A note on verifying the APN property

Pascale Charpin* Gohar M. Kyureghyan†

August 2, 2013

Abstract

We show that for an arbitrary mapping F on $\mathbb{F}_2^n$ to verify that it is APN, it is enough to consider the difference mappings of F defined by elements from an hyperplane.

Keywords: Boolean function, APN functions, hyperplane, cryptographic criteria, differential uniformity.

1 Introduction

Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ and $a \in \mathbb{F}_{2^n}$ be non-zero. The mapping

$$D_aF : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n},\ x \mapsto F(x+a) + F(x)$$

ia called *the difference mapping of F defined by a*, or the derivative of F in direction a. The *differential uniformity* of F is defined as

$$\delta(F) = \max_{a \neq 0,\ \gamma \in \mathbb{F}_{2^n}} |\{x \in \mathbb{F}_{2^n} \mid D_aF(x) = \gamma\ \}. \tag{1}$$

The image set of a difference mapping D_aF contains at most 2^{n-1} elements, since $D_aF(x) = D_aF(x+a)$ for any $a \in \mathbb{F}_{2^n}$. Clearly, the image set of a

*INRIA, SECRET project-team, 78153 Le Chesnay Cedex, France, Pascale.Charpin@inria.fr

†Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany, Gohar.Kyureghyan@ovgu.de

difference mapping D_aF is of that maximal size if and only if D_aF is 2-to-1. A mapping is called *almost perfect nonlinear*, abbreviated APN, if all its difference mappings are 2-to-1. Note that the APN mappings can be defined also as those having differential uniformity 2. APN mappings provide the optimal resistance against the *differential cryptanalysis* when they are used as an S-BOX [5].

To verify the APN property of F it necessitates, a priori, to check that all difference mappings D_aF are 2-to-1. Actually, it is well-known that not all D_aF must be checked. It was notably proved in [2, Eurocrypt 93] that it is sufficient to check 2^{n-1} well-chosen D_aF. In this note, we come back to this result and show that it is equivalent to the following statement: Let H be a hyperplane in $\mathbb{F}_{2^n}$, that is H is an $(n-1)$-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$. A mapping $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is APN if and only if D_aF are 2-to-1 for all non-zero $a \in H$.

Further we give some applications of the latter result.

2 A combinatorial problem

In [2], Beth and Ding introduced a so-called differential representation set of $\mathbb{F}_2^n$, which is defined as follows:

Definition 1 *Let S be a subset of $\mathbb{F}_2^n \setminus \{0\}$. If S satisfies*

$$x \in \mathbb{F}_2^n,\ y \in \mathbb{F}_2^n \text{ with } x \neq 0,\ y \neq 0,\ x \neq y \quad \Rightarrow \quad \{x, y, x+y\} \cap S \neq \emptyset, \quad (2)$$

then S is called a differential representation set of $\mathbb{F}_2^n$. Moreover, S is said minimal when it has minimal size.

It is proved in [2] that the size of differential representation set S is equal to or greater than $2^{n-1} - 1$. This is easy to see. Indeed, set

$$S' = \mathbb{F}_2^n \setminus (S \cup \{0\}) = \{s_1, s_2, \dots, s_\ell\},\ \ell = 2^n - |S| - 1.$$

Thus, the $\ell-1$ elements s_1+s_i, $2 \leq i \leq \ell$, belong to S so that $|S| \geq 2^n - |S| - 2$ providing $|S| \geq 2^{n-1} - 1$. In particular, a minimal differential representation set of $\mathbb{F}_2^n$ has cardinality $2^{n-1} - 1$. The next theorem shows that the minimal differential representation sets are exactly the hyperplanes of $\mathbb{F}_2^n$ without the zero element.

Theorem 1 *A subset $S \subset \mathbb{F}_2^n$ is a minimal differential representation set of $\mathbb{F}_2^n$ if and only if $S \cup \{0\}$ is an hyperplane of $\mathbb{F}_2^n$.*

Proof. Let $k := |S| = 2^{n-1} - 1$. Evidently, if $S \cup \{0\}$ is an hyperplane of $\mathbb{F}_2^n$ then S satisfies (2). So suppose that S satisfies (2) with $k = 2^{n-1} - 1$. Our goal is to prove that $S \cup \{0\}$ is an hyperplane.

We proceed by induction. For $n = 2$ it is clear that the property holds. We assume that the statement is true until $n - 1$ where $n \geq 3$.

