into a sequence of $m$ bits,

$$\boxed{F : \mathbb{F}_2^n \to \mathbb{F}_2^m} \text{ with } \mathbb{F}_2 = \{0, 1\}$$

$$F(x_1, \ldots, x_n) = \begin{pmatrix} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_m(x_1, \ldots, x_n) \end{pmatrix}, \; f_i : \mathbb{F}_2^n \to \mathbb{F}_2$$

If $n = m$ an equivalent representation (univariate polynomial)

$$\boxed{F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}} \qquad F(x) = \sum_{i=0}^{2^n-1} c_i x^i, \; c_i \in \mathbb{F}_{2^n}.$$

Symmetric ciphers are designed by appropriate composition of nonlinear Boolean functions
$\rightarrow$ in **block ciphers** the security depends on S-boxes

Symmetric ciphers are designed by appropriate composition of nonlinear Boolean functions

$\rightarrow$ in **block ciphers** the security depends on S-boxes

Most cryptographic attacks

$\Downarrow$

mathematical properties that measure the resistance of the S-box

Symmetric ciphers are designed by appropriate composition of nonlinear Boolean functions
$\rightarrow$ in **block ciphers** the security depends on S-boxes

Most cryptographic attacks
$$\Downarrow$$
mathematical properties that measure the resistance of the S-box

- differential attack
- linear cryptanalysis

- DIFFERENTIAL ATTACK

- DIFFERENTIAL ATTACK
  how differences in an input can affect the resulting difference at the output.

$$\begin{array}{ccccc} x & \rightarrow & \left[\begin{array}{c} \\ F \\ \\ \end{array}\right] & \rightarrow & y \\ x+a & \rightarrow & & \rightarrow & y+b \end{array}$$

- DIFFERENTIAL ATTACK $\Rightarrow$ differential $\delta$-uniformity
  how differences in an input can affect the resulting difference at the output.

$$\begin{array}{ccccc} x & \rightarrow & \left[\begin{array}{c} \\ F \\ \\ \end{array}\right. & \rightarrow & y \\ x+a & \rightarrow & \left.\right] & \rightarrow & y+b \end{array}$$

$$\delta = \max_{a,b\in\mathbb{F}_2^n a\neq\mathbf{0}} |\{x \in \mathbb{F}_2^n : F(a+x) - F(x) = b\}|$$

- DIFFERENTIAL ATTACK $\Rightarrow$ differential $\delta$-uniformity
  how differences in an input can affect the resulting difference at the output.

$$\begin{array}{ccccc} x & \rightarrow & \left[ \begin{array}{c} \\ F \\ \\ \end{array} \right] & \rightarrow & y \\ x+a & \rightarrow & & \rightarrow & y+b \end{array}$$

$$\delta = \max_{a,b \in \mathbb{F}_2^n a \neq \mathbf{0}} |\{x \in \mathbb{F}_2^n : F(a+x) - F(x) = b\}|$$

  - best resistance when $\delta = 2^{n-m}$: PERFECT NONLINEAR (PN) $n$ even and $m \leq \frac{n}{2}$
  - if $n = m$ smallest $\delta = 2$: ALMOST PERFECT NONLINEAR (APN)

- LINEAR CRYPTANALYSIS

- LINEAR CRYPTANALYSIS
  finding affine approximations to the action of a cipher

$$g : \mathbb{F}_2^n \to \mathbb{F}_2 \text{ is affine if degree is at most 1 } (g \in \mathcal{A})$$

$$d_H(f,g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}| \text{ (Hamming distance)}$$

- LINEAR CRYPTANALYSIS $\Rightarrow$ nonlinearity NL
  finding affine approximations to the action of a cipher

$$g : \mathbb{F}_2^n \to \mathbb{F}_2 \text{ is affine if degree is at most 1 } (g \in \mathcal{A})$$

$$d_H(f,g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}| \text{ (Hamming distance)}$$

$$NL(F) = \min_{g \in \mathcal{A}, \lambda \in \mathbb{F}_2^{m*}} d_H(\lambda \cdot F, g) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$$

- LINEAR CRYPTANALYSIS $\Rightarrow$ nonlinearity NL
  finding affine approximations to the action of a cipher

$$g : \mathbb{F}_2^n \to \mathbb{F}_2 \text{ is affine if degree is at most 1 } (g \in \mathcal{A})$$

$$d_H(f,g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}| \text{ (Hamming distance)}$$

$$NL(F) = \min_{g \in \mathcal{A}, \lambda \in \mathbb{F}_2^{m*}} d_H(\lambda \cdot F, g) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$$

  - best resistance when NL is maximum: BENT
    $n$ even and $m \leq \frac{n}{2}$
  - if $n = m$: $NL(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$ ALMOST BENT (AB)

# CCZ-equivalence relation

Most general equivalence relation known that preserves $\delta$ and NL

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

$F_1$ and $F_2$ are CCZ-equivalent if $\mathcal{L}(\Gamma_{F_1}) = \Gamma_{F_2}$, for an affine permutation $\mathcal{L}$.

