

# On a Generalisation of Dillon's APN Permutation

Anne Canteaut

Anne.Canteaut@inria.fr

Sébastien Duval

Sebastien.Duval@inria.fr

Léo Perrin

leo.perrin@uni.lu

April 24, 2017



# Table of Contents

- 1 Introduction
- 2 Generalisation of Butterflies
- 3 Properties of Generalised Butterflies
- 4 Walsh Spectrum and Table of Differences
- 5 Conclusion

# S-Box

## Definition 1 (S-Box)

We will call *Substitution-Box* or *S-Box* any mapping from  $\mathbb{F}_2^m$  into  $\mathbb{F}_2^n$ ,  $n, m \geq 0$ .

## Main Desirable Properties

- ▶ Permutation ( $\Rightarrow n = m$ )
- ▶ Non-linear ( $\Rightarrow n$  small)
- ▶ Resistant to differential attacks
- ▶ Resistant to linear attacks
- ▶ High algebraic degree

# Differential Properties

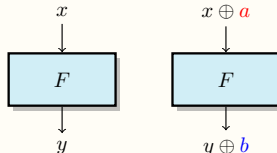
## Definition 2 (Differential Uniformity)

Let  $F$  be a function over  $\mathbb{F}_2^n$ . The table of differences of  $F$  is:

$$\delta_F(a, b) = \#\{x \in \mathbb{F}_2^n \mid F(x \oplus a) = F(x) \oplus b\}.$$

Moreover, the differential uniformity of  $F$  is

$$\delta(F) = \max_{a \neq 0, b} \delta_F(a, b).$$



- ▶  $F$  is resistant against differential attacks if  $\delta(F)$  is small
- ▶  $F$  is called **APN** if  $\delta(F) = 2$

# The Big APN Problem

## The Big APN Problem

We know how to get:

- ▶ APN functions on  $\mathbb{F}_2^n$ ,
- ▶ APN permutations on  $\mathbb{F}_2^n$ ,  $n$  odd,
- ▶ permutations with  $\delta = 4$  on  $\mathbb{F}_2^n$ .

Are there any APN permutations on  $\mathbb{F}_2^n$ ,  $n$  even ?

## 2009: Dillon S-Box

Browning, Dillon, McQuistan, Wolfe: APN permutation on  $\mathbb{F}_2^6$ .

## The Still Big APN Problem

Are there any other APN permutations on  $\mathbb{F}_2^n$ ,  $n$  even ?

# Linear Properties

## Definition 3 (Linearity)

Let  $F$  be a function over  $\mathbb{F}_2^n$ . The table of linear biases of  $F$  is:

$$\lambda_F(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x \oplus b \cdot F(x)}.$$

Moreover, the linearity of  $F$  is

$$\mathcal{L}(F) = \max_{a, b \neq 0} |\lambda_F(a, b)|.$$

- ▶  $F$  is resistant to linear attacks if  $\mathcal{L}(F)$  is small

# Algebraic Degree

## Definition 4 (Univariate degree vs algebraic degree)

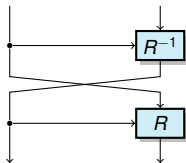
Let  $F$  be a function from  $\mathbb{F}_2^n$  into  $\mathbb{F}_2^n$ .

The *algebraic degree* (aka multivariate degree) of  $F$  is the maximal degree of the algebraic normal forms of its coordinates.

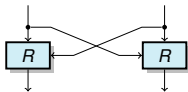
The *univariate degree* of  $F$  is the degree of the univariate polynomial in  $\mathbb{F}_{2^n}[X]$  representing  $F$  when it is identified with a function from  $\mathbb{F}_{2^n}$  into itself.

The algebraic degree of the univariate polynomial  $x \mapsto x^e$  of  $\mathbb{F}_{2^n}$  is the Hamming weight of the binary expansion of  $e$ .

# Butterflies: Definitions (1) [Perrin et al.]



$H_R$ : Open Butterfly



$V_R$ : Closed Butterfly

$R_k : x \mapsto R(x, k)$  permutation  $\forall k$ .

Open Butterfly and Closed Butterfly are CCZ-equivalent  $\Rightarrow$  share the same sets

$$\{\delta_{H_R}(a, b)\}_{a,b} = \{\delta_{V_R}(a, b)\}_{a,b},$$

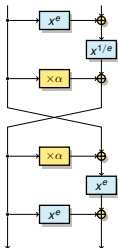
$$\{\mathcal{L}_{H_R}(a, b)\}_{a,b} = \{\mathcal{L}_{V_R}(a, b)\}_{a,b}.$$

In particular,  $\delta(H_R) = \delta(V_R)$  and  $\mathcal{L}(H_R) = \mathcal{L}(V_R)$ .

