Finite Fields and Their Applications 18 (2012) 522–528

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On weakly APN functions and 4-bit S-Boxes

Claudio Fontanari [a,*], Valentina Pulice [a], Anna Rimoldi [b], Massimiliano Sala [a]

[a] *Department of Mathematics, University of Trento, Italy*
[b] *eRISCS, Université de la Méditerranée, Marseille, France*

ARTICLE INFO

Article history:
Received 5 March 2011
Revised 4 November 2011
Accepted 9 November 2011
Available online 17 November 2011
Communicated by Gary McGuire

MSC:
94A60
06E30
20B40

Keywords:
S-Box
Permutation
Translation-base cipher
Boolean functions
Weak uniformity
Antiinvariance

ABSTRACT

S-Boxes are important security components of block ciphers. We provide theoretical results on necessary or sufficient criteria for an (invertible) 4-bit S-Box to be weakly APN. Thanks to a classification of 4-bit invertible S-Boxes achieved independently by De Cannière and Leander–Poschmann, we can strengthen our results with a computer-aided proof. We also propose a class of 4-bit S-Boxes which are very strong from a security point of view.

1. Introduction

We consider block ciphers acting on a vector space $(\mathbb{F}_2)^n$. It is important to identify conditions on the components of the cipher that may ensure its security. There are many competing notions of security, hence several kinds of security criteria, and some of them focus on the role of the S-Boxes. For a large class of nowadays block ciphers, the S-Boxes are bijective vectorial Boolean functions $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$, hence they are functions from the finite field $(\mathbb{F}_2)^m$ to itself.

* Corresponding author.
E-mail addresses: fontanar@science.unitn.it (C. Fontanari), pulice@science.unitn.it (V. Pulice), rimoldi@science.unitn.it (A. Rimoldi), maxsalacodes@gmail.com (M. Sala).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.11.003

In this paper we focus on 4-bit S-Boxes, as used for example in SERPENT [2] and PRESENT [4], although we present also a theorem for the general case. Several security criteria are affine-invariant and this justifies the work done to achieve the classification of 4-bit S-Boxes in affine-equivalence classes, due to De Cannière [8] and Leander and Poschmann [9] (these classifications have been obtained independently).

There is a new security criteria for S-Boxes which is affine-invariant, the weakly differential uniformity. Particularly interesting is the concept of weakly APN. We determine several conditions (some computational and some theoretical), which are either sufficient or necessary for a 4-bit Boolean permutation to be weakly APN.

Our paper is structured as follows. In Section 2 we introduce and motivate the notion of *weakly APN function*, highlighting the case of dimension four. In Section 3 we present our theoretical results, including a theorem for any dimension. In Section 4 we discuss our computational results. Finally, in Section 5 we provide further computations that may be interesting and we draw our conclusions.

2. Preliminaries on weakly APN functions

We provide some standard notation and terminology to be freely used in the sequel.

If X is any set, then $|X|$ denotes its cardinality, while if V is a vector space over $\mathbb{F}_2$, then $\dim(V)$ denotes its dimension.

If p is a polynomial in $\mathbb{F}_2[x_1, \dots, x_m]$ then $\deg(p)$ denotes its total degree.

Without loss of generality, we consider only vectorial Boolean functions (v.B.f.) $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$ such that $f(0) = 0$.

If $v \in (\mathbb{F}_2)^m$, then the function $\langle f, v\rangle(x)$ is defined by $\langle f(x), v\rangle$, where $\langle , \rangle$ denotes the standard scalar product in $(\mathbb{F}_2)^m$.

Two permutations $f, g : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$ are *affine equivalent*, $f \sim g$, if there exist two invertible linear $m \times m$ matrices A, B and two constants $a, b \in (\mathbb{F}_2)^m$ such that $g(x) = B(f(A(x) + a)) + b$.

If a property of a v.B.f. is invariant under the action of the affine group, then it is called *affine-invariant*.

