If a generalised butterfly is APN then it operates on 6 bits

Anne Canteaut, Léo Perrin, Shizhu Tian

If a Generalised Butterfly is APN then it Operates on 6 Bits

Anne Canteaut[1], Léo Perrin[1], Shizhu Tian[1,2,3]

[1] Inria, Paris, France.
[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[3] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

{firstname.lastname}@inria.fr

Abstract

Whether there exist Almost Perfect Non-linear permutations (APN) operating on an even number of bit is the so-called *Big APN Problem*. It has been solved in the 6-bit case by Dillon et al. in 2009 but, since then, the general case has remained an open problem.

In 2016, Perrin et al. discovered the butterfly structure which contains Dillon et al.'s permutation over $\mathbb{F}_{2^6}$. Later, Canteaut et al. generalised this structure and proved that no other butterflies with exponent 3 can be APN. Recently, Yongqiang et al. further generalized the structure with Gold exponent and obtained more differentially 4-uniform permutations with the optimal nonlinearity. However, the existence of more APN permutations in their generalization was left as an open problem.

In this paper, we adapt the proof technique of Canteaut et al. to handle all Gold exponents and prove that a generalised butterfly with Gold exponents over $\mathbb{F}_{2^{2n}}$ can never be APN when $n > 3$. More precisely, we prove that such a generalised butterfly being APN implies that the branch size is strictly smaller than 5. Hence, the only APN butterflies operate on 3-bit branches, i.e. on 6 bits in total.

Keywords. Boolean function, Sbox, APN, Differential uniformity, Butterflies

1 Introduction

S(ubstitution)-boxes are core components in symmetric ciphers where they serve as the confusion part. In most cases, they are their only nonlinear components. In order for the algorithm to resist the two most prominent cryptanalysis techniques, namely differential [2, 3] and linear attacks [13], S-boxes should have a low differential uniformity [14] and a high nonlinearity [7].

Let F be a function from $\mathbb{F}_2^m$ into $\mathbb{F}_2^m$. We say that F is *differentially δ-uniform* if, for any nonzero a in $\mathbb{F}_2^m$ and $b \in \mathbb{F}_2^m$, the equation $F(x) + F(x+a) = b$ has at most δ solutions in $\mathbb{F}_2^m$. The lower bound for functions on $\mathbb{F}_2^m$ is 2, and the functions that achieve this bound are called *Almost Perfect Nonlinear (APN)* [15]. That is, a function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is APN if the following equation has at most two solutions:

$$F(x) + F(x+a) = b$$

for any $b \in \mathbb{F}_2^m$ and any $a \in \mathbb{F}_2^m$ such that $a \neq 0$. An APN permutation over $\mathbb{F}_2^m$ would be an S-box providing optimal protection against differential attacks. Such components are easy to find for m odd: the Gold functions $x \mapsto x^{2^i+1}$ and the inverse mapping $x \mapsto x^{2^m-2}$, which are defined by identifying $\mathbb{F}_{2^m}$ with $\mathbb{F}_2^m$, are APN permutations in this case. However, the very existence of APN permutations operating on an even number of bits is an open problem nicknamed the *big APN problem*.

Open Problem 1 (Big APN Problem)**.** *Is there an APN permutation of $\mathbb{F}_{2^m}$ where $m = 2n$?*

It has been an open problem in the field of vectorial Boolean functions since Nyberg introduced the differential uniformity in the early 90's [14].

Some negative results are known. For instance, Hou proved in [10] that there are no APN permutations over $\mathbb{F}_{2^4}$ and that there are no APN permutations over $\mathbb{F}_{2^{2n}}$ with coefficients in $\mathbb{F}_{2^n}$. Also, an APN permutation over $\mathbb{F}_{2^{2n}}$ cannot neither be a monomial function nor a quadratic function [1].

The only known solution to this problem is a sporadic case found by Dillon et al. [4] for $m = 6$. At the time of writing, it remains the only known APN permutation over $\mathbb{F}_{2^{2n}}$. This solution was constructed by finding a permutation in the CCZ-equivalence class of a known quadratic APN function, namely the Kim mapping $x \mapsto x^3 + x^{10} + gx^{24}$ where g is a root of the primitive polynomial used to define $\mathbb{F}_{2^6}$.

To try and use a similar approach, Yu et al. [17] designed a new matrix-based method to generate quadratic APN functions. They obtained 8157 new quadratic APN functions over $\mathbb{F}_{2^8}$. However, none of these APN functions are CCZ-equivalent to permutations.

In [16], Perrin et al. identified a specific structure called *Open Butterfly* which is affine-equivalent to Dillon et al.'s permutation. This structure is easily defined over higher dimensions, but, unfortunately, Canteaut et al. [5] proved that an even broader family of permutations containing the butterflies of Perrin et al. did not contain any APN permutations for $m > 6$.

Several teams then studied other generalizations of the original butterfly of [16]. Firstly, it was shown in [8] that changing the exponent from 3 to $2^i + 1$ in the construction of Perrin et al. still yielded differentially 4-uniform permutations. Then, Li et al. showed that the generalization of Canteaut et al. had the same properties [11], and that this family of generalised butterflies contains some functions which are not CCZ-equivalent to the functions studied in [5]. In each case, the authors established that such generalizations have a differential uniformity at most equal to 4 except in some sporadic cases but they left the existence of APN permutations among them as an open problem. In this paper, we answer this question by proving the following theorem.

Theorem 1. *If a generalised butterfly is APN then it operates on 6 bits.*

In other words, natural quadratic generalizations of the initial structure of Perrin et al. do not provide any new solutions to the big APN problem.

The remainder of the paper is our proof of this theorem. First, we formally describe generalized butterflies and some of their basic properties in Section 2. Then, in Section 3, we present some useful propositions, both new ones and from the literature, which will be used further in the paper. Our proof then operates in two high level steps. In Section 4, we establish a necessary criterion for a butterfly to be APN which we call the *refined trace condition*. Then, in Section 5, we show that this condition implies that the block size is upperbounded by 6 so that Theorem 1 holds.

2 Generalised Butterflies

In this section, we formally define the generalisation of the butterfly structure we consider in this paper and establish some of its most basic properties.

2.1 Definition

In the remainder of the paper, we consider an even integer $m = 2n$ which is not divisible by 4, i.e., n is always odd. Also, vectorial Boolean functions from $\mathbb{F}_2^m$ into $\mathbb{F}_2^m$ are identified with mappings from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ to itself. It is worth noticing that the choice of the basis used for identifying $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ does not affect the cryptographic properties of the functions we are studying since different bases lead to functions which are affine-equivalent.

We now define the family of vectorial functions that will be studied in the paper.

Definition 1 (Generalised Butterflies)**.** *Let R be a bivariate polynomial of $\mathbb{F}_{2^n}$ such that $R_y : x \mapsto R(x,y)$ is a permutation of $\mathbb{F}_{2^n}$ for all y in $\mathbb{F}_{2^n}$. The* closed butterfly V_R *is the function of $(\mathbb{F}_{2^n})^2$ defined by*

$$\mathsf{V}_R(x,y) \;=\; \big(R(x,y),\; R(y,x)\big)$$

and the open butterfly H_R *is the permutation of $(\mathbb{F}_{2^n})^2$ defined by*

$$\mathsf{H}_R(x,y) \;=\; \big(R_{R_y^{-1}(x)}(y),\; R_y^{-1}(x)\big)$$

where $R_y(x) = R(x,y)$ and $R_y^{-1}\left(R_y(x)\right) = x$ for any x, y. A representation of H_R is given in Figure 1a and one of V_R is given in Figure 1b.