# OPTIMAL BOOLEAN FUNCTIONS

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

or equivalently

$$\boxed{F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}} \; F(x) = \sum_{i=0}^{2^n-1} c_i x^i.$$

we are interested in APN and AB functions

# OPTIMAL BOOLEAN FUNCTIONS

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

or equivalently

$$\boxed{F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}} \; F(x) = \sum_{i=0}^{2^n-1} c_i x^i.$$

we are interested in APN and AB functions

Other applications of APN and AB functions:

- coding theory
- sequence design
- combinatorial analysis

# On APN and AB functions $\boxed{F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}}$

- classification of APN, AB f. is an hard open problem
- complete classification known only for $n \leq 5$
- few infinite classes of APN and AB functions known
  - 6 infinite families of power APN f. (4 are also AB)
    (for example $x^{2^i+1}$ with $\gcd(i, n)=1$)
  - 11 infinite families of quadratic APN f. (4 are also AB)
- even for small $n$ there are too many vectorial Boolean functions to just use a purely computer search
- just one APN permutation is known in even dimension

We have to come up with new methods to construct new optimal functions and to analyse them

- combination of theoretic results and computational insights to find new families
- studying equivalence relations between already known functions
- finding new invariant of the CCZ-equivalence to easily prove CCZ-inequivalent functions
- finding more general equivalence relations that preserve optimal properties

# Example

- many known APN functions in small dimensions are of the form $F(x) = L_1(x^3) + L_2(x^9)$, with $L_1, L_2$ linear functions:
  - $x^3$ and $x^3 + Tr(x^9)$ are infinite families of APN functions
  - for $n = 8$ out of 23 APN functions (2008) 17 are of this form

# Example

- many known APN functions in small dimensions are of the form $F(x) = L_1(x^3) + L_2(x^9)$, with $L_1, L_2$ linear functions:
  • $x^3$ and $x^3 + Tr(x^9)$ are infinite families of APN functions
  • for $n = 8$ out of 23 APN functions (2008) 17 are of this form
- theoretical properties and restrictions on $L_1$ and $L_2$ for such function to be APN in $\mathbb{F}_{2^n}$:
  • if $F(x)$ is APN for an even $n$ then $F(a) \neq 0$ for any $a \neq 0$;
  • if $F(x)$ is APN for $n = 6m$ then $L_1(a^3\beta) \neq 0$ for any $a \neq 0$ and $\beta \in \mathbb{F}_{2^3}^*$ with $\mathrm{Tr}_3(\beta) = \beta^{2^2} + \beta^2 + \beta = 0$;

# Example

- many known APN functions in small dimensions are of the form $F(x) = L_1(x^3) + L_2(x^9)$, with $L_1, L_2$ linear functions:
  • $x^3$ and $x^3 + Tr(x^9)$ are infinite families of APN functions
  • for $n = 8$ out of 23 APN functions (2008) 17 are of this form
- theoretical properties and restrictions on $L_1$ and $L_2$ for such function to be APN in $\mathbb{F}_{2^n}$:
  • if $F(x)$ is APN for an even $n$ then $F(a) \neq 0$ for any $a \neq 0$;
  • if $F(x)$ is APN for $n = 6m$ then $L_1(a^3\beta) \neq 0$ for any $a \neq 0$ and $\beta \in \mathbb{F}_{2^3}^*$ with $\mathrm{Tr}_3(\beta) = \beta^{2^2} + \beta^2 + \beta = 0$;
- with some restrictions it is possible to perform a lighter computational search in bigger dimensions

# Example

- many known APN functions in small dimensions are of the form $F(x) = L_1(x^3) + L_2(x^9)$, with $L_1, L_2$ linear functions:
  • $x^3$ and $x^3 + Tr(x^9)$ are infinite families of APN functions
  • for $n = 8$ out of 23 APN functions (2008) 17 are of this form
- theoretical properties and restrictions on $L_1$ and $L_2$ for such function to be APN in $\mathbb{F}_{2^n}$:
  • if $F(x)$ is APN for an even $n$ then $F(a) \neq 0$ for any $a \neq 0$;
  • if $F(x)$ is APN for $n = 6m$ then $L_1(a^3\beta) \neq 0$ for any $a \neq 0$ and $\beta \in \mathbb{F}^*_{2^3}$ with $\mathrm{Tr}_3(\beta) = \beta^{2^2} + \beta^2 + \beta = 0$;
- with some restrictions it is possible to perform a lighter computational search in bigger dimensions
  • $n = 8$ $x^9 + L(x^3)$ w. $L(x) = \alpha x^4 + \alpha^{-1}x^2 + \alpha^{-2}x$ is APN
  • $n = 10$ $x^9 + L(x^3)$ w. $L(x) = \alpha x^4 + \alpha^{-1}x^2 + \alpha^{-2}x$ is APN