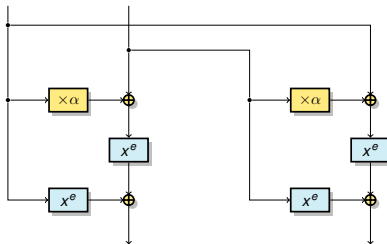


# Butterflies: Definitions (2)

$$R_k[e, \alpha] = (x \oplus \alpha k)^e \oplus k^e, \text{ with } \gcd(e, 2^n - 1) = 1.$$



$H_R$ : Open Butterfly



$V_R$ : Closed Butterfly

Most interesting case for study:  $e = 3 \times 2^t$ .  
Then  $R$  is **quadratic**, and  $V_R$  is **quadratic**.

# Butterflies: Properties

## Theorem 1 (Properties of Butterflies)

Let  $e = 3 \times 2^t$ ,  $\alpha \notin \{0, 1\}$ ,  $n$  odd.

- ▶  $\delta(H_R) \leq 4$ ,  $\delta(V_R) \leq 4$ ,
- ▶  $V_R$  is quadratic,
- ▶  $H_R$  has algebraic degree  $n + 1$ .

## Theorem 2 (APN Butterflies)

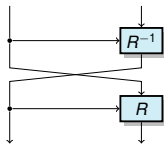
If  $n = 3$  and  $x \mapsto x^e$  is APN, then  $H_R$  is an APN permutation (affine equivalent to the Dillon permutation).

## Open Questions of [Perrin et al.]

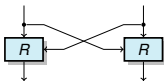
### Open Questions of [Perrin et al.]

- ▶ Nonlinearity/Linearity of  $H_R$  (and  $V_R$ ),
- ▶ Can we find  $\alpha$  such that  $H_R$  is APN for some  $n > 6$  ?

# Generalised Butterflies: Definitions



$H_{\alpha,\beta}$ : *Open Butterfly*



$V_{\alpha,\beta}$ : *Closed Butterfly*

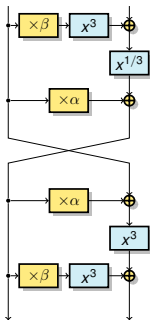
Degree restriction:

- ▶  $R_y : x \mapsto R(x, y)$  permutation  $\forall y$ .
- ▶ Degree of  $R$  is at most 3:
- ▶ Then  $R$  can be written:

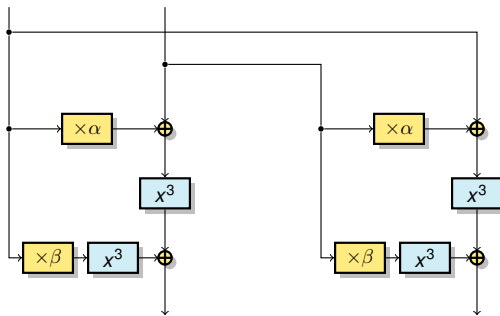
$$R(x, y) = (x \oplus \alpha y)^3 \oplus \beta y^3$$

with  $\alpha, \beta \in \mathbb{F}_2^n$ .

# Generalised Butterflies: Definitions (2)



$H_{\alpha, \beta}$ : Open Butterfly



$V_{\alpha, \beta}$ : Closed Butterfly

# Equivalences

- ▶  $H_{\alpha,\beta}$  and  $V_{\alpha,\beta}$  are CCZ-equivalent.
- ▶ When  $\alpha = 1$ ,  $H_{\alpha,\beta}$  is equivalent to a 3-round Feistel network.
- ▶ Butterfly with  $e = 3 \times 2^t$  is affine-equivalent to Butterfly with  $e = 3$ .
- ▶  $V_{\alpha,\beta}$  and  $V_{\alpha^2,\beta^2}$  are affine-equivalent.
- ▶ If  $\alpha \neq 1$ ,  $V_{\alpha,\beta}$  and  $V_{\alpha,\beta^{-1}(1+\alpha)^6}$  are affine-equivalent.

# Property of Quadratic Functions

## Property 1 (Linearity of Quadratic Functions)

*Let  $f$  be a quadratic Boolean function of  $n$  variables.*

$$\text{LS}(f) = \{a \in \mathbb{F}_2^n : D_a f \text{ is constant}\}$$

*Then  $\mathcal{L}(f) = 2^{\frac{n+s}{2}}$ , with  $s = \dim \text{LS}(f)$ .*

*Moreover, the Walsh coefficients of  $f$  only the values  $\pm 2^{\frac{n+s}{2}}$  and 0.*

# Linear Properties

## Theorem 3

Let  $n > 1$  be an odd integer and  $(\alpha, \beta)$  be a pair of nonzero elements in  $\mathbb{F}_{2^n}$ .

- ▶ If  $\beta \neq (1 + \alpha)^3$ ,

$$\mathcal{L}(V_{\alpha,\beta}) = 2^{n+1}$$

and the Walsh coefficients of  $V_{\alpha,\beta}$  belong to  $\{0, \pm 2^n, \pm 2^{n+1}\}$ .

