Functions 3-to-1 and power APN S-boxes

Deepak Dalai

Functions 3-to-1 and power APN S-boxes

Deepak Kumar Dalai

Project CODES, INRIA,
Rocquencourt, France - 78153.
deepak.dalai@inria.fr

Abstract

Almost Perfect Nonlinear(APN) S-boxes are used in block ciphers to prevent differential attacks. The non-evidence of permutation APN S-box on even number of variables and the efficiency of power functions bring the importance of power APN S-boxes to use in block ciphers. We present a special class of 3-to-1 S-box on even number of variables. The power APN S-boxes on even number of variables fall in this class. We study some other known APN S-boxes on even number of variables whether they fall in this class. Then we present a necessary condition for power functions to be APN. Using this necessary condition we can filter out some non-APN power functions. Specifically, if the number of variables is multiple of small primes, then one can filter many non-APN functions.

Keywords: S-box, Power Function, APN Function, Differential Cryptanalysis.

Applications 3-vers-1 et boites S utilisant une fonction puissance APN

Résumé

Les boites S utilisées dans un système de chiffrement par bloc doivent garantir ce système contre les attaques les plus connues, notamment l'attaque dite *différentielle*. Une boite S s'identifie en fait à une fonction qui doit satisfaire certains critères pour prévenir une attaque différentielle : elle doit être, idéalement, *presque parfaitement non linéaire* (APN). Nous parlerons de *boites S APN*. Lorsque la fonction induite a un nombre pair de variables, elle n'est pas bijective car l'existence de permutation APN en dimension paire reste à déterminer. On choisira donc plutot des fonctions *monômes*, dites *fonctions puissances* et l'on parlera de *boites S monômiales APN*. Dans cet article, nous présentons une classe particulière de fonctions, dites 3-vers-1 (*i.e.,* d'image 1/3) en dimension paire. Cette classe $\mathcal{C}$ couvre les boites S monômiales APN. Nous étudions le cas d'autres fonctions APN, également en dimension paire, dans l'idée de tester leur appartenance à $\mathcal{C}$. Nous proposons une condition nécessaire pour qu'une fonction puissance soit APN, en utilisant la propriété d'appartenance à la classe $\mathcal{C}$. Nous concevons ainsi un filtre qui nous permet de tester si une fonction puissance donnée peut être APN. Notre filtre permet d'éliminer un grand nombre de candidates, en particulier lorsque l'on traite des fonctions à n variables où n est le produit de plusieurs petits nombres premiers.

1 Introduction

We denote by V_m the field $GF(2^m)$ of all m-dimensional binary vectors. A substitution box (in short, S-box) is a mapping $F : V_m \mapsto V_n$, which can be viewed as a multi-output Boolean function. The S-boxes of the form $F : V_m \mapsto V_m$ are used by many block ciphers for the confusion part of the round function. For example, some very popular block ciphers like AES, DES, RC6 etc. use S-boxes. Therefore, most of the cryptanalytic techniques on block ciphers are based on the cryptographic strengths of underlying S-box. Differential cryptanalysis is one of the important techniques to verify the strength of S-box against differential attack [2]. Differential attack can be applied successfully if the number of solutions of $F(x + a) + F(x) = b$ for $a \neq 0, b \in V_m$ are non uniform. Hence, to prevent differential attack the output derivative $F(x+a)+F(x), a \neq 0$ should be uniformly distributed. The S-box satisfies this property is called Almost Perfect Nonlinear (APN) S-box [7].

The randomness criteria demands to use permutation S-boxes in the design of block ciphers. At the same time, the S-boxes on even variable are being preferred in the design of some block ciphers for the reason of easy implementation and hardware friendliness of even variable S-box. Unfortunately, there is no evidence of existence of permutation APN S-box on even number of variables. Further, the power functions are being preferred in design of block ciphers for the reason of fast implementation of S-box. For example, the most popular block cipher AES uses inverse function as underlying S-box. However, the power APN functions on even number of variables are of the form X^{3d}. The S-boxes on even number of variables of the form X^{3d} are 3-to-1 functions (i.e, each nonzero element has either 3 or 0 pre-images and zero maps zero). For an instance, the function X^3 is 3-to-1 function and APN when m is even. Therefore, 3-to-1 functions on even number of variables have an important role in the study of APN S-boxes. In Section 3 we have studied on 3-to-1 APN S-box. We have presented a special type of 3-to-1 functions. Then we present some theoretical and experimental results that some of the known APN S-boxes on even number of variables fall in this special category of 3-to-1 functions.

Since the power functions are being used as underlying S-boxes in many popular block ciphers for its efficiency, the identification of APN power functions is an important topic in the study of design of block ciphers. In Section 4 we present a necessary condition for a power function to be APN. Using the necessary condition we can filter out some non-APN X^d's. Towards the end of the section we have presented some experimental results on the number of non-APN power functions can be filtered out. The necessary condition shows that if m is multiple of small primes, one can filter many power non-APN functions. In the following section we present some preliminary stuffs which are required for our results.

2 Preliminary

In this section we introduce some notations and motivations which are necessary for the main works. In this paper, we always consider the S-boxes are of the form $F : V_m \mapsto V_m$.

The derivative of F with respect to $a \in V_m$ is defined as follows.

Definition 1 *Let $F : V_m \mapsto V_m$ be a S-box. The derivative of F with respect to $a \in V_m$ is the function $D_aF : V_m \mapsto V_m$ is defined as*

$$D_aF(x) = F(x) + F(x + a), \forall x \in V_m.$$

δ is an integer valued function from $V_m \times V_m$ is defined as

$$\delta(a, b) = |\{x \in V_m, D_aF(x) = b\}| \text{ for } a, b \in V_m.$$

Abusing the notation δ, we define

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

$\delta(F)$ needs to be as low as possible to resist differential attacks on block ciphers [7]. Since $D_aF(x) = D_aF(x + a)$ for $a \neq 0 \in V_m$, we have $\delta(F) \geq 2$. The S-boxes for which the equality holds are the best choices against the differential attack.

