

**On the behaviors  
of affine equivalent Sboxes  
regarding differential and linear attacks**

**Anne Canteaut and Joëlle Roué**

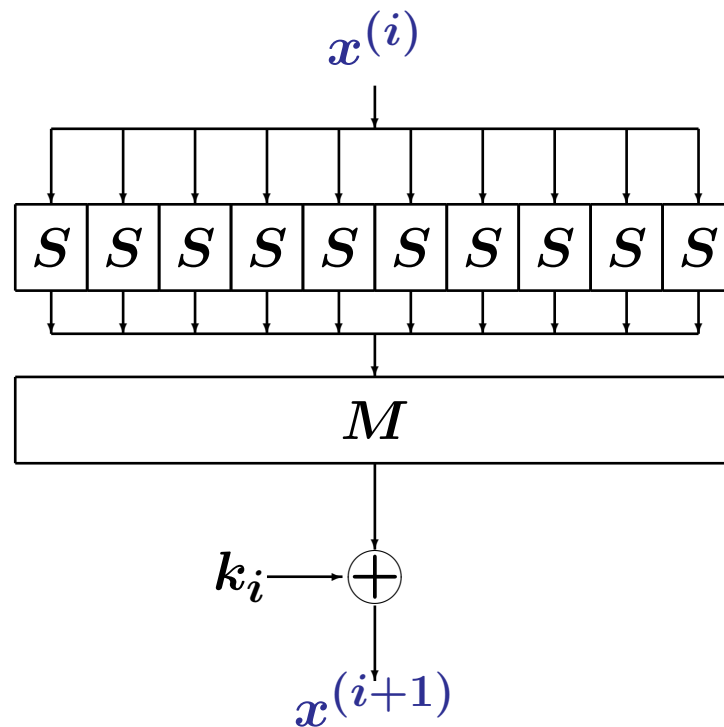
Inria, France

Eurocrypt 2015

## Round function of $\text{SPN}(\textcolor{red}{m}, \textcolor{green}{t}, S, M)$

$S$ : a permutation of  $\mathbb{F}_2^{\textcolor{red}{m}}$

$M$ : a linear permutation mixing the outputs of  $\textcolor{green}{t}$  copies of  $S$



The AES superbox corresponds to two rounds of  $\text{SPN}(8, 4, S, \text{MixColumns})$

## MEDP and MELP

Expected probability of a differential  $(a, b)$

$$\text{EDP}_r(a, b) = 2^{-\kappa} \sum_{k \in \mathbb{F}_2^\kappa} \Pr_X[E_k(X) + E_k(X + a) = b]$$

Maximum expected differential probability for  $r$  rounds:

$$\text{MEDP}_r = \max_{a \neq 0, b} \text{EDP}_r(a, b)$$

Expected square correlation (linear potential) of a mask  $(u, v)$ :

$$\text{ELP}_r(u, v) = 2^{-2n-\kappa} \sum_{k \in \mathbb{F}_2^\kappa} \left( \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot E_k(x)} \right)^2$$

Maximum expected square correlation for  $r$  rounds :

$$\text{MELP}_r = \max_{u, v \neq 0} \text{ELP}_r(u, v)$$

## Expected 2-round differential probability

Difference table of  $S$ .

$$\delta(a, b) = \#\{x \in \mathbb{F}_2^m, S(x + a) + S(x) = b\} .$$

**Problem.** A differential may aggregate many differential trails

First upper bound on  $\text{MEDP}_2$  [Hong et al00][Daemen-Rijmen02]:

$$\text{MEDP}_2 \leq \left( 2^{-m} \max_{a \neq 0, b} \delta(a, b) \right)^{d-1}$$

where  $d$  is the differential branch number of  $M$  over  $\mathbb{F}_2^m$ .

FSE 2003 bound [Park et al. 03]:

$$\text{MEDP}_2 \leq 2^{-md} \max \left( \max_{a \in (\mathbb{F}_2^m)^*} \sum_{\gamma \in (\mathbb{F}_2^m)^*} \delta(a, \gamma)^d, \max_{b \in (\mathbb{F}_2^m)^*} \sum_{\gamma \in (\mathbb{F}_2^m)^*} \delta(\gamma, b)^d \right)$$

