HIGHER ORDER DERIVATIVES

OR CUBE, OR ALGEBRAIC, OR INTEGRAL

Yann Rotella

Université de Versailles Saint Quentin en Yvelines

kodeketa eta kriptografiaren egunak
Hendaye, le 14 avril 2022

LMV
Laboratoire de mathématiques
de Versailles - CNRS UMR 8100

UVSQ
université PARIS-SACLAY

cnrs

Outline

The Algebraic Normal Form

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ Then f can be uniquely represented as an element of

$$\mathbb{F}_2[x_0, \ldots, x_{n-1}]/(x_0^2 - x_0, \ldots, x_{n-1}^2 - x_{n-1})$$

That is a sum of monomials, i.e. for some $u \in \mathbb{F}_2^n$

$$x^u = \prod_{i=0}^{n-1} x_i^{u_i}$$

Example : $x_0 x_2 x_3 = x^{10110000}$

The Algebraic Normal Form

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ Then f can be uniquely represented as an element of

$$\mathbb{F}_2[x_0, \ldots, x_{n-1}]/(x_0^2 - x_0, \ldots, x_{n-1}^2 - x_{n-1})$$

That is a sum of monomials, i.e. for some $u \in \mathbb{F}_2^n$

$$x^u = \prod_{i=0}^{n-1} x_i^{u_i}$$

Example : $x_0 x_2 x_3 = x^{10110000}$

$$f(x_0, \ldots, x_{n-1}) = \bigoplus_{u \in \mathbb{F}_2^n} c_u x^u$$

with $c_u \in \mathbb{F}_2$.

Truth table and Monomials

$$f(x_0,\ldots,x_{n-1}) = \bigoplus_{u\in\mathbb{F}_2^n} c_u x^u$$

$$f(a) = \bigoplus_{u\prec a} c_u \text{ and } c_u = \bigoplus_{a\prec u} f(a)$$

Where $a \prec u$ iff $\mathrm{supp}(a) \subset \mathrm{supp}(u)$

Truth table and Monomials

$$f(x_0,\ldots,x_{n-1}) = \bigoplus_{u\in\mathbb{F}_2^n} c_u x^u$$

$$f(a) = \bigoplus_{u\prec a} c_u \text{ and } c_u = \bigoplus_{a\prec u} f(a)$$

Where $a \prec u$ iff $\mathrm{supp}(a) \subset \mathrm{supp}(u)$ Also

$$\mathrm{wt}(u) = \#\mathrm{supp}(u)$$

FUNCTIONS

A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is represented as a collection of m boolean functions, called component functions.

- For permutations, the monomial $x_0 x_1 \cdots x_{n-1}$ never appears
- A random function has its monomials appearing each with probability $1/2$ in each component function.

REPRESENTATION

DEGREE

DIVISION PROPERTY

ATTACK STRATEGIES

RANDOM DIRECTIONS

Higher-order differential attacks [Lai 94]

$$f(x_0, \ldots, x_{n-1}) = \bigoplus_{u \in \mathbb{F}_2^n} c_u x^u$$

Definition (Multivariate degree)

$$d = \deg(f) = \max\{\mathrm{wt}(u), c_u = 1\}$$

Higher-order differential attacks [Lai 94]

$$f(x_0, \ldots, x_{n-1}) = \bigoplus_{u \in \mathbb{F}_2^n} c_u x^u$$

Definition (Multivariate degree)

$$d = \deg(f) = \max\{\mathrm{wt}(u), c_u = 1\}$$

Distinguisher :

For all linear space V, with $\dim(V) \geq d + 1$,

$$g : x \mapsto \sum_{v \in V} f(x + v)$$

is constant to zero.

Degree evaluation

At different level :

- For any F and G, $\deg(F \circ G) \leq \deg(F) \times \deg(G)$

Degree evaluation

At different level :

- For any F and G, $\deg(F \circ G) \leq \deg(F) \times \deg(G)$
- A better bound by A. Canteau and C. Boura [2011, FSE]

Degree evaluation

At different level :

- For any F and G, $\deg(F \circ G) \leq \deg(F) \times \deg(G)$
- A better bound by A. Canteau and C. Boura [2011, FSE]
- Better upper bound when the structure is specific [CGGLRS, 2020]

Going further

What is missing ?