We also write $D_u(f)(x) := f(x+u) + f(x)$ (the *derivative* of f) and $\mathrm{Im}(f) = \{f(x) \mid x \in (\mathbb{F}_2)^m\}$ (the *image* of f).

A notion of non-linearity for S-Boxes that has received a lot of attention is the following.

Definition 1. The v.B.f. f is *δ-differentially uniform* if for any $u \in (\mathbb{F}_2)^m \setminus \{0\}$ and for any $v \in (\mathbb{F}_2)^m$, $|\{x \in (\mathbb{F}_2)^m\colon\ D_u(f)(x) = v\}| \leqslant \delta$.

If f is 2-differentially uniform, then it is called an *Almost Perfectly Non-linear* (*APN*) function.

The property of being δ-differentially uniform is affine-invariant. W.r.t. differential uniformity, the best S-Boxes are the APN S-Boxes. APN functions are indeed a very hot research topic (see for instance the recent contributions [3] and [5]). Unfortunately, for some even dimensions, no APN permutation exists. This is the case for dimension $m = 4$, which has cryptographic significance at least for SERPENT and PRESENT. In this case, the best we can have is $\delta = 4$.

There is a natural generalization of differential uniformity presented recently in [7], which we recall in the following definition.

Definition 2. The v.B.f. f is *weakly δ-differentially uniform* if for any $u \in (\mathbb{F}_2)^m \setminus \{0\}$ we have $|\mathrm{Im}(D_u(f))| > 2^{m-1}/\delta$.

If f is weakly 2-differentially uniform, then it is called a *weakly Almost Perfectly Non-linear* (*weakly APN*) function.

By [7, Section 4, Fact 3], a δ-differentially uniform map is weakly δ-differentially uniform, and it is easy to check that weak δ-differential uniformity is affine-invariant.

The significance for the previous definition lies in [7, Theorem 4.4]. In order to appreciate it, we need another definition.

Definition 3. A v.B.f. f is *strongly l-anti-invariant* if for any two subspaces $V, W \leqslant (\mathbb{F}_2)^m$ such that $f(V) = W$ then either $\dim(V) = \dim(W) < m - l$ or $V = W = (\mathbb{F}_2)^m$.

The cryptographic significance of the previous definition becomes clear provided that f is a permutation: the greater l, the larger the non-linearity of f.

An iterated block cipher is obtained by the composition of several rounds (or round functions), i.e., key-dependent permutations of the message/cipher space. To avoid potential weaknesses of a given cipher $\mathcal{C}$, it is desirable that the permutation group $\Gamma_\infty(\mathcal{C})$ generated by its round functions with the key varying in the key space is primitive (for instance, a way to construct a trapdoor using imprimitivity is presented in [11]). Translation-based ciphers (see [7, Definition 3.1]) form an interesting class of iterated block ciphers containing AES [10], SERPENT, PRESENT. According to Theorem 4.4 in [7], if $\mathcal{C}$ is a translation-based cipher and each brick γ' of every parallel S-Box γ used in the proper round under consideration is both weakly 2^r-differentially uniform and strongly r-anti-invariant for some r with $1 \leqslant r \leqslant m/2$, then $\Gamma_\infty(\mathcal{C})$ is primitive. It may seem that Theorem 4.4 in [7] requires too strong conditions in order to ensure primitivity, but indeed they turn out to be quite natural, as shown in [7, Section 5]. In the case of 4-bit S-Boxes, we have only two possibilities: $r = 1$, requiring every γ' to be both strongly 1-anti-invariant (which always holds if it is maximally non-linear, see for instance [7, footnote 4 on p. 347]) and weakly APN; or $r = 2$, requiring every γ' to be both weakly 4-differentially uniform (which always holds if it is 4-differentially uniform) and 2-strongly-anti-invariant.