$$\max_{a \neq 0} \sum_{\gamma \neq 0} \delta(a, \gamma)^d$$

	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	2	2	2	4	0	2	0	0	2	0	0	0	0	0	2
2	4	2	0	0	0	0	2	0	0	0	2	2	2	0	2
3	0	2	4	0	2	0	0	2	2	0	2	0	2	0	0
4	0	4	0	2	0	2	0	0	0	2	2	0	2	2	0
5	0	2	0	2	2	4	2	2	0	0	0	2	0	0	0
6	0	0	2	0	2	2	2	0	0	2	0	0	2	0	4
7	2	0	0	0	2	2	2	0	4	0	2	0	0	2	0
8	0	0	0	2	0	0	2	2	2	0	0	0	2	4	2
9	2	0	0	0	0	2	0	2	2	2	0	2	4	0	0
a	2	2	0	0	4	0	0	2	0	2	0	0	0	2	2
b	2	0	2	2	2	0	0	0	0	0	0	4	2	2	0
c	0	0	0	2	2	0	0	0	2	4	2	2	0	0	2
d	0	0	2	0	0	2	0	2	0	0	4	2	0	2	2
e	2	0	2	2	0	0	2	4	0	2	2	0	0	0	0
f	0	2	2	0	0	0	4	0	2	2	0	2	0	2	0

## Invariance

$$\text{MEDP}_2 \leq 2^{-md} \max \left( \max_{a \neq 0} \sum_{\gamma \neq 0} \delta(a, \gamma)^d, \max_{b \neq 0} \sum_{\gamma \neq 0} \delta(\gamma, b)^d \right)$$

This bound only depends on the affine equivalence class of  $S$ :

$$\{A_2 \circ S \circ A_1, \quad A_1, A_2 \in GA(\mathbb{F}_2^m)\}$$

**This is not the case of the exact values of  $\text{MEDP}_2$ :**

- AES Sbox  $S(x) = A(x^{254})$ :  $\text{MEDP}_2 = 53 \times 2^{-34}$  [Keliher-Sui 07]
- Naive Sbox  $S(x) = x^{254}$ :  $\text{MEDP}_2 = 79 \times 2^{-34}$  (= FSE 2003 bound).

## Expected 2-round linear potential

Walsh transform of  $S$ .

$$\mathcal{W}(u, v) = \sum_{x \in \mathbb{F}_2^m} (-1)^{u \cdot x + v \cdot S(x)}$$

FSE 2003 bound [Park et al. 03]

$$\text{MELP}_2 \leq \max \left( \max_{u \in (\mathbb{F}_2^m)^*} \sum_{\gamma \in (\mathbb{F}_2^m)^*} \left( \frac{\mathcal{W}(u, \gamma)}{2^m} \right)^{2d^\perp}, \max_{v \in (\mathbb{F}_2^m)^*} \sum_{\gamma \in (\mathbb{F}_2^m)^*} \left( \frac{\mathcal{W}(\gamma, v)}{2^m} \right)^{2d^\perp} \right)$$

where  $d^\perp$  is the linear branch number of  $M$ .

Exact values:

- AES Sbox:  $\text{MELP}_2 = 1.638 \times 2^{-28}$  [Keliher-Sui 07]
- Naive Sbox:  $\text{MELP}_2 = 2.873 \times 2^{-28}$  (= FSE 2003 bound).

## $GF$ -representation

$\mathcal{M}$ : an  $\mathbb{F}_{2^m}$ -linear permutation of  $(\mathbb{F}_{2^m})^t$

$\mathcal{S}$ : a permutation of  $\mathbb{F}_{2^m}$

$$\text{SPN}_{\mathbf{F}}(m, t, \mathcal{S}, \mathcal{M})$$

All quantities can be expressed by means of the  $GF$ -representation:

$$\mathcal{W}_{\mathbf{F}}(\alpha, \beta) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}(\alpha x + \beta \mathcal{S}(x))}$$

$$\delta_{\mathbf{F}}(\alpha, \beta) = \#\{x \in \mathbb{F}_{2^m}, \mathcal{S}(x + \alpha) + \mathcal{S}(x) = \beta\}$$

Link between both representations:

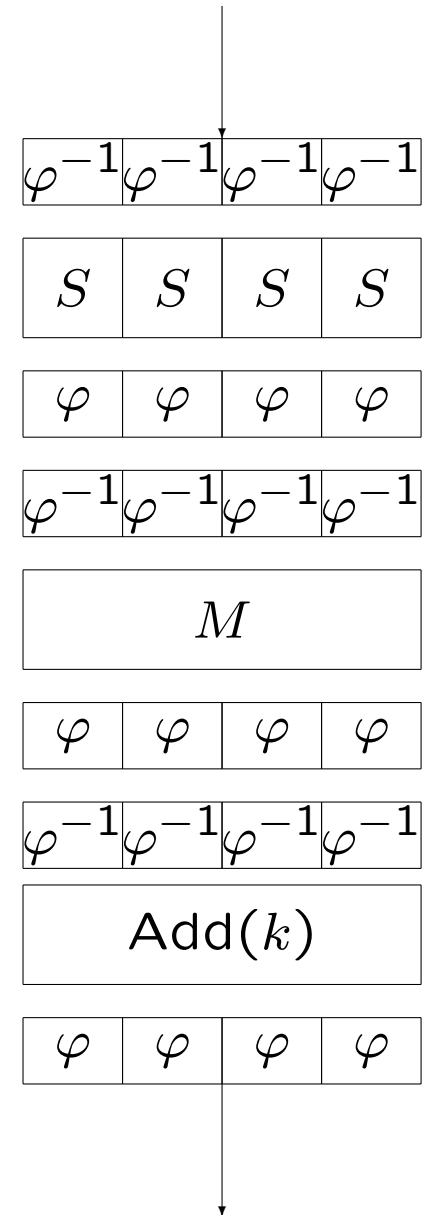
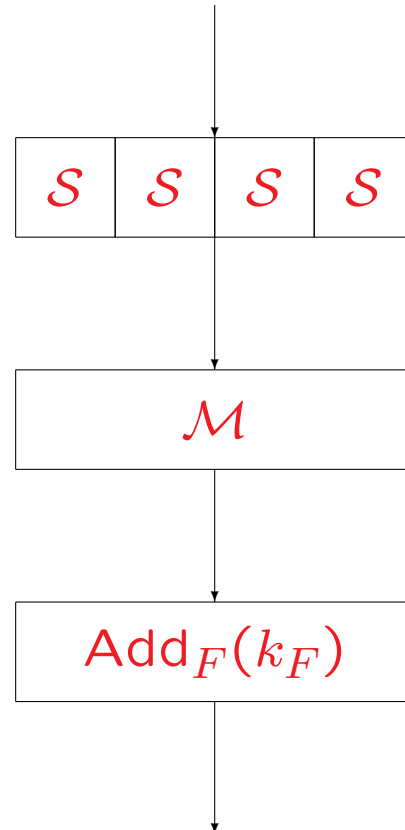
For a given basis  $(\alpha_0, \dots, \alpha_{m-1})$  of  $\mathbb{F}_{2^m}$ ,

$$\varphi : (x_0, \dots, x_{m-1}) \in \mathbb{F}_2^m \longmapsto \sum_{i=0}^{m-1} x_i \alpha_i \in \mathbb{F}_{2^m}$$

$$\Rightarrow \mathcal{S} = \varphi \circ S \circ \varphi^{-1} \text{ and } \mathcal{M} = (\varphi, \dots, \varphi) \circ M \circ (\varphi^{-1}, \dots, \varphi^{-1})$$



The choice of the basis does not affect  $\text{MEDP}_r$  and  $\text{MELP}_r$



**New bounds on  $\text{MEDP}_2$  and  $\text{MELP}_2$**

## New upper bound

**Theorem.** For  $\text{SPN}_F(m, t, \mathcal{S}, \mathcal{M})$  where  $\mathcal{M}$  is an  $\mathbb{F}_{2^m}$ -linear permutation, let

$$\mathcal{B}(\mu) = \max_{\alpha, \beta, \lambda \neq 0} \max_{1 \leq u < d} \sum_{\gamma \neq 0} \delta_F(\alpha, \gamma)^u \delta_F(\gamma \lambda + \mu, \beta)^{(d-u)}$$

Then,

$$\text{MEDP}_2 \leq 2^{-md} \max_{\mu \in \mathbb{F}_{2^m}} \mathcal{B}(\mu)$$

**For the AES Sbox and  $d = d^\perp = 5$ :**

$\text{MEDP}_2 \leq 55.5 \times 2^{-34}$  compared to the FSE 2003 bound:  $79 \times 2^{-34}$

$\text{MELP}_2 \leq 1.862 \times 2^{-28}$  compared to the FSE 2003 bound:  $2.873 \times 2^{-28}$

$$\max_{1 \leq u < d} \sum_{\gamma \neq 0} \delta_F(\alpha, \gamma)^u \delta_F(\gamma, \beta)^{(d-u)}$$