Definition 2 *An S-box $F : V_m \mapsto V_m$ is called* Almost Perfect Nonlinear *(in short, APN) if $\delta(F) = 2$.*

The following result is easily derived from the above definition.

Lemma 1 *$F : V_m \mapsto V_m$ is APN iff there do not exist different $x, y, z \in V_m$ such that $F(x) + F(y) + F(z) + F(x + y + z) = 0$.*

Now we define a class of functions as following.

Definition 3 *Consider m is even. An S-box $F : V_m \mapsto V_m$ is defined as 3-to-1 S-box if $F^{-1}(0) = \{0\}$ and $|F^{-1}(a)| = 3$ or, 0 for $a \in V_m^* = V_m \setminus \{0\}$.*

Note that, the 3-to-1 S-box is defined for even variable S-boxes. Since $2^m - 1$ is not divisible by 3 when m is odd, the 3-to-1 S-box is not defined for odd variable S-boxes.

The APN property is being preserved by some transformations like Extended Affine (EA) transformation [8] and CCZ transformation [4]. Two S-boxes F and F' are EA-equivalent if there exist two affine permutations A_1, A_2 and an affine function A such that $F' = A_1 \circ F \circ A_2 + A$. CCZ-equivalence corresponds to the affine equivalence of the graphs of two S-boxes [4]. EA-equivalence is a particular case of CCZ-equivalence. In [3] one can find a list of APN functions which are EA-inequivalent and CCZ-inequivalent to power functions. In this paper we will show that some even variable S-boxes of them are 3-to-1 S-box. Hence, it shows that 3-to-1 S-boxes has an important contribution in the class of APN S-boxes.

We denote $e \subseteq d$ for two non-negative integers e and d if $e \wedge d = e$ where $\wedge$ is the bitwise logical AND operation i.e., $e_i \leq d_i, 0 \leq i < n$ where e_i and d_i's are ith bit of the n-bit binary representation of e and d respectively. In this paper we use Lucas' theorem [6, page 79] several times for the proof of some results. From Lucas' theorem, we have $\binom{d}{e} = 1 \bmod 2$ iff $e \subseteq d$ for two non-negative integers d and e.

3 3-to-1 APN S-box

In this section, we present a construction of a class of 3-to-1 APN S-box and show some of the known constructions of S-boxes on even variables are of this type. Note that, in this section we always consider m as even positive integer and $k = \frac{2^m-1}{3}$.

Construction 1 *Let V_m be partitioned into disjoint parts, $P_0 = \{0\}, P_1, P_2, \ldots, P_k$, such that each set P_i, $1 \leq i \leq k$ contains 3 different elements a, b, c where $a+b = c$. Further, let $U \subset V_m$ such that $|U| = k+1$. Then the S-box $F : V_m \mapsto V_m$ is constructed as $F(x) = u_i$ where $x \in P_i$ and u_i is the ith element in U following an ordering.*

Notation 1 *Referring to the partitions P_i in Construction 1, we denote (1) $F(P_i) = \{F(x) : x \in P_i\}$ and (2) for $x \in V_m$, $P(x) = P_i$ where $x \in P_i$.*

In the following proposition, we present a simple case when the functions in the above construction are APN.

Proposition 1 *Referring to the Construction 1, if there is no four elements $w, x, y, z \in U$ such that $w + x + y + z = 0$, then F is APN.*

Proof : To prove it, we have to show that for any $a, b, c, d \in V_m$, $a+b+c+d = 0$ implies $F(a) + F(b) + F(c) + F(d) \neq 0$. If a, b, c, d are from four distinct partitions then from the supposition $F(a) + F(b) + F(c) + F(d) \neq 0$. If at least two elements, say a and b, are from one partition, then $F(a) + F(b) + F(c) + F(d) = F(c) + f(d)$. To be $F(c) + F(d) = 0$, c and d has to be in one partition. c and d can not be in same partition where a and b belong because each partition contains 3 elements or 1 element. If c and d are in another partition then $a + b + c + d = (a + b) + (c + d)$ can not be 0 because $(a + b) \in P(a)$ and $(c + d) \in P(c)$ are two different elements. ∎

If one can choose $k + 1$ elements from V_m of size $2^m = 3k + 1$ such that no four elements from them can add to 0, then it is possible to construct an APN function. The question is whether such type of set exists for some even m ? For $m = 4$ the set $U = \{0, a_1, a_2, a_3, a_4, a_1+a_2+a_3+a_4\}$ where $\{a_1, a_2, a_3, a_4\}$ is a basis of vector space V_4, satisfies the condition. Here we present an example of APN when $m = 4$.

Example 1 *Let denote the m-dimensional vector $(e_0, \ldots, e_{m-1})$ by an integer $\sum_{i=0}^{m-1} e_i 2^i$. The partition of V_4 is as $P_0 = \{0\}, P_1 = \{1, 2, 3\}, P_2 = \{4, 8, 12\}, P_3 = \{5, 10, 15\}, P_4 = \{6, 11, 13\}, P_5 = \{7, 9, 14\}$ and the set $U = \{0, 1, 2, 4, 8, 15\}$. Now, define F as $F(P_0) = 0; F(P_1) = 1; F(P_2) = 2; F(P_3) = 4; F(P_4) = 8; F(P_5) = 15$. Then F is APN.*

Unfortunately, the following theorem tells about the non-existence of such set when $m \geq 6$.