3. Theoretical results on weakly APN functions

Generally speaking, two different $r' > r$ give logically independent hypotheses in the statement of Theorem 4.4 in [7], because weakly 2^r-differential uniformity implies weakly $2^{r'}$-differential uniformity, while r'-anti-invariance implies r-anti-invariance. Our first result is to show that for 4-differentially uniform functions the case $r = 2$ of Theorem 4.4 in [7] is just a sub-case of the case $r = 1$.

Proposition 1. *Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ be an invertible v.B.f. such that*

(i) *f is 4-differentially uniform,*
(ii) *f is strongly 2-anti-invariant.*

Then f is weakly APN.

Proof. Assume by contradiction that $|\mathrm{Im}(D_u(f))| \leqslant 4$. Then from (i) we deduce that $|D_u(f)^{-1}(y)| = 4$ for every $y \in \mathrm{Im}(D_u(f))$. Hence we have $D_u(f)^{-1}(f(u)) = \{0, u, x, u + x\}$ for some x, in particular $D_u(f)^{-1}(f(u))$ is a 2-dimensional vector subspace. On the other hand, $D_u(f)(x) = D_u(f)(u)$ implies $f(x + u) = f(u) - f(x)$. It follows that $f(\{0, u, x, u + x\})$ is a 2-dimensional vector subspace, contradicting (ii). □

In other words, Proposition 1 provides some sufficient conditions for a 4-bit S-Box to be weakly APN. Other sufficient conditions are presented in the next proposition and are based on the following non-linearity measures:

$$n_i(f) = \left|\left\{v \in (\mathbb{F}_2)^m \setminus \{0\}\colon \deg\big(\langle f, v\rangle\big) = i\right\}\right| \tag{1}$$

and

$$\hat{n}(f) = \max_{u \in (\mathbb{F}_2)^m \setminus \{0\}} \left|\left\{v \in (\mathbb{F}_2)^m \setminus \{0\}\colon \deg\big(\langle D_u(f), v\rangle\big) = 0\right\}\right|. \tag{2}$$

Proposition 2. *Let $f:(\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ be a v.B.f. such that $\hat{n}(f)=0$.*
Then f is weakly APN.

Proof. Let $(\mathbb{F}_2)^4=\{x_1,\ldots,x_{16}\}$ and given $u \in (\mathbb{F}_2)^m \setminus \{0\}$ let $M=(m_{ij}) \in (\mathbb{F}_2)^{4\times 16}$ with $m_{ij}:=(D_u(f))_i(x_j)$. By definition, f is weakly APN if and only if $|\mathrm{Im}(D_u(f))|>4$, hence if and only if M has more than 4 distinct columns.

Assume by contradiction that M has $n \leqslant 4$ distinct columns and let $M' \in (\mathbb{F}_2)^{4\times n}$ be the corresponding submatrix.

If M' has rank 4, then we may write $(1,1,1,1)$ as a linear combination (over $\mathbb{F}_2$) of the rows of M':

$$(1,1,1,1)=aM'_1+bM'_2+cM'_3+dM'_4.$$

Since all the other columns of M are equal to the columns of M', we may write $(1,\ldots,1) \in (\mathbb{F}_2)^{16}$ as the same linear combination of the rows of M:

$$(1,\ldots,1)=aM_1+bM_2+cM_3+dM_4.$$

Hence the function $\langle D_u(f),(a,b,c,d)\rangle$ is the constant 1, contradiction.

If instead M' has rank at most 3, then we may write $(0,0,0,0)$ as a non-zero linear combination of the rows of M':

$$(0,0,0,0)=aM'_1+bM'_2+cM'_3+dM'_4.$$

Since all the other columns of M are equal to the columns of M', we may write $(0,\ldots,0) \in (\mathbb{F}_2)^{16}$ as the same linear combination of the rows of M:

$$(0,\ldots,0)=aM_1+bM_2+cM_3+dM_4.$$

Hence the function $\langle D_u(f),(a,b,c,d)\rangle$ is the constant 0, contradiction. □

The following partial converse to Proposition 2 gives necessary conditions and holds for *any* $m \geqslant 2$.