	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	2	2	2	4	0	2	0	0	2	0	0	0	0	0	2
2	4	2	0	0	0	0	2	0	0	0	2	2	2	0	2
3	0	2	4	0	2	0	0	2	2	0	2	0	2	0	0
4	0	4	0	2	0	2	0	0	0	2	2	0	2	2	0
5	0	2	0	2	2	4	2	2	0	0	0	2	0	0	0
6	0	0	2	0	2	2	2	0	0	2	0	0	2	0	4
7	2	0	0	0	2	2	2	0	4	0	2	0	0	2	0
8	0	0	0	2	0	0	2	2	2	0	0	0	2	4	2
9	2	0	0	0	0	2	0	2	2	2	0	2	4	0	0
a	2	2	0	0	4	0	0	2	0	2	0	0	0	2	2
b	2	0	2	2	2	0	0	0	0	0	0	4	2	2	0
c	0	0	0	2	2	0	0	0	2	4	2	2	0	0	2
d	0	0	2	0	0	2	0	2	0	0	4	2	0	2	2
e	2	0	2	2	0	0	2	4	0	2	2	0	0	0	0
f	0	2	2	0	0	0	4	0	2	2	0	2	0	2	0

## A lower bound

$$\mathcal{B}(\mu) = \max_{1 \leq u < d} \max_{\alpha, \beta, \lambda \in \mathbb{F}_{2^m}^*} \sum_{\gamma \in \mathbb{F}_{2^m}^*} \delta_F(\alpha, \gamma)^u \delta_F(\gamma\lambda + \mu, \beta)^{(d-u)}$$

$$\Rightarrow \text{MEDP}_2 \leq 2^{-md} \max_{\mu \in \mathbb{F}_{2^m}} \mathcal{B}(\mu)$$

**Theorem.** There exists an  $\mathbb{F}_2^m$ -linear permutation  $\mathcal{M}$  with maximal branch number  $d = t + 1$  such that the corresponding  $\text{SPN}_F(m, t, \mathcal{S}, \mathcal{M})$  satisfies

$$\text{MEDP}_2 \geq 2^{-md} \mathcal{B}(0)$$

**For involutions:**

If  $\mathcal{S}$  is an involution over  $\mathbb{F}_{2^m}$ , both lower and upper bounds are equal to the FSE 2003 bound.

## Example: $\text{SPN}(4, 4, S, M)$

$x$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$S(x)$	0	1	2	13	4	7	15	6	8	14	11	10	9	3	12	5

- For any  $\mathbb{F}_2$ -linear permutation  $M$  with  $d = 5$ ,

$$\text{MEDP}_2 \leq 34 \times 2^{-14} \text{ (FSE 2003 bound)}$$

- For any  $\mathbb{F}_{2^4}$ -linear permutation  $\mathcal{M}$  with  $d = 5$  defined over  $\mathbb{F}_{2^4}$  where  $\mathbb{F}_{16}$  is identified with  $\mathbb{F}_2^4$  by  $\{1, \alpha, \alpha^2, \alpha^3\}$ ,  $\alpha$  is a root of  $X^4 + X^3 + X^2 + X + 1$ ,

$$\text{MEDP}_2 \leq 33 \times 2^{-14} \text{ (our upper bound)}$$

- There exists an  $\mathbb{F}_{2^4}$ -linear permutation  $\mathcal{M}'$  with  $d = 5$  defined over  $\mathbb{F}_{16}$  where  $\mathbb{F}_{2^4}$  is identified with  $\mathbb{F}_2^4$  by  $\{1, \beta, \beta^2, \beta^3\}$  where  $\beta$  is a root of  $X^4 + X + 1$  such that

$$\text{MEDP}_2 = 34 \times 2^{-14} \text{ (our lower bound)}$$

**Lower bounds for all  $F_{2^m}$ -linear layers**

## Multiplicative invariance for Sboxes

$\mathcal{S}$  has multiplicative-invariant derivatives if, for any  $x \in \mathbb{F}_{2^m}^*$  there exists a permutation  $\pi_x$  of  $\mathbb{F}_{2^m}^*$  such that

$$\delta_F(\alpha, xy) = \delta_F(\pi_x(\alpha), y), \quad \forall y \in \mathbb{F}_{2^m}^*.$$

If  $S$  is a power permutation  $x^s$ :

$\mathcal{S}$  and  $\mathcal{S}^{-1}$  have multiplicative-invariant derivatives.