Theorem 1 *For $m \geq 6$ (m even), there does not exist a set $U \subset V_m$ such that $w + x + y + z \neq 0$ for all distinct $w, x, y, z \in U$.*

Proof : We use induction to prove it. For base case, we will show for $m = 6$. Now, we will construct a largest set $W \subset V_6$ such that there is no distinct $w, x, y, z \in W$ such that $w + x + y + z = 0$. Since W is largest, it must contain a basis of V_6. Without loss of generality we consider that W contains the unit basis $e_1 = (0, 0, 0, 0, 0, 1), e_2 = (0, 0, 0, 0, 1, 0), \ldots, e_6 = (1, 0, 0, 0, 0, 0)$ and all zero element (otherwise, one can use an affine transformation get the unit basis and 0). Now we will start with $W = \{0, e_1, \ldots, e_6\}$ and will try to add more to W. It is easy to check that we can not add any vector of weight 2 and 3. Further, it can be checked that the addition of the vector of weight 6 does not allow to add any vector of weight 4 or 5. Then one can not add two or more vectors of weight 5, because addition of two vectors of weight 5 results a vector of weight 2. Finally, one can not add more than 2 vectors of weight 4, since there always exist 2 vectors out of 3 vectors of weight 4 such that their sum results a vector of weight 2. So, one can add at most three more (two of weight 4 and one of weight 5). The size of W will be at most 10, but we need of weight $\frac{2^6-1}{3} = 21$. Therefore, the theorem is true for $m = 6$.

Now we suppose it is true for $m = t$ and we will prove for $m = t + 2$. We prove it by contradiction. Consider such set U of size $\frac{2^{t+2}-1}{3}$ exist for $n = t + 2$. Now divide U into 4 parts U_{00}, U_{01}, U_{10} and U_{11} such that $U_{ij} \subset U$ contains the vectors having $(t + 1)$th and $(t+2)$th co-ordinates are i and j respectively. Hence from pigeonhole principle, there must be a U_{ij} such that $|U_{ij}| \geq \frac{1}{4} \times \frac{2^{t+2}-1}{3} = \frac{2^t - \frac{1}{4}}{3} \geq \frac{2^t-1}{3}$. Now one can use this U_{ij} (excluding $t + 1$ and $t + 2$ th coordinates) for $m = t$, which contradicts our supposition. ∎

Using Lemma 1 over Construction 1, we have the following result to be APN S-box.

Theorem 2 *The constructed S-box F in Construction 1 is APN iff for all $x, y \in V_m$ such that $P(x) \neq P(y)$, $F(x) + F(y) + F(z) + F(x + y + z) \neq 0$ for all $z \in V_m$, $z \notin P(x) \cup P(y) \cup P(x + y)$.*

Proof : For the proof, we use Lemma 1. For this class of S-boxes the search domains of y and z are decreased by putting some extra conditions. Now we will show that the discarded y's and z's will not satisfy the condition $F(x) + F(y) + F(z) + F(x + y + z) = 0$.

Let $y \in P(x)$. Then from the construction of P_i's, we have $x + y \in P(x)$. $F(x) + F(y) + F(z) + F(x + y + z) = 0$ i.e., $F(z) + F(x + y + z) = 0$ implies $x + y + z \in P(z)$ i.e, $x + y \in P(z)$. Which implies $x, y, z, x + y + z \in P(x)$, a contradiction that x, y, z and $x + y + z$ are all distinct. Hence, $F(x) + F(y) + F(z) + F(x + y + z) \neq 0$. The exclusion of z's can be proved in similar way. ∎

Note 1 *In Construction 1, each set $P_i \cup \{0\}$, $0 < i \leq k$, forms a subspace of dimension 2. If P_i would have dimension greater than 2 then for the following reason F can not be APN. Consider P_i such that $P_i \cup \{0\}$ is of dimension greater than 2. Then P_i will contain a subset $\{x, y, x + y, z, x + z, y + z, x + y + z\}$. Here the last 4 elements add to zero. This implies that we can not consider the partitions $P_i, 0 < i \leq k$, such that $P_i \cup \{0\}$ is 3 dimensional.*

In the remaining part of this section we will present theoretical and experimental results on some known APN S-boxes.

1. Power APN functions

The power APN functions on even number of variables are of the form $F(X) = X^{3d}$ where $\gcd(d,k) = 1$ and $k = \frac{2^m-1}{3}$. Let α be a primitive element of V_m. Since m is even, V_2 is a subfield of V_m with $\beta = \alpha^k$ is a generator of $V_2^* = \{1, \beta, \beta^2\}$. Now consider $P_{i+1} = \alpha^i V_2^* = \{\alpha^i, \alpha^i\beta, \alpha^i\beta^2\}$ for $0 \leq i < k$ and $P_0 = \{0\}$. $\{P_i, 0 \leq i \leq k\}$ makes a disjoint partition over V_m and $\alpha^i + \alpha^i\beta + \alpha^i\beta^2 = \alpha^i(1+\beta+\beta^2) = \alpha^i.0 = 0$ for $0 \leq i < k$. Now for the S-box $F(X) = X^{3d}$, $F(P_{i+1}) = \{\alpha^{3di}, \alpha^{3di}\beta^{3d}, \alpha^{3di}\beta^{6d}\} = \alpha^{3di}$ for $0 \leq i < k$. Since $\gcd(d,k) = 1$, $\alpha^{3di} \neq \alpha^{3dj}$ for $0 \leq i < j < k$ i.e., $|F^{-1}(\alpha^{3di})| = 3$. Here $U = \{0\} \bigcup \{\alpha^{3i}, 0 \leq i \leq k-1\}$. Therefore, the APN power functions i.e., $X^{3d}, \gcd(d,k) = 1$ satisfies Construction 1. Hence, the power APN functions follow the restriction imposed on a S-box to be APN in Theorem 2.