Going further

What is missing?

A component of $E_k(x)$ can be represented as

$$\sum_{u \in \mathbb{F}_2^n} c_u(k) x^u$$

and assume that for any $v \succ u$, $c_v(k) = 0$.

Then what is the possible degree of $E_k(x)$ in x?

Going further

What is missing?
A component of $E_k(x)$ can be represented as

$$\sum_{u \in \mathbb{F}_2^n} c_u(k) x^u$$

and assume that for any $v \succ u$, $c_v(k) = 0$.
Then what is the possible degree of $E_k(x)$ in x?

$$f(x) = x_0 x_1 x_2 x_3 x_4 x_6 + x_3 + x_4 x_5 + x_6$$

Going further

What is missing?
A component of $E_k(x)$ can be represented as

$$\sum_{u \in \mathbb{F}_2^n} c_u(k) x^u$$

and assume that for any $v \succ u$, $c_v(k) = 0$.
Then what is the possible degree of $E_k(x)$ in x?

$$f(x) = x_0 x_1 x_2 x_3 x_4 x_6 + x_3 + x_4 x_5 + x_6$$

Upper bound is not enough : lower bound [HLLT 2020]

Specific Higher order derivative

Assume that for any $w \succ u$, $c_w(k) = 0$, then let $V = \{v, v \prec u\}$. Then for any x,

$$\sum_{v \in V} E_k(x + v) = 0$$

Specific Higher order derivative

Assume that for any $w \succ u$, $c_w(k) = 0$, then let $V = \{v, v \prec u\}$. Then for any x,

$$\sum_{v \in V} E_k(x + v) = 0$$

We do not want :
"there do not exist a family of monomials of the form $\{x^u, u \succ u_0\}$".

Specific Higher order derivative

Assume that for any $w \succ u$, $c_w(k) = 0$, then let $V = \{v, v \prec u\}$. Then for any x,

$$\sum_{v \in V} E_k(x + v) = 0$$

We do not want :
"there do not exist a family of monomials of the form $\{x^u, u \succ u_0\}$".

Division Property [Todo 2015]

TECHNIQUES

- Using the representation of the Sbox and the linear layer, this division property can be used for iterated construction
- Mixed Integer Linear Programming
- Lower bound the degree
- Monomial prediction, monomial trails

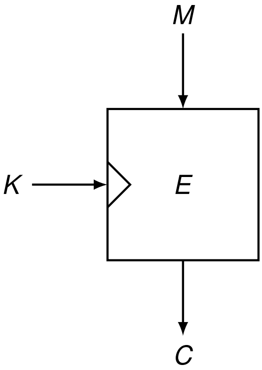
PROBLEMS

- Easy for one monomial, not easy for all...

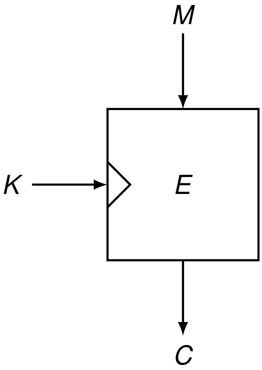
PROBLEMS

- Easy for one monomial, not easy for all...
- Not linearly equivalent [LDF, 2020]

