On a Generalisation of Dillon's APN Permutation

Anne Canteaut
Anne.Canteaut@inria.fr

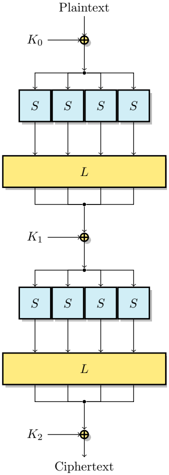
Sébastien Duval
Sebastien.Duval@inria.fr

Léo Perrin
leo.perrin@uni.lu

May 11, 2017

Table of Contents

SPN Ciphers



- Rijndael/AES (J. Daemen, V. Rijmen, 1988)
- Succession of confusion/diffusion layers
- Good for parallelism and easy to implement

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

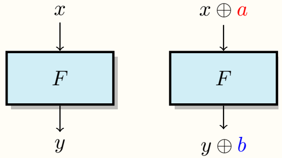
Definition 2 (Differential Uniformity)

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

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



- 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

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

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

Algebraic Degree

Definition 4 (Univariate degree vs algebraic degree)

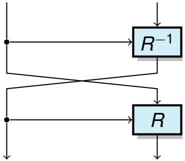
Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$.

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

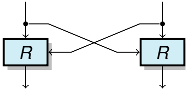
The *univariate degree* of F is the degree of the univariate polynomial in $\mathbb{F}_{2^n}[X]$ representing F when it is identified with a function from $\mathbb{F}_{2^n}$ into itself.

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

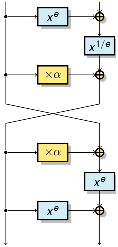
$$\{\delta_{\mathsf{H}_R}(a,\ b)\}_{a,b} = \{\delta_{\mathsf{V}_R}(a,\ b)\}_{a,b},$$

$$\{\mathcal{L}_{\mathsf{H}_R}(a,\ b)\}_{a,b} = \{\mathcal{L}_{\mathsf{V}_R}(a,\ b)\}_{a,b}.$$

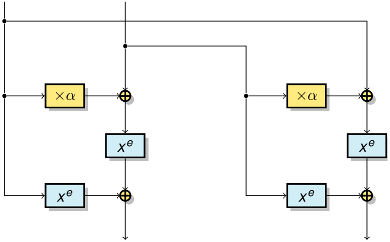
In particular, $\delta(\mathsf{H}_R) = \delta(\mathsf{V}_R)$ and $\mathcal{L}(\mathsf{H}_R) = \mathcal{L}(\mathsf{V}_R)$.

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.

- $\delta(\mathrm{H}_R) \leq 4$, $\delta(\mathrm{V}_R) \leq 4$,
- 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 α such that H_R is APN for some $n > 6$?

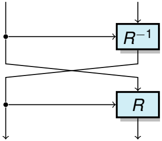
Objective of this Work

- Deeper study of butterflies:
  - Linearity
  - Are there other APN butterflies ?
- Generalise butterflies: from the structure

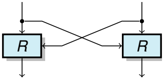
Results

- Generalisation of butterflies (quadratic case)
- Study of generalised butterflies
- Computed linearity of (generalised) butterflies
- Condition for APN $\Rightarrow$ No other APN butterflies

Generalised Butterflies: Definitions



$\mathsf{H}_{\alpha,\beta}$: *Open Butterfly*



$\mathsf{V}_{\alpha,\beta}$: *Closed Butterfly*

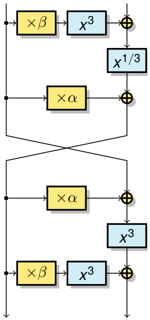
Degree restriction:

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

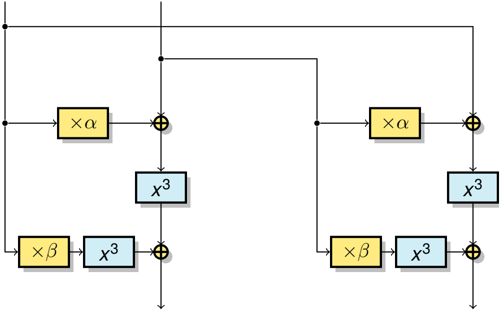
$$R(x, y) = (x \oplus \alpha y)^3 \oplus \beta y^3$$

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

Generalised Butterflies: Definitions (2)



$\mathrm{H}_{\alpha,\beta}$: *Open Butterfly*



$\mathrm{V}_{\alpha,\beta}$: *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_{α^2,β^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.