(a) The open butterfly H_R (bijective). (b) The closed butterfly V_R.

Figure 1: The butterfly constructions.

It can be easily checked that, for any choice of the keyed permutation R, the open butterfly H_R is an involution and, as such, a permutation.

Several particular cases of this structure have been presented in the literature. They consist in iterative generalizations of the first butterfly structure which was introduced in [16].

- In [16], Perrin et al. found that Dillon et al.'s permutation is affine equivalent to H_R with $R_y(x) = (x + \alpha y)^3 + y^3$, for $n = 3$, where $\mathrm{Tr}\,(\alpha) = 0$. They showed that such structures always have algebraic degree $n+1$ and a differential uniformity at most equal to 4 whenever $\alpha \neq 0$ and n is odd. However, they left their nonlinearity as an open problem along with the existence of APN permutations for $n > 3$ among them.

- Canteaut et al. [5] considered the broader class of polynomials $R_y(x) = (x + \alpha y)^3 + \beta y^3$ which, up to equivalence, contains all R of degree 3 such that R_y is always a permutation. They showed that it was always differentially 4 (except for some sporadic cases) and that it could only be APN when $n = 3$. They also showed that the nonlinearity of butterflies was always equal to the best known one (except for some sporadic cases). Their results are trivially generalized to exponents of the form 3×2^i.

- Fu et al. [8] instead chose to look at different exponents, i.e. at $R_y = (x + \alpha y)^{2^i+1} + y^{2^i+1}$ with $\gcd(i, n) = 1$. They showed that, again, such structures were always differentially 4-uniform and always have the best nonlinearity known to be possible. They also proved that the *closed* butterfly with $\alpha = 1$ was always a permutation.

- Li et al. [11] investigated the broadest class of butterflies, namely those with $R_y = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1}$ with $\gcd(i, n) = 1$. They showed that, except in some sporadic cases, the nonlinearity of such constructions was the best known to be possible and the differential uniformity was at most 4. However, they left the existence of APN functions among them as an open problem.

In this paper, we focus on the broadest definition, i.e. on the case where

$$R_y = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1}$$

with $\gcd(i, n) = 1$. As Li et al. already proved that such structures yield the best known nonlinearity and differential uniformity, we focus only on whether they can be APN or not.

2.2 Equivalence Relations

To begin with, we recall some basic notations of equivalence relations among vectorial Boolean functions. Two functions F_1, F_2 from $\mathbb{F}_2^m$ into $\mathbb{F}_2^m$ are *E(xtended) A(ffine)-equivalent* if there exist two affine permutations A_1, A_2 from $\mathbb{F}_2^m$ into $\mathbb{F}_2^m$ and an affine function A_3 from $\mathbb{F}_2^m$ into $\mathbb{F}_2^m$ such that

$$F_1(x) = A_1(F_2(A_2(x))) + A_3(x) \ .$$

A more general framework is introduced by considering the graphs of the functions [6]. Two functions F_1, F_2 from $\mathbb{F}_2^m$ into $\mathbb{F}_2^m$ are called CCZ-equivalent (after Carlet, Charpin and Zinoviev) if there exists an affine permutation $\mathcal{L}$ over $\mathbb{F}_2^{2m}$ such that

$$\mathcal{L}\left(\left\{(x, F_1(x)), \forall x \in \mathbb{F}_2^m\right\}\right) \ = \ \left\{(x, F_2(x)), \forall x \in \mathbb{F}_2^m\right\}$$

Both the differential uniformity and the nonlinearity are invariant under both EA-equivalence and CCZ-equivalence. In particular, all functions CCZ-equivalent to an APN function are APN themselves.

As in the case studied in [5], the generalised butterflies with $R_y(x) = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1}$ are linked by the following relations.

- If the exponent is equal to $e = (2^i + 1) \times 2^t$, the corresponding closed butterfly is affine-equivalent to the closed butterfly with $e = 2^i + 1$ and the same α, β. Therefore, all results presented in the paper also hold when

  $$R(x, y) = (x + \alpha y)^{(2^i+1)\times 2^t} + \beta y^{(2^i+1)\times 2^t}$$

  for some t.

- The closed butterflies $\mathsf{V}_{\alpha,\beta}$ and $\mathsf{V}_{\alpha^2,\beta^2}$ are affine-equivalent as $\mathsf{V}_{\alpha^2,\beta^2}(x^2, y^2) = (\mathsf{V}_{\alpha,\beta}(x, y))^2$.

- For any $\alpha \neq 1$, the closed butterflies $\mathsf{V}_{\alpha,\beta}$ and $\mathsf{V}_{\alpha,\beta'}$ with $\beta' = \beta^{-1}(1 + \alpha)^{2(2^i+1)}$ are affine-equivalent.

  This equivalence is obtained by composing $\mathsf{V}_{\alpha,\beta}$ with the inverse of the linear permutation

  $$L : (x, y) \mapsto (z_1, z_2) = (\alpha x + y, x + \alpha y) \ .$$

  Indeed,

  $$\begin{aligned} & \mathsf{V}_{\alpha,\beta} \circ L^{-1}(x, y) \\ = \ & \left(z_2^{2^i+1} + \beta\left[(1 + \alpha)^{-2}(z_1 + \alpha z_2)\right]^{2^i+1}, z_1^{2^i+1} + \beta\left[(1 + \alpha)^{-2}(z_2 + \alpha z_1)\right]^{2^i+1}\right) \\ = \ & \left((1 + \alpha)^{-2(2^i+1)}\left[(z_1 + \alpha z_2)^{2^i+1} + \beta' z_2^{2^i+1}\right], (1 + \alpha)^{-2(2^i+1)}\left[(z_2 + \alpha z_1)^{2^i+1} + \beta' z_1^{2^i+1}\right]\right) \ . \end{aligned}$$

3 Useful Results

Several steps of our reasoning require counting the number of solutions of an equation. The following two propositions allow us to predict this number for two simple equations.

The first is a well known result established by Helleseth and Kholosha in 2008.

Proposition 1. *(Theorem 1 in [9]). Let n be odd and i be such that $i < n$ and $\gcd(i,n) = 1$. Let $\mathcal{S}_k$ for any integer k be defined as*

$$\mathcal{S}_k = \{a \neq 0, x^{2^i+1} + x = a \text{ has exactly } k \text{ solutions}\}$$

Then $\mathcal{S}_k$ is empty unless $k \in \{0,1,3\}$ and the non-empty ones have the following sizes:

$$\begin{aligned} |\mathcal{S}_0| &= \frac{2^n+1}{3} \\ |\mathcal{S}_1| &= 2^{n-1}-1 \\ |\mathcal{S}_3| &= \frac{2^{n-1}-1}{3}. \end{aligned}$$

Furthermore, if x is such that $x^{2^i+1} + x + a = 0$ then $x^{2^i+1} + x + a = 0$ has exactly 1 solution if and only if $\mathrm{Tr}\left((1+x^{-1})^\tau\right) = 1$ where $\tau(2^i-1) \equiv 1 \mod (2^n-1)$.