2. $F(X) = X^3 + tr(X^9)$

The function $F(X) = X^3 + tr(X^9)$ (where $tr(X) = \sum_{i=0}^{m-1} X^{2^i}$ is the trace function from V_m to V_1) is APN function and when $m \geq 7$ and $m > 2p$ where p is the smallest positive integer such that $m \neq 1, m \neq 3$ and $\gcd(m,p) = 1$, $X^3 + tr(X^9)$ is CCZ-inequivalent to all power functions on V_m [3]. Similar to the power function case (i.e., Item 1), one can easily prove that $F(\alpha^i) = F(\alpha^{i+k}) = F(\alpha^{i+2k})$ for $0 \leq i < k = \frac{2^m-1}{3}$ and $F(0) = 0$ where α is a primitive element in V_m. Let $x = \alpha^i$ and $y = \alpha^j$ where $0 \leq i < j < k$. Now we will show that $F(x) \neq F(y)$ i.e., $x^3 + tr(x^9) \neq y^3 + tr(y^9)$ i.e., $tr(x^9 + y^9) \neq x^3 + y^3$. If $tr(x^9 + y^9) = 0$ then we are done because $x^3 \neq y^3$. Now consider $tr(x^9 + y^9) = 1$. If $x^3 + y^3 = 1$ i.e., $y^3 = 1 + x^3$ then $tr(x^9 + y^9) = tr(x^9 + (1+x^3)^3) = tr(1 + x^3 + x^6) = \sum_{i=0}^{m-1}(1 + x^3 + x^6)^{2^i} = \sum_{i=0}^{m-1}(1 + x^{3.2^i} + x^{6.2^i}) = \sum_{i=0}^{m-1}(1 + x^{3.2^i} + x^{3.2^{i+1}}) = x^3 + x^{3.2^m} = x^3 + x^3 = 0$ which is a contradiction. Therefore $F(x) \neq F(y)$ implies $X^3 + tr(X^9)$ satisfies Consruction 1.

3. $F(X) = X^{2^i+1} + (X^{2^i} + X + tr(1) + 1)tr(X^{2^i+1} + Xtr(1))$

The function $F(X) = X^{2^i+1} + (X^{2^i} + X + tr(1) + 1)tr(X^{2^i+1} + Xtr(1))$ is APN if $m \geq 4$ and $\gcd(i,m) = 1$. $F(X)$ is EA-inequivalent to all power functions. Since $tr(1) = 0$ for even m, we have $F(X) = X^{2^i+1} + (X^{2^i} + X + 1)tr(X^{2^i+1}) = X^{2^i+1} + ((1+X)^{2^i+1} + X^{2^i+1})tr(X^{2^i+1})$. That is, $F(X) = X^{2^i+1}$ when $tr(X^{2^i+1}) = 0$ and $F(X) = (1+X)^{2^i+1}$ when $tr(X^{2^i+1}) = 1$. Since m is even and $\gcd(i,m) = 1$, i is odd. Hence, $2^i + 1$ is multiple of 3. Similar to the power function case (i.e., Item 1), it is easy to prove that prove that $F(\alpha^i) = F(\alpha^{i+k}) = F(\alpha^{i+2k})$ for $0 \leq i < k = \frac{2^m-1}{3}$ and $F(0) = 0$ where α is a primitive element in V_m. Here, $\alpha^i + \alpha^i\beta + \alpha^i\beta^2 = 0$, which satisfy the constraint on P_i in Construction 1. But, experimentally we find that there are $0 \leq i < j < k$ such that $F(\alpha^i) = F(\alpha^j)$ which denies to be 3-to-1.

Those above studies make the 3-to-1 power functions and the functions of type Construction 1 interesting. The study on finding the exact relation of the ordered set U and the partitions P_i which makes F APN will be even more intersting.

4 Power function

In this section we present a necessary condition for a power function, $F : X \mapsto X^d, X \in V_m$, to be APN. Unlike the previous section, in this section we study for general m unless it is specified as even or odd. There is not complete characterization of all APN power functions

but some results on the characterization of APN power functions are available in literature. If a power function F is APN then $\gcd(d, 2^m - 1) = 1$ for odd m and $\gcd(d, 2^m - 1) = 3$ for even m. For another instance, if there is h which divides m and $d = l(2^h - 1) + 2^r$ for some l and r then F is not APN [5, 4]. Therefore, to be an APN S-box, a power function must not have the above property. For more detail one can refer [1]. In this section we have presented another necessary condition for F to be an APN functions. If F is a power function then the Lemma 1 can be simplified as in the following lemma.

Lemma 2 *A power S-box $F : V_m \mapsto V_m$ is APN iff there do not exist different $x \neq 1$ and $y \neq 1$ in V_m such that $1 + S(x) + S(y) + S(1 + x + y) = 0$.*

The proof is simple, since for different $x \neq 0, y, z \in V_m$, $x^d + y^d + z^d + (x + y + z)^d = 1 + (\frac{y}{x})^d + (\frac{z}{x})^d + (1 + \frac{y}{x} + \frac{z}{x})^d$. Now Lemma 2 can be written in terms of primitive elements as following.

Proposition 2 *A power S-box $F : V_m \mapsto V_m$ is APN iff there do not exist*

1. *$0 < i < 2^m - 1$ such that $1 + F(\alpha^i) + F(1 + \alpha^i) \neq 0$ (the case when one of $x, y, 1 + x + y$ is zero), and*

2. *$0 < i < j < 2^m - 1$ such that $1 + F(\alpha^i) + F(\alpha^j) + F(1 + \alpha^i + \alpha^j) \neq 0$ (the case when none of $x, y, 1 + x + y$ is zero),*

where α is a primitive element in V_m.

Therefore, the APN property of a power function (say, X^d) can be checked by solving Conditions 1 and 2 in the Proposition 2 for given m. It will be simpler if Condition 2 can be reduced to Condition 1. Now the question: does Condition 1 imply Condition 2 for some d and m. In the following theorem we find an instance where it is possible.