BLOCK CIPHERS

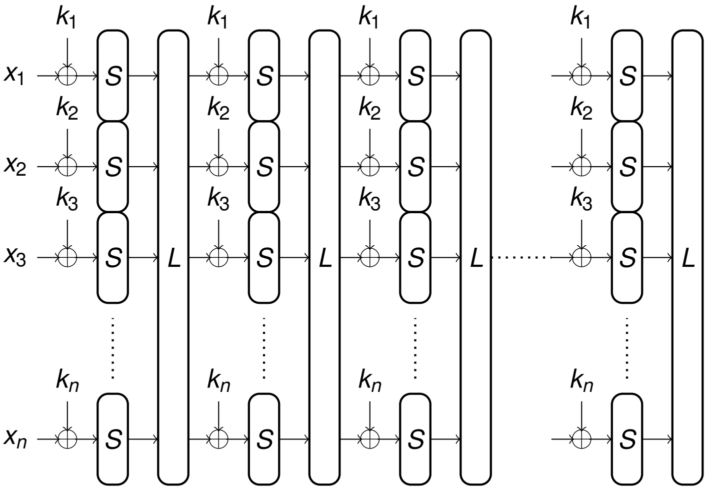


Block ciphers

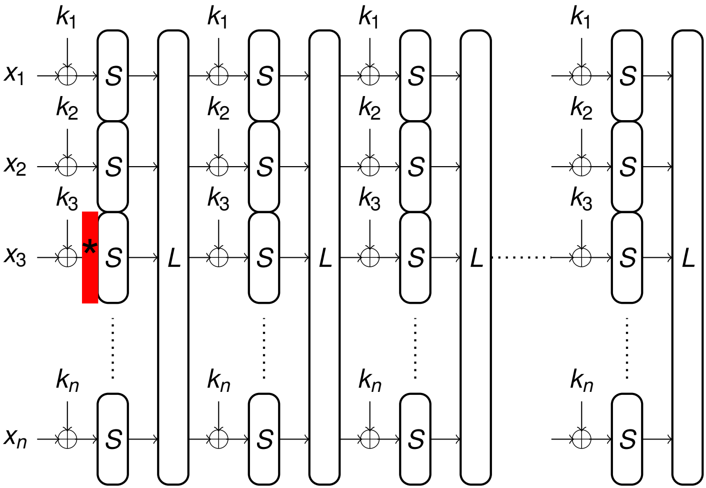


- Proofs of modes, wrt indistinguishability
- Same reasoning for permutation-based constructions.