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

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

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 (α, β) 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 $\beta \neq (1+\alpha)^3$, $\delta(\mathrm{H}_{\alpha,\beta}) \leq 4$.*
- *If $\beta = (1+\alpha)^3$, $\delta(\mathrm{H}_{\alpha,\beta}) = 2^{n+1}$.*

Theorem 5 (APN Condition)

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

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

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

This condition implies that $n = 3$.

Differential Properties

Theorem 4 (Differential uniformity)

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

- *If $\beta \neq (1+\alpha)^3$, $\delta(\mathrm{H}_{\alpha,\beta}) \leq 4$.*
- *If $\beta = (1+\alpha)^3$, $\delta(\mathrm{H}_{\alpha,\beta}) = 2^{n+1}$.*

Theorem 5 (APN Condition)

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

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

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

This condition implies that $n = 3$.

Overview of the proof of APN $\Rightarrow n = 3$

Theorem 6 (APN Condition)

Let $\alpha \neq 0, 1$. $\mathrm{H}_{\alpha,\beta}$ *is APN if and only if:*

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

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

Steps:

- Simplify to $\mathrm{Tr}\left(\mathcal{C}_\alpha(v)\right) = 1,\ \forall\ u \notin \left\{0, 1, 1/(1+\alpha^{-2})\right\}$ with

$$\mathcal{C}_\alpha(v) = \left(\frac{1}{1+\alpha^{-1}}\right)^4 \frac{1}{u+u^3}.$$

- Prove that APN $\Rightarrow n = 3$.

Simplification (1)

APN Conditions

$$\mathrm{Tr}\left(\mathcal{A}_\alpha(e)\right) = 1$$

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

$$\beta \in \{\beta_0, \beta_1\} = \{\alpha+\alpha^3, (\alpha+1)^4/\alpha\}$$

$$e \notin \{0, \alpha, \alpha^{-1}\}$$

$$\alpha \neq 1$$

$$\ell = (e+\alpha)(1+\alpha)^2$$

$$e(1+\alpha)^2 = \ell + \alpha + \alpha^3$$

$$(1+\alpha e)(1+\alpha)^2 = \alpha(\ell + \frac{(1+\alpha)^4}{\alpha})$$

$$\Downarrow$$

$$\mathcal{A}_\alpha(\ell) = \frac{\beta_0\beta_1}{\ell^2}\,\frac{\ell+\beta_0}{\ell+\beta_1}$$

Simplification (2)

<u>APN Conditions</u>

$$\mathrm{Tr}\left(\mathcal{A}_\alpha(\ell)\right) = 1$$

$$\mathcal{A}_\alpha(\ell) = \frac{\beta_0\beta_1}{\ell^2}\frac{\ell+\beta_0}{\ell+\beta_1}$$

$$\beta \in \{\beta_0, \beta_1\} = \{\alpha+\alpha^3, (\alpha+1)^4/\alpha\}$$

$$\ell \notin \{\beta_0, 0, \beta_1\}$$

$$\alpha \neq 1$$

$$\mathcal{B}_\alpha(v) = \frac{v^2(v+1)}{(v+\beta_0/\beta_1)}$$

$$\mathcal{B}_\alpha\left(\frac{\beta_0}{\ell}\right) = \frac{\beta_0\beta_1}{\ell^2}\frac{\ell+\beta_0}{\ell+\beta_1} = \mathcal{A}_\alpha(\ell)$$

Simplification (3)