Lemma 3 *Suppose $wt(d) = 2$. Then $a^d + b^d + c^d + (a + b + c)^d = (a + b)^d + (a + c)^d + (b + c)^d$ for $a, b, c \in V_m$ and any $m > 0$.*

Proof : let $d = 2^p + 2^q$. Then $a^d + b^d + c^d + (a + b + c)^d = a^d + b^d + c^d + \sum_{i=0}^{d} \binom{d}{i} a^i (b + c)^{d-i}$. According to Lucas' theorem, we have $\binom{d}{i} = 1 \bmod 2$ iff $i = 0, 2^p, 2^q$ or d. Hence, $a^d + b^d + c^d + (a + b + c)^d = a^d + b^d + c^d + (a^d + a^{2^p}(b + c)^{2^q} + a^{2^q}(b + c)^{2^p} + (b + c)^d) = a^d + b^d + c^d + a^d + a^{2^p}(b^{2^q} + c^{2^q}) + a^{2^q}(b^{2^p} + c^{2^p}) + (b + c)^d) = a^d + a^{2^p} b^{2^q} + a^{2^q} b^{2^p} + b^d + a^d + a^{2^p} c^{2^q} + a^{2^q} c^{2^p} + c^d + (b + c)^d) = (a + b)^d + (a + c)^d + (b + c)^d$. ∎

Theorem 3 *A quadratic S-box $F : V_m \mapsto V_m$ such that $F(X) = X^d$, where $wt(d) = 2$, is APN iff there does not exit $0 < i < 2^m - 1$ such that $1 + \alpha^{id} + (1 + \alpha^i)^d = 0$ where α is a primitive element in F_{2^m}.*

Proof : Here we reduce the item 2 to item 1 in Definition 2. For $0 < i < j < 2^m - 1$, $1 + \alpha^{id} + \alpha^{jd} + (1 + \alpha^i + \alpha^j)^d \neq 0$
i.e., $(1 + \alpha^i)^d + (1 + \alpha^j)^d + (\alpha^i + \alpha^j)^d \neq 0$ (according to Lemma 3)
i.e., $1 + [(1 + \alpha^i)^{-1}(1 + \alpha^j)]^d + (1 + (1 + \alpha^i)^{-1}(1 + \alpha^j))^d \neq 0$
i.e., $1 + \alpha^{ld} + (1 + \alpha^l)^d \neq 0$ for some $0 < l < 2^m - 1$. ■

Hence a quadratic function $F(X) = X^d$ is APN iff the equation $1+x^d+(1+x)^d = 0$ has no solution in $V_m \setminus \{0, 1\}$. Using Lucas' theorem we have $1 + x^d + (1 + x)^d = x^{2^p} + x^{2^q} = 0$, iff $gcd(2^p - 2^q, 2^m - 1) \neq 1$ where $d = 2^p + 2^q$. Hence X^d is APN iff $gcd(2^p - 2^q, 2^m - 1) = 1$ i.e., $\gcd(p - q, m) = 1$. Certainly, this is not a new result. It has been done by Nyberg in [8]. But the motivation is to find any other situations where Condition 2 can be reduced to Condition 1 which could be solved easily (because Condition 1 is dependent on one variable).

Since the Condition 1 is easier to solve, in the next part we study the S-box X^d using Condition 1 to find some situations when they are not APN. Since X^d is APN iff X^{2d} is APN, we consider d is an odd positive number. We can write every odd positive integer d of the form $(2^{a_0} - 1) + 2^{a_0+b_0}(2^{a_1} - 1) + \ldots + 2^{\sum_{i=0}^{q-2}(a_i+b_i)}(2^{a_{q-1}} - 1) + 2^{\sum_{i=0}^{q-1}(a_i+b_i)}(2^{a_q} - 1)$ where $a_i, 0 \leq i \leq q$ and $b_i, 0 \leq i < q$ are the number of ith contiguous 1's and 0's in the binary representation of d. For example, $(77)_{10} = (1001101)_2$ where $a_0 = 1, b_0 = 1, a_1 = 2, b_1 = 2, a_2 = 1$ and $q = 2$.

Theorem 4 *Let d be of the form $(2^{a_0} - 1) + 2^{a_0+b_0}(2^{a_1} - 1) + \ldots + 2^{\sum_{i=0}^{q-2}(a_i+b_i)}(2^{a_{q-1}} - 1) + 2^{\sum_{i=0}^{q-1}(a_i+b_i)}(2^{a_q} - 1)$. Let denote $l_0 = d$,*
$l_1 = 2^{a_0+b_0}(2^{a_1} - 1) + 2^{a_0+b_0+a_1+b_1}(2^{a_2} - 1) + \ldots + 2^{\sum_{i=0}^{q-1}(a_i+b_i)}(2^{a_q} - 1)$,
$l_j = 2^{a_{j-1}+b_{j-1}}(2^{a_j} - 1) + 2^{a_{j-1}+b_{j-1}+a_j+b_j}(2^{a_{j+1}} - 1) + \ldots + 2^{\sum_{i=j-1}^{q-1}(a_i+b_i)}(2^{a_q} - 1)$
(that is, $l_j = l_{j-1} >> (a_{j-2} + b_{j-2}) - (2^{a_{j-1}} - 1)$, where $(t >> n)$ is bit wise right shift of integer t by n places) for $1 < j \leq q$. If

- *$gcd(l_{i+1} - 1, 2^m - 1) \neq 1$ or, $gcd(a_i, m) \neq 1$ for $0 \leq i < q$.*
- *and $gcd(a_q - 1, m) \neq 1$.*

then $F(X) = X^d$ is not APN.