Theorem 1. *Let $f:(\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$ be a weakly APN function.*
Then $\hat{n}(f) \leqslant 1$.

Proof. Let $f=(f_1,f_2,\ldots,f_m)$ with $f_i:(\mathbb{F}_2)^m \to \mathbb{F}_2$ and assume by contradiction that both $\langle D_u(f),v_1\rangle$ and $\langle D_u(f),v_2\rangle$ are constant for some $u, v_1 \neq v_2 \in (\mathbb{F}_2)^m \setminus \{0\}$. Up to a linear transformation sending v_1 to $(1,0,0,\ldots,0)$ and v_2 to $(0,1,0,\ldots,0)$, without loss of generality we may assume that both the first component $(D_u(f))_1$ and the second component $(D_u(f))_2$ of $D_u(f)$ are constant. It follows that $|\mathrm{Im}(D_u(f))| \leqslant 2^{m-2}$ and f is not weakly APN, contradiction. □

As an application of Theorem 1, we obtain the following:

Proposition 3. *Let $f:(\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ be a weakly APN permutation.*
Then $\deg(f)=3$ *and* $n_3(f) \in \{12,14,15\}$.

Proof. It is well known that $\deg f \leqslant 3$ (see for instance [15]). If

$$\left|\left\{v \in (\mathbb{F}_2)^4 \setminus \{0\}\colon \deg\bigl(\langle f,v\rangle\bigr) \leqslant 2\right\}\right| \leqslant 5$$

then our claim holds, since $\{v \in (\mathbb{F}_2)^4 \setminus \{0\}\colon \deg(\langle f,v\rangle) \leqslant 2\} \cup \{0\}$ is a vector subspace of $(\mathbb{F}_2)^4$.

Let $f = (f_1, f_2, f_3, f_4)$ with $f_i : (\mathbb{F}_2)^4 \to \mathbb{F}_2$ and assume by contradiction that $\deg(S) \leqslant 2$ for 6 different linear combinations $S = \sum_{i=1}^{4} v_i f_i$. From the basic theory of quadratic Boolean functions (see for instance [6, Section 2.2]), it follows that the derivative $D_u(S)$ is constant for every $u \in V(S) \subseteq (\mathbb{F}_2)^4$, where $V(S)$ is a vector subspace and its dimension is 0 if and only if S is bent, 4 if and only if S is linear (affine), and 2 otherwise. Now, S is not bent since it is balanced (see for instance [1]) and bent functions are never balanced (see for instance [12]). Thus $\dim V(S) \geqslant 2$ for every S and $|V(S) \setminus \{0\}| \geqslant 3$, in particular 6 sets $V(S) \setminus \{0\} \subseteq (\mathbb{F}_2)^4 \setminus \{0\}$ cannot be disjoint. Hence there is $u \in (\mathbb{F}_2)^4 \setminus \{0\}$ and two different non-zero linear combinations S_1 and S_2 such that both $D_u(S_1)$ and $D_u(S_2)$ are constant and this contradicts Theorem 1. □

4. Computational results on weakly APN function

The problem of classifying (invertible) S-Boxes $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$ (w.r.t. affine-equivalence) was solved in [8,9] in the case $m = 4$ and has been recently checked in [13,14]. By a direct check on the class representatives, we may draw a series of consequences, that we call *Facts*.

First of all, we see that three of our theoretical results cannot be inverted, as follows.