# Example

- many known APN functions in small dimensions are of the form $F(x) = L_1(x^3) + L_2(x^9)$, with $L_1, L_2$ linear functions:
  - $x^3$ and $x^3 + Tr(x^9)$ are infinite families of APN functions
  - for $n = 8$ out of 23 APN functions (2008) 17 are of this form
- theoretical properties and restrictions on $L_1$ and $L_2$ for such function to be APN in $\mathbb{F}_{2^n}$:
  - if $F(x)$ is APN for an even $n$ then $F(a) \neq 0$ for any $a \neq 0$;
  - if $F(x)$ is APN for $n = 6m$ then $L_1(a^3\beta) \neq 0$ for any $a \neq 0$ and $\beta \in \mathbb{F}_{2^3}^*$ with $\mathrm{Tr}_3(\beta) = \beta^{2^2} + \beta^2 + \beta = 0$;
- with some restrictions it is possible to perform a lighter computational search in bigger dimensions
  - $n = 8$ $x^9 + L(x^3)$ w. $L(x) = \alpha x^4 + \alpha^{-1}x^2 + \alpha^{-2}x$ is APN
  - $n = 10$ $x^9 + L(x^3)$ w. $L(x) = \alpha x^4 + \alpha^{-1}x^2 + \alpha^{-2}x$ is APN
- when $n$ is even the function $x^9 + L(x^3)$ is APN in $\mathbb{F}_{2^n}$ with $L(x) = \gamma x^4 + \gamma^{-1}x^2 + \gamma^{-2}x$ for any $\gamma$ that is not a cube

# Example

- many known APN functions in small dimensions are of the form $F(x) = L_1(x^3) + L_2(x^9)$, with $L_1, L_2$ linear functions:
  • $x^3$ and $x^3 + Tr(x^9)$ are infinite families of APN functions
  • for $n = 8$ out of 23 APN functions (2008) 17 are of this form
- theoretical properties and restrictions on $L_1$ and $L_2$ for such function to be APN in $\mathbb{F}_{2^n}$:
  • if $F(x)$ is APN for an even $n$ then $F(a) \neq 0$ for any $a \neq 0$;
  • if $F(x)$ is APN for $n = 6m$ then $L_1(a^3\beta) \neq 0$ for any $a \neq 0$ and $\beta \in \mathbb{F}_{2^3}^*$ with $\mathrm{Tr}_3(\beta) = \beta^{2^2} + \beta^2 + \beta = 0$;
- with some restrictions it is possible to perform a lighter computational search in bigger dimensions
  • $n = 8$ $x^9 + L(x^3)$ w. $L(x) = \alpha x^4 + \alpha^{-1}x^2 + \alpha^{-2}x$ is APN
  • $n = 10$ $x^9 + L(x^3)$ w. $L(x) = \alpha x^4 + \alpha^{-1}x^2 + \alpha^{-2}x$ is APN
- when $n$ is even the function $x^9 + L(x^3)$ is APN in $\mathbb{F}_{2^n}$ with $L(x) = \gamma x^4 + \gamma^{-1}x^2 + \gamma^{-2}x$ for any $\gamma$ that is not a cube
- CCZ-equivalent to an already known APN function $x^3$

# On APN Permutations

In many situations we want the cipher to be invertible

PERMUTATION S-Box

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

# On APN Permutations

In many situations we want the cipher to be invertible

PERMUTATION S-Box

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

- $n$ odd: known APN permutations in every dimension ($x^{2^n-2} = x^{-1}$)

# On APN Permutations

In many situations we want the cipher to be invertible

PERMUTATION S-Box

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

- $n$ odd: known APN permutations in every dimension $(x^{2^n-2} = x^{-1})$
- $n$ even:
  - $n = 4$ no APN permutation (first computational proof and then theoretic one)
  - $n = 6$ found 1 APN permutation in 2010 by Dillon et al. (NSA) : applied CCZ-equivalence to an already known quadratic APN function
  - $n \geq 8$ ?

# On APN Permutations

In many situations we want the cipher to be invertible

PERMUTATION S-Box

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

- $n$ odd: known APN permutations in every dimension ($x^{2^n-2} = x^{-1}$)
- $n$ even:
  - $n = 4$ no APN permutation (first computational proof and then theoretic one)
  - $n = 6$ found 1 APN permutation in 2010 by Dillon et al. (NSA) : applied CCZ-equivalence to an already known quadratic APN function
  - $n \geq 8$ ?

Dream goal:

- find other APN permutations in even dimension
- find a family of APN permutations in even dimension

# Takk