The second proposition is an adaptation of Lemma 4 of [5] to the case where the exponents are 2^i and 2^{2i} rather than 2 and 4 respectively.

Proposition 2. *Let U, V be elements of $\mathbb{F}_{2^n}$ with n odd. The linearised equation in z*

$$Uz^{2^{2i}} + Vz^{2^i} + (U+V)z = C$$

with $\gcd(i,n) = 1$ has

- *0 or 2^n solutions if $U = V = 0$,*
- *0 or 4 solutions if $U \neq 0$, $U \neq V$ and $\mathrm{Tr}\left(\left(1+\frac{V}{U}\right)^\tau\right) = 0$,*
- *0 or 2 solutions otherwise, that is if one of the following is true:*
  - *$U = 0, V \neq 0$,*
  - *$U \neq 0$ and $V = U$,*
  - *$U \neq 0$ and $\mathrm{Tr}\left(\left(1+\frac{V}{U}\right)^\tau\right) = 1$,*

where $\tau(2^i-1) \equiv 1 \mod (2^n-1)$.

Proof. First of all, for any value of the constant C, the number of solutions of the equation is either zero or equal to the number of solutions of the linearised equation $Uz^{2^{2i}} + Vz^{2^i} + (U+V)z = 0$. We then only need to study the case $C = 0$. Obviously, the number of solutions is always even as if z is a solution then $z+1$ is too.

We consider each case separately.

- If $U = V = 0$ then the linearised equation does not involve z, meaning that all values of z satisfy it. We now suppose that either $U \neq 0$ or $V \neq 0$.
- If $U = 0, V \neq 0$ then the equation corresponds to $Vz(z^{2^i-1}+1) = 0$, implying that it has 2 solutions since $\gcd(i,n) = 1$.

- Let us now suppose that $U \neq 0$. In this case, we can rewrite the equation as

$$Uz(z^{2^i-1}+1)\big(1+V/U+(z^{2^i}+z)^{2^i-1}\big)=0.$$

Both $z=0$ and $z=1$ are obviously solutions. In fact, they are the only ones if $V=U$ so that the equation has 0 or 2 solutions in this case. Let us now suppose that $V \neq U$. In this case, the equation $\big(1+V/U+(z^{2^i}+z)^{2^i-1}\big)=0$ can be rewritten as

$$z^{2^i}+z+\left(1+\frac{V}{U}\right)^{\tau}=0.$$

This equation has two solutions when $\mathrm{Tr}\left(\left(1+\frac{V}{U}\right)^{\tau}\right)=0$ while it has no solution when $\mathrm{Tr}\left(\left(1+\frac{V}{U}\right)^{\tau}\right)=1$, meaning that the linearised equation has 2 solutions if $\mathrm{Tr}\left(\left(1+\frac{V}{U}\right)^{\tau}\right)=1$ and 4 otherwise.

□

Finally, an a priori complex trace will appear further in this paper. The following lemma establishes that it is in fact constant.

Lemma 1. *Let n be an odd integer and $i<n$ with $\gcd(i,n)=1$. For any $\alpha,\beta\in\mathbb{F}_{2^n}^*$, we define*

$$\mathcal{B}_{\alpha,\beta} \;=\; (\alpha+\alpha^{2^{i+1}-1})^{2^i-1}\times\frac{\alpha^{2^{i+1}+1}+\alpha^{2^{i+1}-1}+\alpha^{2^i}\beta}{\alpha^{2^{2i+1}+2^i}+\alpha^{2^i}+\alpha^{2^{2i}}\beta^{2^i}}\;.$$

Then, for all $\alpha,\beta\neq 0$, we have that $\mathrm{Tr}\left(\mathcal{B}_{\alpha,\beta}^{\tau}\right)=0$ where $\tau(2^i-1)\equiv 1 \mod (2^n-1)$.

Proof. We note that $\mathcal{B}_{\alpha,\beta}$ is equal to

$$\begin{aligned}
\mathcal{B}_{\alpha,\beta} &= (\alpha+\alpha^{2^{i+1}-1})^{2^i-1}\times\frac{\alpha^{2^{i+1}+1}+\alpha^{2^{i+1}-1}+\alpha^{2^i}\beta}{\alpha^{2^{2i+1}+2^i}+\alpha^{2^i}+\alpha^{2^{2i}}\beta^{2^i}}\\
&= (\alpha+\alpha^{2^{i+1}-1})^{2^i-1}\frac{\alpha^{2^i}\left(\alpha^{2^i+1}+\alpha^{2^i-1}+\beta\right)}{\alpha^{2^{2i}}\left(\alpha^{2^{2i}+2^i}+\alpha^{2^i-2^{2i}}+\beta^{2^i}\right)}\\
&= \left(\frac{\alpha+\alpha^{2^{i+1}-1}}{\alpha^{2^i}}\right)^{2^i-1}\frac{\alpha^{2^i+1}+\alpha^{2^i-1}+\beta}{\left(\alpha^{2^i+1}+\alpha^{1-2^i}+\beta\right)^{2^i}}\\
&= \left(\alpha^{1-2^i}+\alpha^{2^i-1}\right)^{2^i-1}\frac{\alpha^{2^i+1}+\alpha^{2^i-1}+\beta}{\left(\alpha^{2^i+1}+\alpha^{1-2^i}+\beta\right)^{2^i}}\;,
\end{aligned}$$

which we simplify using $\lambda_\alpha=\alpha^{2^i-1}+\alpha^{1-2^i}$ and $Q_\alpha(\beta)=\alpha^{2^i+1}+\alpha^{1-2^i}+\beta$ by writing

$$\mathcal{B}_{\alpha,\beta} \;=\; \lambda_\alpha^{2^i-1}\times\frac{\lambda_\alpha+Q_\alpha(\beta)}{Q_\alpha(\beta)^{2^i}} \;=\; \left(\frac{\lambda_\alpha}{Q_\alpha(\beta)}\right)^{2^i}+\left(\frac{\lambda_\alpha}{Q_\alpha(\beta)}\right)^{2^i-1}\;.$$

The trace of $\left((1+q)^{2^i}+(1+q)^{2^i-1}\right)^{\tau}$ is equal to 0 for any q. Indeed, we have

$$(1+q)^{2^i}+(1+q)^{2^i-1} \;=\; \frac{(1+q)^{2^i+1}+(1+q)^{2^i}}{1+q} \;=\; \frac{q^{2^i+1}+q}{1+q} \;=\; q(q+1)^{2^i-1}\;,$$

from which we deduce that

$$\left((1+q)^{2^i}+(1+q)^{2^i-1}\right)^{\tau} \;=\; q^{\tau}(1+q) \;=\; q^{\tau}+q^{\tau+1}\;.$$

We note that $2^i\tau \equiv \tau + 1 \mod (2^n - 1)$ and deduce that

$$\mathrm{Tr}\left(\left((1+q)^{2^i} + (1+q)^{2^i-1}\right)^{\tau}\right) = \mathrm{Tr}\left(q^{\tau} + q^{2^i\tau}\right) = 0 .$$

As a consequence, since

$$\mathrm{Tr}\left(\mathcal{B}^{\tau}_{\alpha,\beta}\right) = \mathrm{Tr}\left(\left(\left(\frac{\lambda_\alpha}{Q_\alpha(\beta)}\right)^{2^i} + \left(\frac{\lambda_\alpha}{Q_\alpha(\beta)}\right)^{2^i-1}\right)^{\tau}\right) ,$$

we have that $\mathrm{Tr}\left(\mathcal{B}^{\tau}_{\alpha,\beta}\right) = 0$ for any $\alpha, \beta \neq 0$. □

4 Necessary Condition for a Generalized Butterfly to be APN

We first show that, in order for a generalized butterfly to be APN, it is necessary that β takes some very specific values.