Fact 1. *The converse of Proposition* 1 *does not hold.*

Proof. $(0, 1, 2, 13, 4, 15, 14, 7, 8, 3, 5, 9, 10, 6, 12, 11)$ is weakly APN but is *not* 4-differentially uniform. □

Fact 2. *The converse of Proposition* 2 *does not hold.*

Proof. $(0, 1, 2, 13, 4, 15, 14, 7, 8, 3, 5, 9, 10, 6, 12, 11)$ is weakly APN but $\hat{n} = 1$. □

Fact 3. *The converse of Theorem* 1 *does not hold.*

Proof. For $f = (0, 1, 2, 7, 4, 10, 15, 9, 8, 3, 13, 14, 12, 5, 6, 11)$ we have $\hat{n}(f) = 1$ but f is not weakly APN. □

Next, we can strengthen Proposition 3:

Fact 4. *Let* $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ *be a weakly APN permutation. Then* $\deg(f) = 3$ *and* $n_3(f) \in \{14, 15\}$.

Unfortunately, the previous fact cannot be inverted:

Fact 5. *The converse of Fact* 4 *does not hold.*

Proof. For $f = (0, 1, 2, 7, 4, 10, 15, 9, 8, 3, 13, 14, 12, 5, 6, 11)$ we have $\deg(f) = 3$ and $n_3(f) = 14$, but f is not weakly APN. □

Finally, we want to provide some sufficient conditions (for f to be weakly APN), involving also the following classical concept of non-linearity:

Definition 4.

$$\mathrm{Lin}(f) = \max_{a \in (\mathbb{F}_2)^m, b \in (\mathbb{F}_2)^m \setminus \{0\}} \left| \langle f, b \rangle^{\mathcal{W}}(a) \right|,$$

where $\mathcal{W}$ denotes the Walsh coefficient (see for instance (1) in [9]).

Since for $m = 4$ we have that $\mathrm{Lin}(f) \geqslant 8$, we find of interest the following result:

Fact 6. *Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ be a Boolean permutation such that*

$$\mathrm{Lin}(f) = 8, \qquad f \text{ is 4-differentially uniform}, \qquad n_3(f) \geqslant 14.$$

Then f is weakly APN.

Regrettably, the assumptions of Fact 6 cannot be weakened. We provide two (affine-independent) counterexamples:

- with $f = (0, 1, 2, 12, 4, 13, 11, 10, 8, 15, 5, 9, 6, 14, 7, 3)$ we have $\mathrm{Lin}(f) = 8$ and $n_3(f) = 14$, but f is not weakly APN,
- with $f = (0, 1, 2, 12, 4, 6, 14, 5, 8, 3, 13, 10, 9, 7, 15, 11)$ we have that f is 4-differentially uniform and that $n_3(f) = 14$, but again f is not weakly APN.

5. More computational results and conclusions

Let we recall from [9] the further measures of non-linearity:

– $\mathrm{Lin}_1(f) = \max_{a,b\in(\mathbb{F}_2)^m, \mathrm{w}(a)=\mathrm{w}(b)=1} \{|\langle f, b\rangle^{\mathcal{W}}(a)|\}$,
– $\mathrm{Diff}_1(f) = \max_{a,b\in(\mathbb{F}_2)^m, \mathrm{w}(a)=\mathrm{w}(b)=1} \{|D_a(f)^{-1}(b)|\}$.

Then we introduce a new class of S-Boxes suitable for block ciphers construction:

Definition 5. We say that an invertible v.B.f. $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ is a *strong* S-Box if f is weakly APN, 4-differentially uniform, and

$$\mathrm{Lin}(f) = 8, \qquad \mathrm{Diff}_1(f) = 0, \qquad \mathrm{Lin}_1(f) = 4, \qquad n_3(f) \geqslant 14.$$

Moreover, we say that f is *very strong* if it is strong and strongly 2-anti-invariant.

Note that a very strong function is in particular both optimal [9, Definition 1] and Serpent-type [9, Definition 2], and also it satisfies Theorem 4.4 of [7]. A direct computation (see [13]) allows us to conclude:

Fact 7. *There are* 55 296 *strong S-Boxes and* 2304 *very strong ones.*

Remark 1. As in the rest of the paper, all statements in this section assume $f(0) = 0$. So Fact 7 implies that there are actually $55\,296 * 16 = 884\,736$ invertible 4-bit S-Boxes equivalent via a translation to strong S-Boxes, therefore sharing their security robustness. The same goes for $2304 * 16 = 36\,864$ S-Boxes equivalent to very strong S-Boxes.