- ▶ If  $\beta = (1 + \alpha)^3$ ,

$$\mathcal{L}(V_{\alpha,\beta}) = 2^{\frac{3n+1}{2}}.$$



# Differential Properties

## Theorem 4 (Differential uniformity)

Let  $n > 1$  odd,  $\alpha, \beta \in \mathbb{F}_{2^n} \setminus \{0\}$ . Then:

- ▶ If  $\beta \neq (1 + \alpha)^3$ ,  $\delta(H_{\alpha,\beta}) \leq 4$ .
- ▶ If  $\beta = (1 + \alpha)^3$ ,  $\delta(H_{\alpha,\beta}) = 2^{n+1}$ .

## Theorem 5 (APN Condition)

Let  $\alpha \neq 0, 1$ .  $H_{\alpha,\beta}$  is APN if and only if:

$$\beta \in \{(\alpha + \alpha^3), (\alpha^{-1} + \alpha^3)\} \text{ and } \text{Tr}(\mathcal{A}_\alpha(\mathbf{e})) = 1, \forall \mathbf{e} \notin \{0, \alpha, 1/\alpha\},$$

where  $\mathcal{A}_\alpha(\mathbf{e}) = \frac{\mathbf{e}\alpha(1+\alpha)^2}{(1+\alpha\mathbf{e})(\alpha+\mathbf{e})^2}$ .

This condition implies that  $n = 3$ .

# Algebraic Degree

## Theorem 6

Let  $\alpha$  and  $\beta$  be two nonzero elements in  $\mathbb{F}_{2^n}$ .

$H_{\alpha,\beta}$  has an algebraic degree equal to  $n$  or  $n + 1$ .

It is equal to  $n$  if and only if

$$(1 + \alpha\beta + \alpha^4)^3 = \beta(\beta + \alpha + \alpha^3)^3.$$

# $\alpha = 1$ : 3-round Feistel Network

## Proposition 1

*For  $\alpha = \beta = 1$ , the difference distribution tables of the butterflies  $V_{1,1}$  and  $H_{1,1}$  contain the values 0 and 4 only.*

# Generalised Butterflies

## Corollary 7 (Walsh and differential spectra of generalised butterflies)

Let  $\alpha$  and  $\beta$  be two nonzero elements in  $\mathbb{F}_{2^n}$  such that  $\beta \neq (1 + \alpha)^3$ .

- *Walsh spectrum:*

$$\left| \widehat{H_{\alpha, \beta}}(u, v) \right| = \begin{cases} 0, & 3 \times 2^{2n-2}(2^n - 1)(2^n + 1 - C) \text{ times} \\ 2^n, & 2^{2n}(2^n - 1)C \text{ times} \\ 2^{n+1}, & 2^{2n-2}(2^n - 1)(2^n + 1 - C) \text{ times.} \end{cases}$$

where  $(2^n - 1)C$  is the number of bent components of  $V_{\alpha, \beta}$ .

- *Table of differences:*

$$\delta_{H_{\alpha, \beta}}(a, b) = \begin{cases} 2, & 2^{2n-2}(2^n - 1) \times 3C \text{ times} \\ 4, & 2^{2n-3}(2^n - 1)(2^{n+2} + 4 - 3C) \text{ times} \end{cases}$$

# New Permutations

Value of  $C$  for a Butterfly on 6 bits ( $\mathbb{F}_{2^3}$  defined by the primitive element  $a$  such that  $a^3 + a + 1 = 0$ ).

$\alpha \backslash \beta$	1	$a$	$a^2$	$a^3$	$a^4$	$a^5$	$a^6$
1	0	4	4	4	4	4	4
$a$	6	2	0	2	6	0	0
$a^3$	2	4	2	0	2	4	2

These permutations are **new**:

- ▶ The value of  $C$  determines the differential and Walsh spectra,
- ▶ The case  $\beta = 1$  does not include all possible values for  $C$   
 $\Rightarrow$  the generalisation gives new permutations,
- ▶ **Differential/Linear spectra are different** from any other studied permutations, for example:
  - ▶ For  $n = 3$ , the number of 4 in the differential spectrum is in  $\{0, 336, 672, 1008\}$ ,
  - ▶ Gold and Kasami permutations: number of 4 = 1008,
  - ▶ Inverse mapping: number of 4 = 63,

# Conclusion

This work in brief:

- ▶ We answered the 2 open questions from Perrin et al.,
- ▶ We identified a new family of  $2n$  bit-functions,  $n \geq 3$  odd with:
  - ▶ differential uniformity 4,
  - ▶ linearity  $2^{n+1}$ ,
  - ▶ a simple representation (easier implementation and analysis),
  - ▶ the permutation from Dillon et al. included.
- ▶ We proved that this natural generalisation does not contain any new APN permutation. :-)

Questions ?