Let H be any hyperplane of $\mathbb{F}_2^n$ and denote by $\overline{H}$ its complement in $\mathbb{F}_2^n$. Set

$$T = (S \cup \{0\}) \cap H \quad \text{and} \quad \overline{T} = S \cap \overline{H}.$$

Then $|T| \geq 2^{n-2}$ since T satisfies (2) in $H \setminus \{0\}$. Therefore $\overline{T} \leq 2^{n-2}$. Note that if $|T| = 2^{n-1}$ then $T = H$. So we suppose now that $|T| < 2^{n-1}$.

Fix $y \in H \setminus T$. Then for all $z \in \overline{H} \setminus \overline{T}$ we get $y + z \in \overline{H}$. But $y + z \in \overline{T}$ because $y \notin S$ and $z \notin S$. The set of elements $y + z$, z describing $\overline{H} \setminus \overline{T}$ has cardinality c with $c \geq 2^{n-2}$. This is impossible unless $|\overline{T}| = 2^{n-2}$.

If $|T| = 2^{n-2}$ then T is a subspace of dimension $n - 2$, from the induction hypothesis applied to H. In this case, we have

$$\mathbb{F}_2^n = T \cup (a + T) \cup (b + T) \cup (a + b + T), \ \textit{with } H = (T \cup a) + T,$$

for some (a, b). If $\overline{T}$ is neither equal to $b + T$ nor equal to $(a + b) + T$ then there are

$$x \in b + T \setminus \overline{T}, \ y \in (a + b) + T \setminus \overline{T} \ \text{ providing } x + y \in a + T$$

which contradicts (2). So $\overline{T}$ is a coset of T, completing the proof. ◇

3 Verifying the APN property

Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$. We say that F satisfies the property (p_a), $a \in \mathbb{F}_{2^n}^*$, when the equation

$$F(x) + F(x + a) = b \tag{3}$$

has either 0 or 2 solutions for all $b \in \mathbb{F}_{2^n}$, i.e. the derivative of F in direction a is 2-to-1. In [2], it is shown that to verify that F is APN it is enough to check (p_a) for all elements a from a differential representation set of $\mathbb{F}_{2^n}$. Hence by Theorem 1, this result becomes the next theorem, which is introduced in [4, Theorem 2.1]. We give a sketch of proof for clarity.

Theorem 2 *Let H be a hyperplane in $\mathbb{F}_{2^n}$, that is H is an $(n-1)$-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$. A mapping $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is APN if and only if F satisfies (p_a) for all non-zero $a \in H$.*

Proof. Necessity of the condition follows clearly from definition of APN mappings. To prove that it is also sufficient, suppose that $\alpha \in \mathbb{F}_{2^n} \setminus H$ and $D_\alpha F$ is not 2-to-1. Then there are two distinct $x, y \in \mathbb{F}_{2^n}$ such that $x+y \neq \alpha$ and

$$D_\alpha F(x) = F(x) + F(x+\alpha) = F(y) + F(y+\alpha) = D_\alpha F(y).$$

After that, one prove easily that

$$D_{x+y}F(x) = D_{x+y}F(x+\alpha) \text{ and } D_{x+y+\alpha}F(x) = D_{x+y+\alpha}F(x+\alpha).$$

Thus, $D_{x+y}F$ and $D_{x+y+\alpha}$ are not 2-to-1, which is a contradiction since either $x+y$ or $x+y+\alpha$ belong to H. $\diamond$

With the previous result, we can directly simplify some characterizations of APN functions. For example, [1, Theorem 2] reduces to Theorem 3. We use the notation from [1]: f_λ, $\lambda \in \mathbb{F}_{2^n}^*$, are the *component functions* of F , *i.e.,* the Boolean functions $x \mapsto Tr(\lambda F(x))$ where Tr is the absolute trace on $\mathbb{F}_{2^n}$; also, for any Boolean function f, set

$$\mathcal{F}(f) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} \text{ and } D_a f(x) := f(x) + f(x+a).$$

Theorem 3 *Let H be any hyperplane in $\mathbb{F}_{2^n}$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ let f_λ, $\lambda \in \mathbb{F}_{2^n}$, denote its components. Then, for any nonzero $a \in \mathbb{F}_{2^n}$:*

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1}. \tag{4}$$

Moreover, F is APN if and only if for all nonzero $a \in H$:

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^{2n+1}. \tag{5}$$

Proof. Set $A = \sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda)$ for some λ. Then A is equal to

$$\sum_{\lambda,x,y \ \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda(F(x+a)+F(x)+F(y+a)+F(y)))}.$$