Proposition 3 (Condition on β)**.** *Let $n > 1$ be an odd integer, (α, β) be a pair of nonzero elements in $\mathbb{F}_{2^n}$ and $i > 0$ be an integer such that $\gcd(i, n) = 1$. If the generalised butterfly with parameters α, β and exponent $2^i + 1$ is APN then*

$$\beta \in \left\{(\alpha^{2^i-1} + \alpha^{2^i+1}), (\alpha^{-2^i+1} + \alpha^{2^i+1})\right\} .$$

Proof. In order to bound the differential uniformity of $\mathsf{V}_{\alpha,\beta}$, we must bound the number of solutions (x, y) of the following system:

$$\begin{cases} R(x,y) + R(x+a, y+b) = c \\ R(y,x) + R(y+b, x+a) = d \end{cases}$$

for any tuple (a, b, c, d) of $\mathbb{F}_{2^n}$ with $(a, b) \neq (0, 0)$ and where $R(x, y) = (x + \alpha y)^{2^i+1} + \beta y^{2^i+1}$.

In order to derive the necessary condition on β given by this proposition, we simply need to consider the case $b = 0$. In this case, the system becomes

$$\begin{cases} R(x,y) + R(x+a, y) = c \\ R(y,x) + R(y, x+a) = d \end{cases}$$

where

$$R(x,y) + R(x+a,y) = (x+\alpha y)a^{2^i} + (x+\alpha y)^{2^i}a + a^{2^i+1}$$

and

$$R(y,x) + R(y,x+a) = (\alpha a)^{2^i}(y+\alpha x) + (\alpha a)(y+\alpha x)^{2^i} + (\alpha a)^{2^i+1} + \beta\left(a^{2^i}x + ax^{2^i} + a^{2^i+1}\right)$$

so that the original system can be re-written into

$$\begin{cases} ax^{2^i} + a^{2^i}x + \alpha^{2^i}ay^{2^i} + \alpha a^{2^i}y = c' \\ (\alpha^{2^i+1}a + a\beta)x^{2^i} + (\alpha^{2^i+1}a^{2^i} + a^{2^i}\beta)x + \alpha a y^{2^i} + \alpha^{2^i}a^{2^i}y = d' . \end{cases} \tag{1}$$

By summing the first equation and the second one multiplied by α^{2^i-1}, we get that

$$ya^{2^i}(\alpha + \alpha^{2^{i+1}-1}) = (\alpha^{2^{i+1}}a + a + \alpha^{2^i-1}a\beta)(x^{2^i} + a^{2^i-1}x) + g$$

for some constant g. If $\alpha = 1$ then the corresponding open butterfly is functionally equivalent to a 3-round Feistel network (see [5]). Thus, we can use the results of [12] to deduce that the

differential uniformity in this case is at least equal to 4 and thus that the corresponding butterflies are not APN.

We thus assume that $\alpha \neq 1$. In this case, we replace y by its value

$$y = \frac{(1+\alpha^{2^{i+1}}+\alpha^{2^i-1}\beta)}{a^{2^i-1}(\alpha+\alpha^{2^{i+1}-1})}(x^{2^i}+a^{2^i-1}x)+g'$$

in the first equation of System (1). We get

$$\alpha^{2^i}a\mu^{2^i}x^{2^{2i}} + \left[a+\alpha^{2^i}a^{2^{2i}-2^i+1}\mu^{2^i}+\alpha a^{2^i}\mu\right]x^{2^i} + \left[a^{2^i}+\alpha a^{2^{i+1}-1}\mu\right]x = c'' \ ,$$

where

$$\mu = \frac{(1+\alpha^{2^{i+1}}+\alpha^{2^i-1}\beta)}{a^{2^i-1}(\alpha+\alpha^{2^{i+1}-1})} \ .$$

Using the substitution $x = ax'$, we obtain that

$$Ux'^{2^{2i}} + Vx'^{2^i} + (U+V)x' = c'' \tag{2}$$

with

$$U = \alpha^{2^i}a^{2^{2i}+1}\mu^{2^i} \text{ and } V = a^{2^i+1}+\alpha^{2^i}a^{2^{2i}+1}\mu^{2^i}+\alpha a^{2^{i+1}}\mu \ .$$

Using Proposition 2, this equation has at most four solutions x_i, and each x_i leads to a single y, implying that the whole system has at most four solutions.

We now show that the whole system has 4 solutions for some $a \neq 0$ except for two specific values of β. Recall that we exclude the case $\alpha = 1$. If $\mathsf{V}_{\alpha,\beta}$ is APN, then Equation (2) must have at most two solutions for any $a \neq 0$ and any c''. We derive from Proposition 2 that this happens if and only if, for all $a \neq 0$,

$$U = 0 \text{ and } V \neq 0$$

or

$$U = V \text{ and } U \neq 0$$

or

$$U \neq 0 \text{ and } \mathrm{Tr}\left(\left(1+\frac{V}{U}\right)^{\tau}\right) = 1 \ .$$

We first observe that $V \neq 0$, otherwise

$$\alpha^{2^i}a^{2^{2i}-2^i}\mu^{2^i} + \alpha a^{2^i-1}\mu + 1 = 0$$

which would mean that $(\alpha a^{2^i-1}\mu)$ is a root of X^2+X+1 while this polynomial is irreducible over $\mathbb{F}_{2^n}$, n odd. Then, the first condition means that

$$\mu = \frac{(1+\alpha^{2^{i+1}}+\alpha^{2^i-1}\beta)}{a^{2^i-1}(\alpha+\alpha^{2^{i+1}-1})} = 0 \ ,$$

or equivalently

$$\beta = \alpha^{-2^i+1}+\alpha^{2^i+1} \ .$$

The second condition corresponds to

$$\alpha a^{2^i-1}\mu = 1 \Leftrightarrow 1+\alpha^{2^{i+1}}+\alpha^{2^i-1}\beta = 1+\alpha^{2^{i+1}-2} \ ,$$

which is equivalent to

$$\beta = \alpha^{2^i-1}+\alpha^{2^i+1} \ .$$

The last condition corresponds to

$$1 = \mathrm{Tr}\left((1+\frac{V}{U})^{\tau}\right) = \mathrm{Tr}\left(\left(\frac{a^{2^i+1}+\alpha a^{2^{i+1}}\mu}{\alpha^{2^i}a^{2^{2i}+1}\mu^{2^i}}\right)^{\tau}\right)$$