Following [9], we have tested the properties of the S-Boxes used in SERPENT, denoted by $S_0, S_1, \ldots, S_7$ (for details see [13]), and we get:

Fact 8. *The S-Boxes S_3, S_4, S_5, S_7 are strong. None of the S_i's is very strong.*

In conclusion, we have considered the link between the recent notion of weakly APN function and several more traditional non-linearity properties, such as differential uniformity, algebraic degree and classical non-linearity. We obtained both theoretical and computational results. In particular, sufficient conditions for an S-Box to be weakly APN are presented in Propositions 1 and 2 and Fact 6; while necessary ones can be found in Theorem 1, Proposition 3 and Fact 4.

Acknowledgments

This research has been supported by TELSY S.p.A., MIUR "Rientro dei cervelli", GNSAGA of INdAM and MIUR Cofin 2008 – "Geometria delle varietà algebriche e dei loro spazi di moduli" (Italy).

References

[1] C. Adams, S. Tavares, The structured design of cryptographically good S-boxes, J. Cryptology 3 (1) (1990) 27–41.
[2] R.J. Anderson, E. Biham, L.R. Knudsen, Serpent: A new block cipher proposal, in: Proc. of FSE 1998, in: Lecture Notes in Comput. Sci., vol. 1372, 1998, pp. 222–238.
[3] Y. Aubry, G. McGuire, F. Rodier, A few more functions that are not APN infinitely often, in: Finite Fields: Theory and Applications, in: Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 2010, pp. 23–31.
[4] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, C. Vikkelsoe, PRESENT: An ultra-lightweight block cipher, in: Proc. of CHES 2007, in: Lecture Notes in Comput. Sci., vol. 7427, 2007, pp. 450–466.
[5] C. Bracken, E. Byrne, N. Markin, G. McGuire, Fourier spectra of binomial APN functions, SIAM J. Discrete Math. 23 (2) (2009) 596–608.
[6] A. Canteaut, P. Charpin, G.M. Kyureghyan, A new class of monomial bent functions, Finite Fields Appl. 14 (1) (2008) 221–241.
[7] A. Caranti, F. Dalla Volta, M. Sala, On some block ciphers and imprimitive groups, Appl. Algebra Engrg. Comm. Comput. 20 (5–6) (2009) 339–350.
[8] C. De Cannière, Analysis and design of symmetric encryption algorithms, PhD thesis, Katholieke Universiteit Leuven, 2007.
[9] G. Leander, A. Poschmann, On the classification of 4 bit S-boxes, in: Proc. of WAIFI 2007, in: Lecture Notes in Comput. Sci., vol. 4547, 2007, pp. 159–176.
[10] National Institute of Standards and Technology, The Advanced Encryption Standard, FIPS 197, 2001.
[11] K.G. Paterson, Imprimitive permutation groups and trapdoors in iterated block ciphers, in: Proc. of FSE 1999, in: Lecture Notes in Comput. Sci., vol. 1636, 1999, pp. 201–214.
[12] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle, Propagation characteristics of Boolean functions, in: Proc. of EUROCRYPT 1990, in: Lecture Notes in Comput. Sci., vol. 473, 1991, pp. 161–173.
[13] V. Pulice, A security classification of Boolean functions, Master thesis, Univ. of Trento, 2011.
[14] M.J. Saarinen, Cryptographic analysis of all 4×4-bit S-boxes, in: Proc. of SAC 2011, Toronto, Canada.
[15] W. Zhang, C.-K. Wu, S. Li, Construction of cryptographically important Boolean permutations, Appl. Algebra Engrg. Comm. Comput. 15 (3–4) (2004) 173–177.