So

$$\begin{aligned} A &= 2^n \#\{(x,y) \in \mathbf{F}_{2^n}^2 \mid D_aF(x) = D_aF(y)\} \\ &= 2^{2n+1} \\ &+ \ 2^n \#\{(x,y) | \ D_aF(x) = D_aF(y), x \neq y \neq x+a\}, \end{aligned}$$

implying (4). Moreover $A = 2^{2n+1}$ if and only if D_aF is 2-to-1, *i.e.,*

$$D_aF(x) = D_aF(y) \ \text{ for } y \in \{x, x+a\} \text{ only.}$$

Theorem 2 completes the proof. ◇

Remark 1 *If we look at the components of F, Theorem 2 is related with Theorems V.2 and V.3 from [3] which consider Boolean functions. These theorems show that one can check that a Boolean function is bent (resp. semi-bent) by looking at the derivatives in direction $a \in H$ only, where H is any hyperplane.*

For several classes of mappings, it is well-known that to verify the APN property it is sufficient to check (p_a) for particular values of a. The most simple case is when $F(x) = x^t$ for some fixed integer t. In this case it is enough to check (p_1) only. When F is a polynomial whose coefficients are in a subfield of $\mathbb{F}_{2^n}$, Theorem 1 yields another general simplification.

Theorem 4 *Let $H = \{ \ \alpha \in \mathbb{F}_{2^n} \mid Tr(\alpha) = 0 \ \}$. Set $n = ks$ where $s > 1$ and $k \geq 1$. Let β be a primitive root of $\mathbb{F}_{2^n}$. Let F be a mapping on $\mathbb{F}_{2^n}$ which is given by a polynomial in $\mathbb{F}_{2^k}[x]$. Let I be a set of representatives of 2^k-cyclotomic cosets modulo $2^n - 1$ and $\mathcal{I} = \{i \in I \mid \beta^i \in H\}$.*

Then, F is APN if and only if it satisfies (p_a) for all $a \in \mathcal{I}$.

Proof. From Theorem 1, we can choose any hyperplane H to check the APN property. Here H is the hyperplane which is invariant under the Froebenius isomorphism $\sigma : a \mapsto a^2$. Thus, taking $a \in H$ we get $a^{2^k} \in H$ and

$$D_{a^{2^k}}F(y) = F(y + a^{2^k}) + F(y) = (F(x+a) + F(x))^{2^k} = (D_aF(x))^{2^k}$$

where $y = x^{2^k}$, since $F \in \mathbb{F}_{2^k}[x]$. It is clear that $D_{a^{2^k}}F$ is 2-to-1 if and only if D_aF is, completing the proof. ◇

Example 1 *Let F be any mapping on $\mathbb{F}_{2^7}$ expressed by a polynomial in $\mathbb{F}_2[x]$. There are 18 cyclotomic cosets modulo 127, implying $|\mathcal{I}| = 9$. Then F is APN as soon as D_aF satisfies (p_a) for only 9 elements a.*

4 Conclusion

Many questions arise when the computation of the differential uniformity of mappings is discussed. We give only two examples of problems which appear evidently according to Theorem 1. The first one concerns APN property only.

Problem 1 *Given an arbitrary mapping F, Theorem 2 shows that to verify that F is APN it is enough to check (p_a) for non-zero elements a from a hyperplane. Are there other sets, possibly with less elements than $2^{n-1}-1$, for which a similar statement holds?*

The second one concerns the so-called *differential spectrum* of a mapping F on $\mathbb{F}_{2^n}$, *i.e.,* the multiset of the numbers of solutions of

$$F(x)+F(x+a)=b,\ a\in\mathbb{F}_{2^n}^*,\ b\in\mathbb{F}_{2^n}.$$

Problem 2 *Find new classes of mappings, for which the computation of the differential spectrum or, more simply, of the differential uniformity can be reduced to examine D_aF on a small set of elements a.*

References

[1] T.P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, On Almost Perfect Nonlinear functions over $\mathbf{F}_2^n$, *IEEE Trans. Inform. Theory*, vol. 52, n. 9, pp. 4160-70, September 2006.

[2] T. Beth and C. Ding, On almost perfect nonlinear permutations, Advances in Cryptology–EUROCRYPT 93 (Lofthus, 1993), Lecture Notes in Comput. Sci. 765, Springer, Berlin, 1994, pp. 6576.

[3] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "On cryptographic properties of the cosets of $R(1,m)$", *IEEE Trans. Inform. Theory*, 47(4):1494–1513, 2001.

[4] G. M. Kyureghyan, Special mapping of finite fields, invited survey in Finite Fields and Their Applications, eds. P. Charpin, A. Pott and A. Winterhof, De Gruyter (2013) pp. 117-144.

[5] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in cryptology—EUROCRYPT '91 (Brighton, 1991)*, volume 547 of *Lecture Notes in Comput. Sci.*, pages 378–386. Springer, Berlin, 1991.