We simplify the fraction on the right-hand side as follows:

$$\begin{aligned}\frac{a^{2^i+1}+\alpha a^{2^{i+1}}\mu}{\alpha^{2^i}a^{2^{2i}+1}\mu^{2^i}} &= \frac{1+a^{2^i-1}\alpha\mu}{a^{2^{2i}-2^i}\alpha^{2^i}\mu^{2^i}} \\ &= \frac{\frac{\alpha^{2^{i+1}+1}+\alpha^{2^{i+1}-1}+\alpha^{2^i}\beta}{\alpha+\alpha^{2^{i+1}-1}}}{(\frac{\alpha+\alpha^{2^{i+1}+1}+\alpha^{2^i}\beta}{\alpha+\alpha^{2^{i+1}-1}})^{2^i}} \\ &= \mathcal{B}_{\alpha,\beta}\ ,\end{aligned}$$

where

$$\begin{aligned}\mathcal{B}_{\alpha,\beta} &= \frac{\alpha^{2^{i+1}+1}+\alpha^{2^{i+1}-1}+\alpha^{2^i}\beta}{\alpha+\alpha^{2^{i+1}-1}}\left(\frac{\alpha+\alpha^{2^{i+1}-1}}{\alpha+\alpha^{2^{i+1}+1}+\alpha^{2^i}\beta}\right)^{2^i} \\ &= (\alpha+\alpha^{2^{i+1}-1})^{2^i-1}\times\frac{\alpha^{2^{i+1}+1}+\alpha^{2^{i+1}-1}+\alpha^{2^i}\beta}{(\alpha+\alpha^{2^{i+1}+1}+\alpha^{2^i}\beta)^{2^i}} \\ &= (\alpha+\alpha^{2^{i+1}-1})^{2^i-1}\times\frac{\alpha^{2^{i+1}+1}+\alpha^{2^{i+1}-1}+\alpha^{2^i}\beta}{\alpha^{2^{2i+1}+2^i}+\alpha^{2^i}+\alpha^{2^{2i}}\beta^{2^i}}\ .\end{aligned}$$

We have established in Lemma 1 that $\mathrm{Tr}(\mathcal{B}^{\tau}_{\alpha,\beta})$ is always equal to 0, implying that

$$\mathrm{Tr}\left((1+\frac{V}{U})^{\tau}\right) = 0\ .$$

Therefore, if $\mathsf{V}_{\alpha,\beta}$ is APN then $\beta = \alpha^{-2^i+1}+\alpha^{2^i+1}$ or $\beta = \alpha^{2^i-1}+\alpha^{2^i+1}$. □

We then show that, for the two particular values of β that we consider, the corresponding butterfly is APN if and only if a specific trace is constant on $\mathbb{F}_{2^n}$ except on 3 particular values.

Proposition 4 (Trace Condition)**.** *Let $\alpha \neq 0, 1$. A generalised butterfly with parameters α and β is APN if and only if:*

$$\beta \in \{\alpha^{2^i-1}+\alpha^{2^i+1}, \alpha^{-2^i+1}+\alpha^{2^i+1}\} \text{ and } \mathrm{Tr}\left(\mathcal{A}_{\alpha}(e)^{\tau}\right) = 1,\ \forall\ e \notin \{0, \alpha, 1/\alpha\}\ ,$$

where

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

Proof. Since we have proved in Section 2.2 that generalised butterflies with parameters (α, β_0) and (α, β_1) where $\beta_1 = \beta_0^{-1}(1+\alpha)^{2(2^i+1)}$ are affine-equivalent, we only need to prove the result for $\beta = \alpha^{2^i-1}+\alpha^{2^i+1}$.

As before, we need to count the number of solutions of

$$\begin{cases} R(x,y)+R(x+a,y+b) = c \\ R(y,x)+R(y+b,x+a) = d \end{cases} \tag{3}$$

for any tuple (a,b,c,d) of $\mathbb{F}_{2^n}$ with $(a,b)\neq(0,0)$. We develop each line of this system and obtain

$$\begin{cases}(a+b\alpha)x^{2^i}+(a+b\alpha)^{2^i}x+(\alpha^{2^i}a+\alpha^{2^i-1}b)y^{2^i}+(\alpha a^{2^i}+\alpha^{2^i-1}b^{2^i})y=c_0\\(\alpha^{2^i}b+\alpha^{2^i-1}a)x^{2^i}+(\alpha b^{2^i}+\alpha^{2^i-1}a^{2^i})x+(\alpha a+b)y^{2^i}+(\alpha a+b)^{2^i}y=d_0\ .\end{cases}$$

As $\alpha\neq 1$, we can replace the lines ℓ_1 and ℓ_2 of this system by $\ell_1+\alpha^{2^i-1}\ell_2$ and $\alpha^{2^i-1}\ell_1+\ell_2$ to obtain a system with the exact same number of solutions. We obtain

$$\begin{cases}(a+\alpha b)(1+\alpha^{2^{i+1}-2})x^{2^i}+a^{2^i}(1+\alpha^{2^{i+1}-2})x+a^{2^i}\alpha(1+\alpha^{2^{i+1}-2})y=c_1\\(\alpha a+b)(1+\alpha^{2^{i+1}-2})y^{2^i}+b^{2^i}(1+\alpha^{2^{i+1}-2})y+b^{2^i}\alpha(1+\alpha^{2^{i+1}-2})x=d_1\ ,\end{cases}$$

i.e.,

$$\begin{cases}(a+\alpha b)x^{2^i}+a^{2^i}x+a^{2^i}\alpha y=c_2\\(\alpha a+b)y^{2^i}+b^{2^i}y+b^{2^i}\alpha x=d_2\ ,\end{cases}$$

which can be rewritten as

$$\begin{cases}(ax^{2^i}+a^{2^i}x)+\alpha(bx^{2^i}+a^{2^i}y)=c_2\\(by^{2^i}+b^{2^i}y)+\alpha(ay^{2^i}+b^{2^i}x)=d_2\ .\end{cases}\tag{4}$$

We first consider the cases $a=0$ and $b=0$. Recall that $a=b=0$ is excluded. If $a=0$, then the first line of the system is equivalent to

$$x=\left(\frac{c_2}{\alpha b}\right)^{2^{n-i}}\ .$$

Replacing x by this value in the second line of System (4) yields an equation in y with nonzero coefficients of the form $by^{2^i}+b^{2^i}y=c_3$. Since $\gcd(i,n)=1$, this equation has at most two solutions, implying that (4) has at most two solutions (x,y). The case $b=0$ is similar.

We now suppose $a\neq 0$ and $b\neq 0$, which allows us to set $x=ax'$ and $y=by'$. In this context, System (4) has as many solutions as

$$\begin{cases}a^{2^i+1}(x'^{2^i}+x')+\alpha a^{2^i}b(x'^{2^i}+y')=c_2\\b^{2^i+1}(y'^{2^i}+y')+\alpha ab^{2^i}(y'^{2^i}+x')=d_2\ ,\end{cases}$$

which we rewrite using $e=a/b$ as

$$\begin{cases}e(x'^{2^i}+x')+\alpha(x'^{2^i}+y')=c_3\\e^{-1}(y'^{2^i}+y')+\alpha(y'^{2^i}+x')=d_3\ .\end{cases}\tag{5}$$

Summing its lines yields

$$(x'^{2^i}+x')(e+\alpha)+(y'^{2^i}+y')(e^{-1}+\alpha)\ =\ c_3+d_3\ .$$

If $e=\alpha$, then y' is fixed to either y'_0 or y'_1 with $y'_0+y'_1=1$. The first line of the system implies in this case that $x'=y'_i+c_3/\alpha$ as the terms in x^{2^i} cancel each other, meaning that the system has at most two solutions. The case $e=\alpha^{-1}$ is similar. We now suppose $e\neq\alpha,\alpha^{-1}$.