Proof : Let denote $s_j = \sum_{i=0}^{j}(a_i + b_i), 0 \leq j < q$. Similar to l_j, let denote $k_j, 0 \leq j < q$, as $k_0 = 2^{a_0} - 1$ and $k_j = k_{j-1} + 2^{s_{j-1}}(2^{a_j} - 1)$. Now we open $(1 + x)^d$ using Lucas' theorem.

$$(1+x)^d = \sum_{i:i\subseteq d} x^i = \sum_{i:i\subseteq k_0} x^i + \sum_{i:i\subseteq k_0} x^i \sum_{0\neq i\subseteq 2^{a_1}-1} x^{i2^{s_0}} + \cdots + \sum_{i:i\subseteq k_{q-1}} x^i \sum_{0\neq i\subseteq 2^{a_q}-1} x^{i2^{s_{q-1}}}$$

$$= \sum_{i=0}^{2^{a_0}-1} x^i + \sum_{i:i\subseteq k_0} x^i \sum_{i=1}^{2^{a_1}-1} x^{i2^{s_0}} + \cdots + \sum_{i:i\subseteq k_{q-1}=i} x^i \sum_{i=1}^{2^{a_q}-1} x^{i2^{s_{q-1}}}$$

$$= 1 + \sum_{i=1}^{2^{a_0}-1} x^i + (1+x)^{k_0} \sum_{i=1}^{2^{a_1}-1} (x^{2^{s_0}})^i + \cdots + (1+x)^{k_{q-1}} \sum_{i=1}^{2^{a_q}-1} (x^{2^{s_{q-1}}})^i$$

$$= 1 + \sum_{i=1}^{2^{a_0}-1} x^i + (1+x)^{k_0} \sum_{i=1}^{2^{a_1}-1} (x^{2^{s_0}})^i + \cdots + (1+x)^{k_{q-2}} \sum_{i=1}^{2^{a_{q-1}}-1} (x^{2^{s_{q-2}}})^i$$
$$+(1+x)^{k_{q-1}} \sum_{i=1}^{2^{a_q}-2} (x^{2^{s_{q-1}}})^i + (1+x)^{k_{q-1}} (x^{2^{s_{q-1}}})^{2^{a_q}-1}$$

$$= 1 + x\frac{1+x^{2^{a_0}-1}}{1+x} + (1+x)^{k_0} x^{2^{s_0}} \frac{1+(x^{2^{s_0}})^{2^{a_1}-1}}{1+x^{2^{s_0}}} + \cdots + (1+x)^{k_{q-2}} x^{2^{s_{q-2}}} \frac{1+(x^{2^{s_{q-2}}})^{2^{a_{q-1}}-1}}{1+x^{2^{s_{q-2}}}}$$
$$+(1+x)^{k_{q-1}} x^{2^{s_{q-1}}} \frac{1+(x^{2^{s_{q-1}}})^{2^{a_q}-2}}{1+x^{2^{s_{q-1}}}} + (1+x)^{k_{q-1}} x^{2^{s_{q-1}}(2^{a_q}-1)} \tag{1}$$

Now, opening $(1+x)^{k_{q-1}}$ in the last term of Equation 1 to separate out x^d we have

$$(1+x)^{k_{q-1}} x^{2^{s_{q-1}}(2^{a_q}-1)} = x^d + x^{2^{s_{q-1}}(2^{a_q}-1)}(1+x)^{k_q-2} \sum_{i=0}^{2^{a_{q-1}}-2} x^{i2^{s_{q-2}}} +$$
$$x^{2^{s_{q-1}}(2^{a_q}-1)+2^{s_{q-2}}(2^{a_{q-1}}-1)}(1+x)^{k_q-3} \sum_{i=0}^{2^{a_q-2}-2} x^{i2^{s_{q-3}}} + \cdots + x^{2^{s_{q-1}}(2^{a_q}-1)+\cdots+2^{s_0}(2^{a_1}-1)} \sum_{i=0}^{2^{a_0}-2} x^i$$
$$= x^d + x^{l_q 2^{s_{q-2}}}(1+x)^{k_q-2} \frac{1+(x^{2^{s_{q-2}}})^{2^{a_{q-1}}-1}}{1+x^{2^{s_{q-2}}}} + x^{l_{q-1}2^{s_{q-3}}}(1+x)^{k_q-3} \frac{1+(x^{2^{s_{q-3}}})^{2^{a_{q-2}}-1}}{1+x^{2^{s_{q-3}}}}$$
$$+ \cdots + x^{l_1} \frac{1+x^{2^{a_0-1}}}{1+x} \tag{2}$$

Now from Equations 1 and 2 we have

$$1 + x^d + (1+x)^d = x\frac{1+x^{2^{a_0}-1}}{1+x} + (1+x)^{k_0} x^{2^{s_0}} \frac{1+(x^{2^{s_0}})^{2^{a_1}-1}}{1+x^{2^{s_0}}} + \cdots +$$
$$(1+x)^{k_{q-2}} x^{2^{s_{q-2}}} \frac{1+(x^{2^{s_{q-2}}})^{2^{a_{q-1}}-1}}{1+x^{2^{s_{q-2}}}} + (1+x)^{k_{q-1}} x^{2^{s_{q-1}}} \frac{1+(x^{2^{s_{q-1}}})^{2^{a_q}-2}}{1+x^{2^{s_{q-1}}}}$$
$$+x^{l_q 2^{s_{q-2}}}(1+x)^{k_q-2} \frac{1+(x^{2^{s_{q-2}}})^{2^{a_{q-1}}-1}}{1+x^{2^{s_{q-2}}}} + x^{l_{q-1}2^{s_{q-3}}}(1+x)^{k_q-3} \frac{1+(x^{2^{s_{q-3}}})^{2^{a_{q-2}}-1}}{1+x^{2^{s_{q-3}}}}$$
$$+ \cdots + x^{l_1} \frac{1+x^{2^{a_0-1}}}{1+x}$$
$$= (x+x^{l_1})\frac{1+x^{2^{a_0}-1}}{1+x} + (1+x)^{k_0}(x^{2^{s_0}} + x^{l_2 2^{s_0}}) \frac{1+(x^{2^{s_0}})^{2^{a_1}-1}}{1+x^{2^{s_0}}} + \cdots +$$
$$(1+x)^{k_{q-2}}(x^{2^{s_{q-2}}} + x^{l_q 2^{s_{q-2}}}) \frac{1+(x^{2^{s_{q-2}}})^{2^{a_{q-1}}-1}}{1+x^{2^{s_{q-2}}}} + (1+x)^{k_{q-1}} x^{2^{s_{q-1}}} \frac{1+(x^{2^{s_{q-1}}})^{2^{a_q}-2}}{1+x^{2^{s_{q-1}}}} \tag{3}$$