## Difference table of the inverse function

	1	$a$	$a^2$	$a^3$	$a^4$	$a^5$	$a^6$	$a^7$	$a^8$	$a^9$	$a^{10}$	$a^{11}$	$a^{12}$	$a^{13}$	$a^{14}$
1	4	0	0	0	0	2	0	2	0	0	2	2	0	2	2
$a$	0	0	0	0	2	0	2	0	0	2	2	0	2	2	4
$a^2$	0	0	0	2	0	2	0	0	2	2	0	2	2	4	0
$a^3$	0	0	2	0	2	0	0	2	2	0	2	2	4	0	0
$a^4$	0	2	0	2	0	0	2	2	0	2	2	4	0	0	0
$a^5$	2	0	2	0	0	2	2	0	2	2	4	0	0	0	0
$a^6$	0	2	0	0	2	2	0	2	2	4	0	0	0	0	2
$a^7$	2	0	0	2	2	0	2	2	4	0	0	0	0	2	0
$a^8$	0	0	2	2	0	2	2	4	0	0	0	0	2	0	2
$a^9$	0	2	2	0	2	2	4	0	0	0	0	2	0	2	0
$a^{10}$	2	2	0	2	2	4	0	0	0	0	2	0	2	0	0
$a^{11}$	2	0	2	2	4	0	0	0	0	2	0	2	0	0	2
$a^{12}$	0	2	2	4	0	0	0	0	2	0	2	0	0	2	2
$a^{13}$	2	2	4	0	0	0	0	2	0	2	0	0	2	2	0
$a^{14}$	2	4	0	0	0	0	2	0	2	0	0	2	2	0	2

## A universal lower bounds for multiplication invariant

**Theorem.** For any  $\mathbb{F}_{2^m}$ -linear layer  $\mathcal{M}$  with maximal branch number,

- If both  $\mathcal{S}$  and  $\mathcal{S}^{-1}$  have multiplicative-invariant derivatives, then

$$\text{MEDP}_2 \geq 2^{m(t+1)} \mathcal{B}(0)$$

- if  $\mathcal{S}$  has multiplicative-invariant derivatives, then

$$\text{MEDP}_2 \geq 2^{m(t+1)} \max_{\alpha, \beta \neq 0} \sum_{\gamma \neq 0} \delta_F(\alpha, \gamma)^t \delta_F(\gamma + \mu, \beta)$$

- if  $\mathcal{S}^{-1}$  has multiplicative-invariant derivatives, then

$$\text{MEDP}_2 \geq 2^{m(t+1)} \max_{\alpha, \beta \neq 0} \sum_{\gamma \neq 0} \delta_F(\alpha, \gamma) \delta_F(\gamma + \mu, \beta)^t$$

$\text{SPN}_F(8, 4, \mathcal{S}, \mathcal{M})$  with  $\mathcal{S}(x) = A(x^{254})$  over  $\mathbb{F}_{2^8}$

For any  $\mathbb{F}_{2^8}$ -linear  $\mathcal{M}$  with branch number 5:

- For the affine function  $A$  used in the AES

$$53 \times 2^{-34} \leq \text{MEDP}_2 \leq 55.5 \times 2^{-34}$$

$$1.6384 \times 2^{-28} \leq \text{MELP}_2 \leq 1.8616 \times 2^{-28}$$

For  $\mathcal{M} = \text{MixColumns}$ , the exact values equal the lower bounds.  
There exists some  $\mathcal{M}$  with  $\text{MELP}_2 \geq 1.66 \times 2^{-28}$ .

- For the affine function  $A$  used in SHARK and Square

$$53 \times 2^{-34} \leq \text{MEDP}_2 \leq 56 \times 2^{-34}$$

$$1.7169 \times 2^{-28} \leq \text{MELP}_2 \leq 1.9847 \times 2^{-28}$$

## Involutions with some multiplicative-invariance

Let  $\mathcal{S}$  be an involution of  $\mathbb{F}_{2^m}$ .

If  $\mathcal{S}$  has multiplicative-invariant derivatives, then for any  $\mathbb{F}_{2^m}$ -linear permutation  $\mathcal{M}$  of  $\mathbb{F}_{2^m}^t$  with maximal branch number,

$$\text{MEDP}_2 = 2^{-m(t+1)} \max_{\alpha \in \mathbb{F}_{2^m}^*} \sum_{\gamma \in \mathbb{F}_{2^m}^*} \delta_F(\alpha, \gamma)^{t+1}.$$

**For the naive Sbox:**

$$\text{MEDP}_2 = 79 \times 2^{-34} \text{ and } \text{MELP}_2 = 2.873 \times 2^{-28}$$

for any  $\mathbb{F}_{2^m}$ -linear  $\mathcal{M}$  with branch number 5.

Involutorial power permutations are the weakest Sboxes in their equivalence class whatever MDS linear layer is chosen.

# Conclusions

**Some interactions between  $S$  and  $S^{-1}$  influence MEDP<sub>2</sub> and MELP<sub>2</sub>**

⇒ **Involutions** play a particular role

**Are involutorial Sboxes weak in general?**

- Involutions which do not have any multiplicative-invariant property?
- What happens for more rounds?