The first line of System (5) allows us to express y' as a function of x':

$$y'=\left(\frac{e}{\alpha}+1\right)x'^{2^i}+\frac{e}{\alpha}x'+\frac{c_3}{\alpha}\ .$$

We replace y' by this expression in the second line of (5) and obtain

$$
\begin{aligned}
& \left(e^{-1}+\alpha\right) y'^{2^i} + e^{-1}y' + \alpha x' \\
= \; & \left(e^{-1}+\alpha\right)\left(\left(\frac{e}{\alpha}+1\right)x'^{2^i} + \frac{e}{\alpha}x' + \frac{c_3}{\alpha}\right)^{2^i} + e^{-1}\left(\left(\frac{e}{\alpha}+1\right)x'^{2^i} + \frac{e}{\alpha}x' + \frac{c_3}{\alpha}\right) + \alpha x' \\
= \; & \left(e^{-1}+\alpha\right)\left(\frac{e}{\alpha}+1\right)^{2^i} x'^{2^{2i}} + \left(\left(e^{-1}+\alpha\right)\frac{e^{2^i}}{\alpha^{2^i}} + e^{-1}\left(\frac{e}{\alpha}+1\right)\right)x'^{2^i} + \left(\frac{1}{\alpha}+\alpha\right)x' \\
= \; & d_3 \ ,
\end{aligned}
$$

for some constant d_3. If we let $U = (1+e/\alpha)^{2^i}(\alpha+1/e)$ and $V = U + 1/\alpha + \alpha$, then the number of solutions of this equation can be computed using Proposition 2. First, $U \neq 0$ and $U+V \neq 0$ as $\alpha \neq 1$. Therefore, the possible number of solutions is at most equal to 4 and is given by the trace of $(1+V/U)^\tau$: if $\mathrm{Tr}\left(\left(1+\frac{V}{U}\right)^\tau\right) = 1$ then the equation has at most 2 solutions, otherwise it has 0 or 4 solutions. It holds that

$$
\begin{aligned}
1 + \frac{V}{U} &= \frac{\alpha^{-1}+\alpha}{(e^{-1}+\alpha)(1+e\alpha^{-1})^{2^i}} \\
&= \alpha^{2^i-1}\frac{e(1+\alpha)^2}{(1+\alpha e)(\alpha+e)^{2^i}}
\end{aligned}
$$

so the function is APN if and only if

$$
\mathrm{Tr}\left(\mathcal{A}_\alpha(e)^\tau\right) = 1, \ \forall e \neq 0, \alpha, 1/\alpha, \ \text{with } \mathcal{A}_\alpha(e) = \alpha^{2^i-1} \times \frac{e(1+\alpha)^2}{(1+\alpha e)(\alpha+e)^{2^i}} \ .
$$

□

The trace condition provided by Proposition 4 is sufficient to describe all APN generalised butterflies but it can be greatly simplified. This is stated in the following proposition which presents the *refined trace condition.*

Proposition 5 (Refined Trace Condition)**.** *Let $\alpha \in \mathbb{F}_{2^n} \setminus \{0,1\}$, with n odd. The generalised butterfly with parameters α and $\beta = \alpha^{2^i-1} + \alpha^{2^i+1}$ is APN if and only if:*

$$
\mathrm{Tr}(F_D(t)^\tau) = 1, \ \forall t \notin \{0,1,D\} \ \textit{where} \ \ F_D(t) = \frac{t + t^{2^i+1}}{t+D} \ ,
$$

and $D = 1/(1+\alpha^2)$.

Proof. Based on Proposition 4, we only have to prove that the number of $e \notin \{0, \alpha, 1/\alpha\}$ such that $\mathrm{Tr}(\mathcal{A}_{\alpha,i}(e)^\tau) = 1$ is equal to the number of $t \notin \{0,1,D\}$ such that $\mathrm{Tr}(F_D(t)^\tau) = 1$. Using that $2^i\tau \equiv 1+\tau \mod (2^n-1)$, the term $\mathcal{A}_{\alpha,i}(e)^\tau$ can be re-written as follows

$$
\begin{aligned}
\mathcal{A}_{\alpha,i}(e)^\tau &= \left(\alpha^{2^i-1}\frac{e(1+\alpha)^2}{(1+\alpha e)(\alpha+e)^{2^i}}\right)^\tau \\
&= \alpha\frac{e^\tau(1+\alpha)^{2\tau}}{(1+\alpha e)^\tau(\alpha+e)^{2^i\tau}} \\
&= \alpha\frac{e^\tau(1+\alpha)^{2\tau}}{(1+\alpha e)^\tau(\alpha+e)^{\tau+1}} \\
&= \frac{\alpha}{\alpha+e}\left(\frac{e(1+\alpha)^2}{(1+\alpha e)(\alpha+e)}\right)^\tau \ .
\end{aligned}
$$

We further simplify this expression by reusing the change of variable introduced in [5], namely

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

which implies in particular that, for $\gamma_0 = \alpha + \alpha^3$ and $\gamma_1 = \alpha^{-1} + \alpha^3$:

- $e \notin \{0, \alpha, 1/\alpha\}$ is equivalent to $\ell \notin \{\gamma_0, 0, \gamma_1\}$,
- $e(1+\alpha)^2 = \ell + \gamma_0$, and
- $(1+\alpha e)(1+\alpha)^2 = \alpha(\ell + \gamma_1)$.

We deduce:

$$\begin{aligned}
\mathcal{A}_{\alpha,i}(e)^\tau &= \alpha \left(\frac{e(1+\alpha)^2}{(1+\alpha e)(1+\alpha^2)(\alpha+e)(1+\alpha^2) \;/\; (1+\alpha)^4} \right)^\tau \frac{1}{\alpha+e} \\
&= \alpha \left(\frac{\ell+\gamma_0}{\alpha(\ell+\gamma_1)\;\ell}(1+\alpha^4) \right)^\tau \frac{1+\alpha^2}{\ell} \\
&= \gamma_0 \left(\frac{\gamma_1(\ell+\gamma_0)}{(\ell+\gamma_1)\ell} \right)^\tau \frac{1}{\ell} \,.
\end{aligned}$$

As a sanity check, if we let $\tau = 1$, we can see that we obtain

$$\mathcal{A}_{\alpha,i}(e) = \frac{\gamma_0\gamma_1}{\ell^2} \times \frac{\ell+\gamma_0}{\ell+\gamma_1}$$

which is exactly the equation Canteaut et al. derived on page 7585 of [5].