<u>APN Conditions</u>

$$\mathrm{Tr}\left(\mathcal{B}_\alpha(v)\right) = 1$$

$$\mathcal{B}_\alpha(v) = \frac{v^2(v+1)}{(v+\beta_0/\beta_1)}$$

$$\beta \in \{\beta_0, \beta_1\} = \{\alpha+\alpha^3, (\alpha+1)^4/\alpha\}$$

$$v \notin \{0, 1, \frac{\alpha^2}{1+\alpha^2}\}$$

$$\alpha \neq 1$$

$$\mathrm{Tr}\left(\mathcal{B}_\alpha(v)\right) = \mathrm{Tr}\left(\frac{v^2+v}{\gamma v+1}\right)$$

where $\gamma = 1 + \alpha^{-2}$

$$\mathrm{Tr}\left(\mathcal{B}_\alpha\left(u^{-1}\gamma^{-1}\right)\right) = \mathrm{Tr}\left(\frac{\gamma^{-2}}{u+u^3}\right)$$

with $u \notin \{0, \gamma^{-1}, 1\}$

$$\mathcal{C}_\alpha(u) = \frac{\gamma^{-2}}{u+u^3}$$

$$\mathrm{Tr}\left(\mathcal{C}_\alpha(u)\right) = \mathrm{Tr}\left(\mathcal{B}_\alpha\left(u^{-1}\gamma^{-1}\right)\right)$$

$\square$

Proof that APN $\Rightarrow n = 3$ (1)

Lemma 1 (BRS67)

The cubic equation $x^3 + ax + b = 0$, where $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^*$ has a unique solution in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}\left(a^3/b^2\right) \neq \mathrm{Tr}\left(1\right)$.

Proposition 1 ($n = 3$)

Let $n > 1$ be an odd integer, $\lambda \in \mathbb{F}_{2^n}^*$. If

$$\mathrm{Tr}\left(\frac{\lambda^2}{x + x^3}\right) = 1, \forall x \notin \{0, 1, \lambda\},$$

then $n = 3$.

Proof that APN $\Rightarrow n = 3$ (2)

The condition is $\mathrm{Tr}\left(\frac{\lambda^2}{x+x^3}\right) = 1, \forall x \notin \{0, 1, \lambda\}$.
Let $z \in \mathbb{F}_{2^n}^*, \mathrm{Tr}(z) = 0$. There exists a unique $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ s.t.

$$\frac{1}{x^3 + x} = z$$

Indeed, since $z \neq 0$, we get:

$$x^3 + x + \frac{1}{z} = 0$$

Lemma $\Rightarrow$ unique solution when $\mathrm{Tr}\left(z^2\right) = \mathrm{Tr}(z) = 0$.

Proof that APN $\Rightarrow n = 3$ (3)

Define $z_\lambda = \frac{1}{\lambda^3+\lambda}$ and $\mathcal{Z} = \{z \in \mathbb{F}_{2^n}^* \setminus \{z_\lambda\} : \mathrm{Tr}(z) = 0\}$.
Condition becomes: $\mathrm{Tr}\left(\lambda^2 z\right) = 1$.
If $n \geq 5$, $\mathcal{Z}$ contains $(2^{n-1} - 2) \geq 14$ elements $\Rightarrow$ there exist $z_0, z_1 \in \mathcal{Z}$ s.t. $z_0 + z_1 \in \mathcal{Z}$. Thus,

$$\mathrm{Tr}\left(\lambda^2 z_0\right) = \mathrm{Tr}\left(\lambda^2 z_1\right) = \mathrm{Tr}\left(\lambda^2 (z_0 + z_1)\right) = 1$$

Impossible since

$$\mathrm{Tr}\left(\lambda^2 (z_0 + z_1)\right) = \mathrm{Tr}\left(\lambda^2 z_0\right) + \mathrm{Tr}\left(\lambda^2 z_1\right)$$

When $n = 3$ it is different: $2^{n-1} - 2 = 2$, this argument cannot stand. $\square$

Algebraic Degree

Theorem 7

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

$\mathrm{H}_{\alpha,\beta}$ 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 2

For $\alpha = \beta = 1$, the difference distribution tables of the butterflies $\mathrm{V}_{1,1}$ and $\mathrm{H}_{1,1}$ contain the values 0 and 4 only.

Generalised Butterflies

Corollary 8 (Walsh and differential spectra of generalised butterflies)

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

- *Walsh spectrum:*

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

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

- *Table of differences:*

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

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 ?