If each term in Equation 3 is 0 then $1 + x^d + (1+x)^d = 0$. That is, x^d is not APN if there is a $x \in V_m \setminus \{0,1\}$ such that

$$(x+x^{l_1})\frac{1+x^{2^{a_0}-1}}{1+x} = (1+x)^{k_0}(x^{2^{s_0}} + x^{l_2 2^{s_0}}) \frac{1+(x^{2^{s_0}})^{2^{a_1}-1}}{1+x^{2^{s_0}}} = \cdots$$

$$= (1+x)^{k_{q-2}}(x^{2^{s_{q-2}}} + x^{l_q 2^{s_{q-2}}}) \frac{1+(x^{2^{s_{q-2}}})^{2^{a_{q-1}}-1}}{1+x^{2^{s_{q-2}}}} = (1+x)^{k_{q-1}} x^{2^{s_{q-1}}} \frac{1+(x^{2^{s_{q-1}}})^{2^{a_q}-2}}{1+x^{2^{s_{q-1}}}} = 0.$$

Hence, x^d is not APN if

$(gcd(l_1 - 1, 2^m - 1) \neq 1$ or, $gcd(2^{a_0} - 1, 2^m - 1) \neq 1)$ and
$(gcd(l_2 - 1, 2^m - 1) \neq 1$ or, $gcd(2^{a_1} - 1, 2^m - 1) \neq 1)$ and
$\cdots$ and
$(gcd(l_q - 1, 2^m - 1) \neq 1$ or, $gcd(2^{a_{q-1}} - 1, 2^m - 1) \neq 1)$ and
$gcd(2^{a_q} - 2, 2^m - 1) \neq 1$.

That is, x^d is not APN if
$(gcd(l_1 - 1, 2^m - 1) \neq 1$ or, $gcd(a_0, m) \neq 1)$ and
$(gcd(l_2 - 1, 2^m - 1) \neq 1$ or, $gcd(a_1, m) \neq 1)$ and
$\cdots$ and
$(gcd(l_q - 1, 2^m - 1) \neq 1$ or, $gcd(a_{q-1}, m) \neq 1)$ and
$gcd(a_q - 1, m) \neq 1$. ■

p	d	Result: m such that x^d is not APN
1	1	x can not be APN for any m
2	3	no information for x^3
3	7	x^7 can not be APN if m is even
4	15	x^{15} can not be APN if $3 \mid m$
5	31	x^{31} can not be APN if m is even
6	63	x^{63} can not be APN if $5 \mid m$
7	127	x^{127} can not be APN if $2 \mid m$ or $3 \mid m$
8	255	x^{255} can not be APN if $7 \mid m$
9	511	x^{511} can not be APN if m is even
10	1023	x^{1023} can not be APN if $3 \mid m$

Table 1: $F(X) = X^d, d = 2^p - 1, p \geq 0$

d	Result: m such that x^d is not APN
5	x^5 can not be APN if $3 \mid (2^m - 1)$ i.e., m is even
9	x^9 can not be APN if $7 \mid (2^m - 1)$ i.e., $3 \mid m$
11	x^{11} can not be APN if $2 \mid m$ or $3 \mid m$
13	no information for x^{13}
17	x^{17} can not be APN if $\gcd(15, 2^m - 1) \neq 1$ i.e., m is even
19	x^{19} can not be APN if $2 \mid m$
21	x^{21} can not be APN if $19 \mid (2^m - 1)$ and $2 \mid m$
23	x^{23} can not be APN if $2 \mid m$ or $3 \mid m$
25	no information for x^{25}
27	no information for x^{27}
29	x^{29} can not be APN if $27 \mid (2^m - 1)$ and $2 \mid m$

Table 2: $F(X) = X^d, d \neq 2^p - 1$ and odd.

Following Theorem 4, we can specify some m such that X^d is not APN for a given $d > 0$. At first we present a simple case when d is of the form $2^p - 1$. X^{2^p-1} is not APN if $\gcd(p - 1, m) \neq 1$. We present some initial examples in Table 1. Further, in Table 2 we present some initial examples for general case i.e., for all odd d (because the APN property is being preserved for $2^l d, l \geq 0$) which are not of the form $2^p - 1$. In Table 3, we present

some odd d such that $X^{2^l d}, l > 0$ are not APN for a given m. There are some d, for which Theorem 4 can not say anything. Now we discuss some of such cases in the following notes.

Note 2 *1. If $a_q = 2$ then $\gcd(a_q - 1, m) = 1$ for each m. Hence, we do not earn any information. For example, we can not say anything about $X^3, X^{13}, X^{25}, X^{27}$ etc.*

2. If $a_q > 1$ and m is prime then $\gcd(a_q - 1, m) = 1$. Hence, no information in this case. For example, we can not say anything about X^{11} in V_7, V_{11} etc.

3. If m is Mersenne prime (i.e., $2^m - 1$ is also prime) then all gcd functions in the conditions return 1 except when $d = 1$. Thus, we can say only for linear functions (i.e., X^{2^i}).