We further let $\gamma_1/v = \ell$ and note that $\gamma_0/\gamma_1 = (1+\alpha^{-2})^{-1} = C$. As a consequence, the condition $\ell \notin \{\gamma_0, 0, \gamma_1\}$ becomes $v \notin \{1/C, 0, 1\}$ and we can write:

$$\begin{aligned}
\mathcal{A}_{\alpha,i}(e)^\tau &= \gamma_0 \left(\frac{\gamma_1^2 v^{-1} + \gamma_0\gamma_1}{(\gamma_1 v^{-1} + \gamma_1)\gamma_1 v^{-1}} \right)^\tau v/\gamma_1 \\
&= \gamma_0/\gamma_1 \left(\frac{v^{-1} + \gamma_0/\gamma_1}{(v^{-1}+1)v^{-1}} \right)^\tau v \\
&= C \left(\frac{v^{-1} + C}{(v^{-1}+1)v^{-1}} \right)^\tau v \\
&= C \left(\frac{v + Cv^2}{1+v} \right)^\tau v \\
&= C \left(\frac{v + Cv^2}{1+v} v^{2^i-1} \right)^\tau \\
&= C \left(\frac{v^{2^i} + Cv^{2^i+1}}{1+v} \right)^\tau \,.
\end{aligned}$$

We now let $v = (t+1)/C$, so that $v \notin \{1/C, 0, 1\}$ becomes $t \notin \{0, 1, D\}$ where $D = 1 + C = 1 + 1/(1+\alpha^{-2}) = 1/(1+\alpha^2)$. Thus, we can write:

$$\begin{aligned}
v^{2^i} + Cv^{2^i+1} &= (t+1)^{2^i} C^{-2^i} + C(t+1)^{2^i+1} C^{-2^i-1} \\
&= C^{-2^i}(t^{2^i} + 1 + t^{2^i+1} + t^{2^i} + t + 1) \\
&= C^{-2^i}(t^{2^i+1} + t)
\end{aligned}$$

and $v+1 = C^{-1}(t+1+C)$. The expression then becomes

$$\mathcal{A}_{\alpha,i}(e)^\tau = C\left(\frac{C^{-2^i}(t+t^{2^i+1})}{C^{-1}(t+1+C)}\right)^\tau = \left(\frac{t+t^{2^i+1}}{t+D}\right)^\tau = F_D(t)^\tau \ ,$$

so we can conclude that the number of $e \notin \{0, \alpha, 1/\alpha\}$ such that $\mathrm{Tr}\left(\mathcal{A}_{\alpha,i}(e)^\tau\right) = 1$ is equal to the number of $t \notin \{0, 1, D\}$ such that $\mathrm{Tr}\left(F_D(t)^\tau\right) = 1$. □

5 The Necessary Condition Needs a Small Branch Size

In what follows, we prove the last step of our reasoning: if a butterfly is APN then $n \leq 3$. This statement is given by the following proposition that we prove below.

Proposition 6. *If the refined trace condition of Proposition 5 holds then $n \leq 3$.*

Proof. Suppose that the trace condition holds for some D, i and α. Then we have

$$\mathrm{Tr}\left(F_D(x)^\tau\right) = 1, \forall x \notin \{0, 1, D\}$$

with $F_D(x) = (x^{2^i+1} + x)/(x + D)$ and $D = 1/(1 + \alpha^2)$. Let $\mathrm{Im}(F_D)$ be defined by

$$\mathrm{Im}(F_D) = \left\{c \in \mathbb{F}_{2^n}, \exists x \in \mathbb{F}_{2^n}\backslash\{0, 1, D\}, F_D(x) = c\right\} \ .$$

Since F_D is a well-defined function, we have

$$\bigcup_{c\in\mathrm{Im}(F_D)} \left\{x \in \mathbb{F}_{2^n}\backslash\{0, 1, D\}, F_D(x) = c\right\} \ = \ \mathbb{F}_{2^n}\backslash\{0, 1, D\}$$

so that

$$\sum_{c\in\mathrm{Im}(F_D)} \left|\left\{x \in \mathbb{F}_{2^n}\backslash\{0, 1, D\}, F_D(x) = c\right\}\right| = 2^n - 3 \ .$$

As $F_D(0) = F_D(1) = 0$ and since these are the only two preimages of 0 under F_D, we have that $0 \notin \mathrm{Im}(F_D)$ when the input varies in $\mathbb{F}_{2^n}\backslash\{0, 1, D\}$ and we can therefore simplify this expression into

$$\sum_{c\in\mathrm{Im}(F_D)^*} \left|\left\{x \in \mathbb{F}_{2^n}\backslash\{D\}, F_D(x) = c\right\}\right| = 2^n - 3 \ . \tag{6}$$

Let us rewrite this sum using another expression of c.
Suppose that $c = F_D(x)$ for some $x \notin \{0, 1, D\}$. Then $x^{2^i+1} + x = c(x + D)$, or, equivalently,

$$x^{2^i+1} + x(c + 1) + Dc = 0 \ .$$

If $\mathbf{c = 1}$. In this case, the system is equivalent to $x^{2^i+1} + D = 0$. Thus, 1 has exactly one preimage in $\mathbb{F}_{2^n}\backslash\{0, 1, D\}$.

If $\mathbf{c \neq 1}$. We then have that $c = F_D(x)$ if and only if $x^{2^i+1} + (c+1)x + cD = 0$. Substituting x with D yields $D^{2^i} = 1$, which is impossible as this is equivalent to $\alpha = 0$. Hence, the condition $F_D(x) = c$ already implies $x \neq D$. Using $x = u(1 + c)^{2^{n-i}}$, we rewrite this equation into

$$u^{2^i+1}(1 + c)^{2^{n-i}(2^i+1)} + u(1 + c)^{2^{n-i}+1} + Dc = 0$$

which, after a division by $(1+c)^{2^{n-i}+1}$, is seen to be equivalent to

$$u^{2^i+1} + u + g_D(c) = 0 \ , \quad \text{where} \quad g_D(c) = \frac{cD}{(1+c)^{2^{n-i}+1}} \ .$$

We deduce that

$$\left|\left\{x \in \mathbb{F}_{2^n} \backslash \{0,1,D\}, F_D(x) = c\right\}\right| \ = \ \left|\left\{u \in \mathbb{F}_{2^n}, u^{2^i+1} + u + g_D(c) = 0\right\}\right|$$

when $c \neq 1$.

As a consequence, we can rewrite Equation (6) as

$$2^n - 3 \ = \ \left|\left\{u \in \mathbb{F}_{2^n}, u^{2^i+1} + u + g_D(1) = 0\right\}\right| + \sum_{c \in \mathrm{Im}(F_D)\backslash\{0,1\}} \left|\left\{u \in \mathbb{F}_{2^n}, u^{2^i+1} + u + g_D(c) = 0\right\}\right|$$

which is equivalent to

$$2^n - 4 \ = \ \sum_{c \in \mathrm{Im}(F_D)\backslash\{0,1\}} \left|\left\{u \in \mathbb{F}_{2^n}, u^{2^i+1} + u + g_D(c) = 0\right\}\right| \ . \tag{7}$$

Because of Proposition 1, we have that $u^{2^i+1} + u + g_D(c) = 0$ has exactly 1 or 3 solutions. Indeed, it cannot have 0 solution since it is equivalent to $F_D\left(u(1+c)^{2^{n-i}}\right) = c$ which, by definition of c, has at least one solution. Thus, $g_D(c) \in \mathcal{S}_1 \cup \mathcal{S}_3$, where $\mathcal{S}_1$ and $\mathcal{S}_3$ are defined as in Proposition 1.