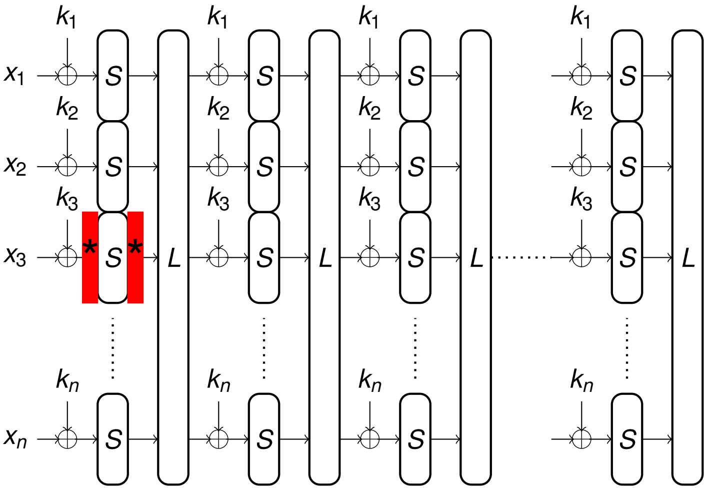
Block ciphers



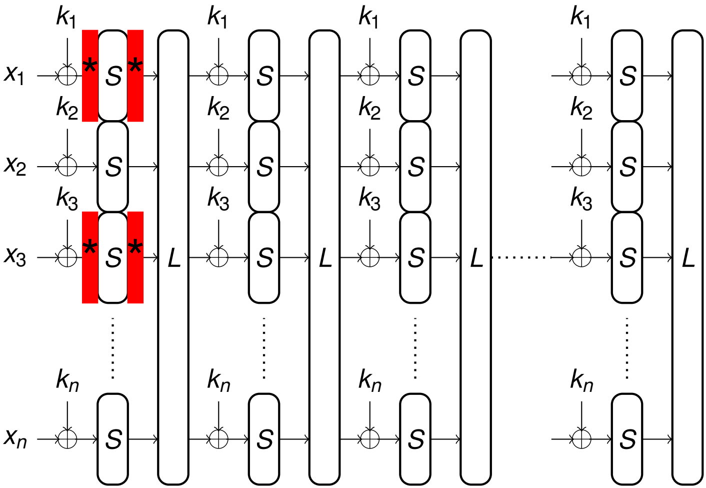
BLOCK CIPHERS



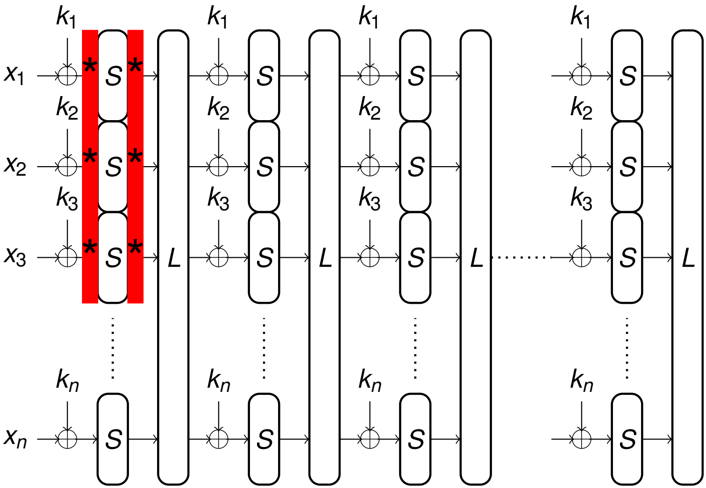
Block ciphers



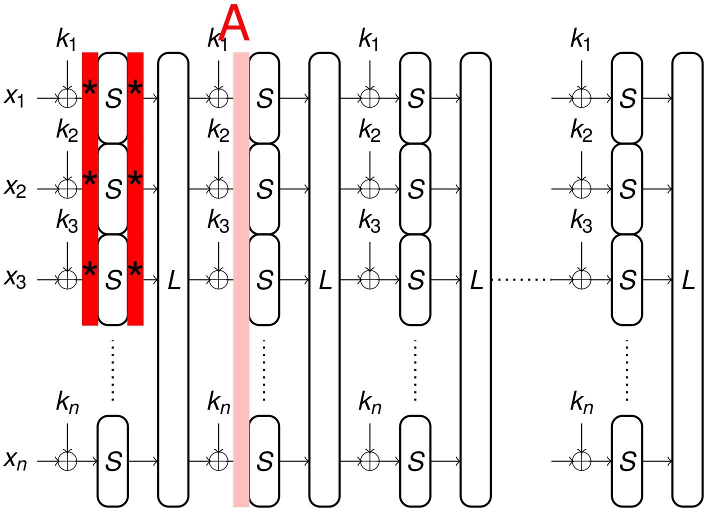
BLOCK CIPHERS



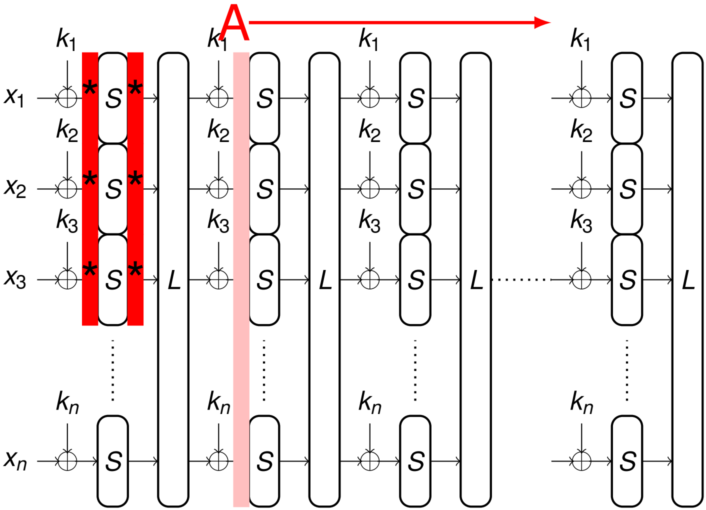
Block ciphers



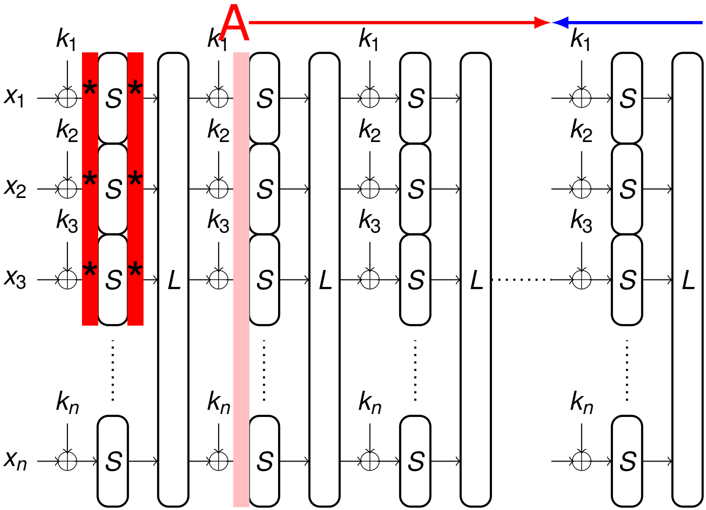
Block ciphers



Block ciphers



Block ciphers



Taking the mode into account

Pyjamask-96

- Distinguisher integral over 10 + 1 rounds
- 3 rounds in the backward direction (monomial count)

Taking the mode into account

Pyjamask-96

- Distinguisher integral over 10 + 1 rounds
- 3 rounds in the backward direction (monomial count)

Considering the mode

- One round in the forward direction
- One round in the backward direction

Taking the mode into account

Pyjamask-96

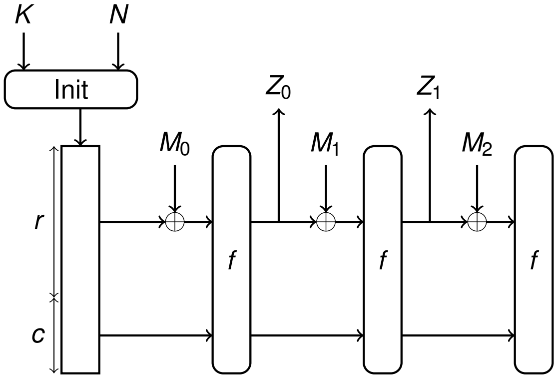
- Distinguisher integral over 10 + 1 rounds
- 3 rounds in the backward direction (monomial count)

Considering the mode

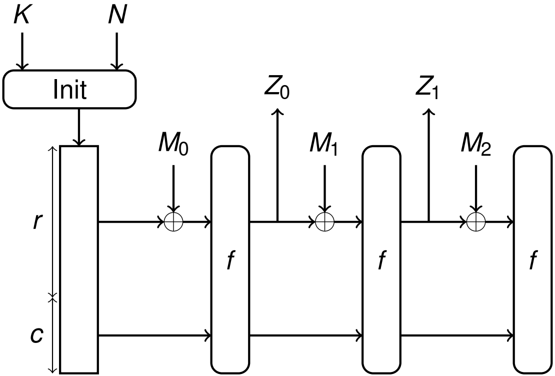
- One round in the forward direction
- One round in the backward direction

Considering the data complexity...

On duplex or stream ciphers



On duplex or stream ciphers



What can you do ?

Representation

Degree

Division property

Attack strategies

Random directions

Random directions

- Representation of polynomials ?

Random directions

- Representation of polynomials ?
- Given a polynomial, find a (non) linear transofrmation that would become an affine space after application ?

Random directions

- Representation of polynomials ?
- Given a polynomial, find a (non) linear transofrmation that would become an affine space after application ?
- Provide a way to state "every $c_u(k)$ is complicated enough" ?

Random directions

- Representation of polynomials ?
- Given a polynomial, find a (non) linear transofrmation that would become an affine space after application ?
- Provide a way to state "every $c_u(k)$ is complicated enough" ?
- Criteria that would be equivalent under the representation of the transformation ?

TAKE AWAY

I'm sure there is a monomial missing somewhere !