4. If m is a multiple of small primes then we can filter out many X^d's as non-APN because the chance of co-primeness with m and $2^m - 1$ decreases.

m	Result: d such that $x^{2^l d}, l > 0$, is not APN
2	1
3	1
4	1, 5, 7, 11
5	1
6	1, 5, 7, 9, 11, 15, 17, 19, 23, 29, 31, 35, 37, 39, 41, 43, 47, 59
7	1
8	1, 5, 7, 11, 17, 19, 23, 29, 31, 35, 41, 43, 47, 57, 59, 65, 67, 71, 77, 79, 83, 89, 91, 95, 113, 115, 117, 119, 125, 127, 131, 137, 139, 143, 155, 161, 163, 167, 173, 175, 177, 179, 183, 185, 187, 189, 191, 227, 233, 235, 237, 239, 251,
9	1, 9, 11, 15, 23, 37, 39, 65, 67, 71, 79, 93, 95, 121, 123, 127, 135, 149, 151, 177, 179, 183, 191, 247, 261, 263, 289, 291, 295, 303, 317, 319, 359, 373, 375, 485, 487

Table 3: some odd $d : X^d$ is not APN in V_m

In block cipher design point of view, this necessary condition may not be very important, because a designer needs APN S-boxes and there are few APN S-boxes. But, using the necessary condition in Theorem 4 we can filter some X^d's which are not APN. There are some X^d's can not be filtered using the necessary condition but $X^e, e = 2^l d \bmod (2^m - 1)$ for some l may satisfy the conditions and can be shown as non-APN. In this case, X^d can too be filtered out. For example, X^{13} can not be shown as non-APN directly in V_4 but X^7 can be used to show X^{13} as non-APN because $13 = (2^2 * 7) \bmod 15$ and X^7 satisfies the necessary condition. Hence, using this technique we can filter out more non-APN S-boxes and present some experimental results on the number of filtered out S-boxes in Table 4. However,we have some interesting facts that we can filter out some power S-boxes X^d, $\gcd(d, 2^m - 1) = 3$ when m is even and $\gcd(d, 2^m - 1) = 1$ when m is odd. In Table 4, we present some experimental results on the number of filtered power non-APN functions comparing with total number of power functions and on the number of filtered power functions from total number power functions satisfying $\gcd(d, 2^m - 1) = 3$ when m is even

m even	(#filtered $X^d, 2^m-2$), (#filtered X^{3e}, t) where $\gcd(e, 2^m-1)=1$, $t=\lvert\{d : \gcd(d, 2^m-1)=3\}\rvert$ $1 \le d \le 2^m-2$ and $1 \le e \le k-1$	m odd	(#filtered $X^d, 2^m-2$), (#filtered X^e, t) where $\gcd(e, 2^m-1)=1$, $t=\lvert\{d : \gcd(d, 2^m-1)=1\}$ $1 \le d \le 2^m-2$ and $1 \le e \le 2^m-2$
2	$(2,2),(0,0)$	3	$(3,6),(3,6)$
4	$(10,14),(0,4)$	5	$(5,30),(5,30)$
6	$(51,62),(6,12)$	7	$(7,126),(7,126)$
8	$(200,254),(32,64)$	9	$(189,510),(189,432)$
10	$(820,1022),(150,300)$	11	$(11,2046),(11,1936)$
12	$(3842,4094),(468,576)$	13	$(13,8190),(13,8190)$
14	$(10885,16382),(1036,5292)$	15	$(10785,32766),(9615,27000)$
16	$(50424,65534),(10384,16384)$	17	$(17,131070),(17,131070)$
18	$(228573,262142),(36540,46656)$	19	$(19,524286),(19,524286)$
20	$(827884,1048574),(178660,240000)$	21	$(297612,2097150),(290997,1778112)$
22	$(2101099,4194302),(199386,1320352)$	23	$(23,8388606),(23,8210080)$
24	$(15070558,16777214),(1961688,2211840)$	25	$(223750,33554430),(223100,32400000)$
26	$(24603358,67108862),(53326,22358700)$	27	$(8321670,134217726),(8160102,113467392)$

Table 4: Comparison of the number of filtered X^d and X^{3e} with the number of all elements

and $\gcd(d, 2^m-1)=1$ when m is odd. In some cases, specifically when m is a multiple of small primes, we can filter out many non-APN functions using our necessary conditions.

Acknowledgment: The authors are very much thankful to Prof. Pascale Charpin for her excellent guidance and suggestions that provided me to gain the ideas and to improve the quality of this paper.

References

[1] T. P. Berger, A. Canteaut, P. Charpin and Y.Laigle-Chapuy. Almost Perfect Nonlinear functions Research report, INRIA, Rocquencourt, Number 5774, 2005.

[2] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystem. In *Journal of Cryptology*, 4(1):3 – 72, 1991.

[3] L. Budaghyan,C. Carlet and G. Leander. Constructing new APN functions from known ones. Cryptology ePrint Archive: report 2007/063.

[4] C. Carlet, P. Charpin and V. Zinoviev. Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystem. *Design, Codes and Cryptography*, 15(2):125 – 156, 1998.

[5] P. Charpin, A. Tietävämen and V. Zinoviev. On binary cyclic codes with minimum distance $d=3$. *Problems Inform. Transmission*, 33(4):287 – 296, 1997.

[6] L. Comtet. *Advanced combinatorics*, Reidel Publication, 1974.

[7] K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. In *Advances in Cryptology - CRYPTO'92*, number 740, pp. 566 – 574 in Lecture Notes in Computer Science. Springer-Verlag, 1993.

[8] K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology - Eurocrypt 1993*, number 765, pp. 55 – 64 in Lecture Notes in Computer Science. Springer-Verlag, 1994.