Let T be the set defined as

$$T = \left\{g_D(c), c \in \mathrm{Im}(F_D)\backslash\{0,1\}\right\} \ .$$

Then (7) can be re-written as

$$2^n - 4 \ = \ \left|T \cap \mathcal{S}_1\right| + 3 \times \left|T \cap \mathcal{S}_3\right| \ . \tag{8}$$

Let us now show that $|T| = |\mathrm{Im}(F_D)\backslash\{0,1\}|$. Let $a' = \frac{c}{(c+1)^{2^{n-i}+1}}$ and let us investigate the number of $c \in \mathrm{Im}_{F_D}$ that correspond to the same a'. Note that

$$\frac{c}{(c+1)^{2^{n-i}+1}} = \frac{1}{(c+1)^{2^{n-i}+1}} + \frac{1}{(c+1)^{2^{n-i}}} \ ,$$

and, by the substitution $b = \frac{1}{(c+1)^{2^{n-i}}}$, we get

$$b^{2^i+1} + b + a' = 0 \ .$$

In order to figure out the number of b corresponding to a given a', we will apply Proposition 1. To this end, we compute the following trace:

$$\begin{aligned}
& \mathrm{Tr}\left((1+b^{-1})^\tau\right) \\
= \ & \mathrm{Tr}\left(\left(1+(c+1)^{2^{n-i}}\right)^\tau\right) \\
= \ & \mathrm{Tr}\left(\left(1+\left(\frac{x^{2^i+1}+D}{x+D}\right)^{2^{n-i}}\right)^\tau\right) \\
= \ & \mathrm{Tr}\left(\left(\frac{x^{2^{n-i}+1}+x^{2^{n-i}}}{x^{2^{n-i}}+D^{2^{n-i}}}\right)^\tau\right) \\
= \ & \mathrm{Tr}\left(\left(\frac{x^{2^{n-i}+1}+x^{2^{n-i}}}{x^{2^{n-i}}+D^{2^{n-i}}}\right)^{2^i\tau}\right) \\
= \ & \mathrm{Tr}\left(\left(\frac{x^{2^i+1}+x}{x+D}\right)^\tau\right) \\
= \ & \mathrm{Tr}(F_D(x)^\tau) \ .
\end{aligned}$$

This trace has to be equal to 1 under our assumption that the refined trace condition holds. Thus, using Proposition 1, we deduce that any given $a' = \frac{c}{(c+1)^{2^{n-i}+1}}$ corresponds to a unique $b = \frac{1}{(c+1)^{2^{n-i}}}$ and, therefore, that $|T| = |\mathrm{Im}(F_D)\backslash\{0,1\}|$.

We define

$$i_1 = \left|T \cap \mathcal{S}_1\right| \quad \text{and} \quad i_3 = \left|T \cap \mathcal{S}_3\right| .$$

From (8), we know that $2^n - 4 = i_1 + 3i_3$. The values of i_1 and i_3 are upperbounded by the sizes of $\mathcal{S}_1$ and $\mathcal{S}_3$ respectively which are given by Proposition 1: $i_1 \leq 2^{n-1} - 1$ and $i_3 \leq (2^{n-1} - 1)/3$. Furthermore, $i_1 + i_3 = |T| = |\mathrm{Im}(F_D)\backslash\{0,1\}|$ and, since we have assumed that the trace of $F_D(x)^\tau$ is constant and equal to 1, the size of the image of F_D is upperbounded by 2^{n-1}, which we decrement because we remove 1 from $\mathrm{Im}(F_D)$. We deduce that

$$\begin{aligned} i_1 &\leq 2^{n-1} - 1 \\ i_3 &\leq (2^{n-1} - 1)/3 \\ i_1 + i_3 &\leq 2^{n-1} - 1 \\ i_1 + 3i_3 &= 2^n - 4 \ . \end{aligned}$$

It holds that $i_1 + 3i_3 = (i_1 + i_3) + 2i_3$ which we can upperbound by $2^{n-1} - 1 + 2(2^{n-1} - 1)/3$, a quantity equal to

$$\begin{aligned} 2^{n-1} - 1 + \frac{2(2^{n-1} - 1)}{3} &= \frac{3(2^{n-1} - 1) + 2(2^{n-1} - 1)}{3} \\ &= \frac{6 \times 2^{n-1} - 2^{n-1} - 5}{3} \\ &= 2^n - \frac{2^{n-1} + 5}{3} \ . \end{aligned}$$

As a consequence, if $(2^{n-1} + 5)/3 > 4$ then we have a contradiction because $i_1 + 3i_3$ would then be both equal to $2^n - 4$ and strictly smaller than $2^n - 4$. This inequality can be re-written as follows:

$$(2^{n-1} + 5)/3 > 4 \ \Leftrightarrow \ 2^{n-1} > 7 \ .$$

Thus, if the refined trace conditions then we have a contradiction whenever $2^{n-1} > 7$ or, equivalently, $n > 3$. We conclude that the refined trace condition implies $n \leq 3$. □

6 Conclusion

Since generalised butterflies defined in [11] have very good differential uniformity and nonlinearity, and, moreover, contain the only known APN permutation, it was natural to hope there would be APN permutations among them. However, we give a negative answer to this question: through a rigorous proof, we confirm that all APN generalised butterflies operate on 6 bits. In other words, all APN generalised butterflies were already known.

Acknowledgements. The work of Léo Perrin was supported by the Fondation Sciences Mathématiques de Paris. The work of Shizhu Tian was supported by the National Science Foundation of China (No. 61772517, 61772516).

References

[1] Thierry P. Berger, Anne Canteaut, Pascale Charpin, and Yann Laigle-Chapuy. On almost perfect nonlinear functions over $\mathbf{F}_2^n$. *IEEE Trans. Inf. Theory*, 52(9):4160–4170, 2006.

[2] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 2–21. Springer, Heidelberg, August 1991.

[3] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.

[4] K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe. An APN permutation in dimension six. In *Finite Fields: Theory and Applications - FQ9*, volume 518 of *Contemporary Mathematics*, pages 33–42. AMS, 2010.

[5] Anne Canteaut, Sébastien Duval, and Léo Perrin. A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}. *IEEE Trans. Inf. Theory*, 63(11):7575–7591, 2017.

[6] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[7] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In Alfredo De Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 356–365. Springer, Heidelberg, May 1995.

[8] Shihui Fu, Xiutao Feng, and Baofeng Wu. Differentially 4-uniform permutations with the best known nonlinearity from butterflies. *IACR Trans. Symm. Cryptol.*, 2017(2):228–249, 2017.

[9] Tor Helleseth and Alexander Kholosha. On the equation $x^{2^l+1} + x + a = 0$ over $GF(2^k)$. *Finite Fields Appl.*, 14(1):159–176, 2008.

[10] Xiang-dong Hou. Affinity of permutations of $\mathbb{F}_{2^n}$. *Discrete Appl. Math.*, 154(2):313–325, 2006.

[11] Yongqiang Li, Shizhu Tian, Yuyin Yu, and Mingsheng Wang. On the generalization of butterfly structure. *IACR Trans. Symm. Cryptol.*, 2018(1):160–179, 2018.

[12] Yongqiang Li and Mingsheng Wang. Constructing S-boxes for lightweight cryptography with Feistel structure. In Lejla Batina and Matthew Robshaw, editors, *CHES 2014*, volume 8731 of *LNCS*, pages 127–146. Springer, Heidelberg, September 2014.

[13] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 386–397. Springer, Heidelberg, May 1994.

[14] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 55–64. Springer, Heidelberg, May 1994.

[15] Kaisa Nyberg and Lars R. Knudsen. Provable security against differential cryptanalysis (rump session). In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 566–574. Springer, Heidelberg, August 1993.

[16] Léo Perrin, Aleksei Udovenko, and Alex Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 93–122. Springer, Heidelberg, August 2016.

[17] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. *Des. Codes and Cryptogr.*, 73(2):587–600, 2014.