On highly nonlinear S-boxes and their inability to thwart DPA attacks (completed version)

Claude Carlet

INRIA, Projet CODES, BP 105 - 78153, Le Chesnay Cedex, FRANCE;
claude.carlet@inria.fr; also member of the University of Paris 8 (MAATICAH).

Abstract. Prouff has introduced recently, at FSE 2005, the notion of transparency order of S-boxes. This new characteristic is related to the ability of an S-box, used in a cryptosystem in which the round keys are introduced by addition, to thwart single-bit or multi-bit DPA attacks on the system. If this parameter has sufficiently small value, then the S-box is able to withstand DPA attacks without that ad-hoc modifications in the implementation be necessary (these modifications make the encryption about twice slower). We prove lower bounds on the transparency order of highly nonlinear S-boxes. We show that some highly nonlinear functions (in odd or even numbers of variables) have very bad transparency orders: the inverse functions (used as S-box in the AES), the Gold functions and the Kasami functions (at least under some assumption).

1 Introduction

Block cipher cryptosystems embedded in cryptographic devices are sensitive to a series of cryptanalyses such as differential and linear attacks. Much is known on the desired characteristics (balancedness, high nonlinearity or high algebraic degree) of their S-boxes which permit an optimal resistance to these attacks. But these cryptosystems and their implementation must also withstand the attacks on the hardware. Indeed, one can obtain information from the side channels in evaluating the timing of operations or their power consumption. The first side channel attack, introduced by Kocher [21], permitted to obtain the whole secret key in several cryptosystems (more precisely, in the implementation of these cryptosystems), thanks to a timing of operations. Since this seminal paper, a large number of very efficient attacks has been performed on various cryptographic implementations (see e.g. [7, 8, 15, 17, 24, 25]), in particular in implementations for smart cards. The *differential power analysis* (DPA) is one of the most powerful such methods. Its efficiency is much greater than that of linear or differential cryptanalyses. For instance, in the case of DES, a DPA attack needs about 2000 bytes of plaintext-ciphertext pairs, whereas linear or differential attacks need terabytes of such pairs (encrypted with a single key, or twice as many encrypted with several keys, this makes them completely unpractical in most situations, and in particular in the case of embedded cryptography, which is the most favourable situation for DPA attacks). Fortunately, countermeasures to DPA attacks exist, that can be added to the implementation to withstand these attacks; for example, adding computations which are not necessary for the encryption itself, or enciphering data so that the attacker has no information on the input to the S-box [9, 13, 15, 29]. But these countermeasures make the code size and the complexity of computation greater. This is a concern in the area of embedded cryptography, because of limited power and memory capability, and it slows down the encryption by a factor of 2, roughly. A potentially better method would be to choose the S-boxes so that they permit a high resistance to linear and differential cryptanalyses and to DPA attacks as well. But is this possible? To study such possibility, E. Prouff, extending in [28] the study made by Guilley et al. [16] for the so-called single-bit DPA, has introduced a new characteristic for S-boxes used in block cryptosystems in which the round keys are introduced by addition: the transparency order. This extension by Prouff to several coordinate functions of the S-box instead of just one (or of a linear combination of the coordinate functions) shows that the transparency order must not be greater that some value, depending on the amount of noise inside the device and on the number of encryptions that a cryptanalyst can obtain with the same key. The introduction of this parameter is interesting, as a first attempt at theoretically characterizing and quantifying the resistance of S-boxes to DPA attacks. Obviously, it would be nice if we could exhibit S-boxes with reasonably high nonlinearities and with low transparency orders; unfortunately, this is still an open problem. Prouff shows that the transparency order of an S-box F is null if the S-box is a (cryptographically useless) affine function of a certain type and that it is the worst possible when the coordinate functions of F are all bent. He also proves that the transparency order of a function satisfying the propagation criterion of high degree has bad value. However, this gives information on the behavior of particular S-boxes, only. We show in the present paper that the most important of those S-boxes currently used in cryptosystems - namely the inverse function, used as S-box in the AES - has a very bad transparency order. This may not mean that the use of inverse S-box is going to diminish because of this. But it proves what was only believed true without proof before: the countermeasures cannot be avoided with this precise S-box. We are able to obtain this result thanks to bounds on the transparency order which relate it to the Walsh spectra of the functions. We prove that the transparency order of the Kasami function is bad too. We calculate, for n odd and for n even, the exact transparency order of the Gold functions (which are not used as S-boxes because of their algebraic degree) and this permits us to evaluate (at least for these functions) how precise are our bounds.

The paper is organized as follows: in Section 2, we recall some preliminaries on S-boxes (Walsh transform, APN and AB functions). In Section 3, we recall the definition of the transparency order and we prove several lower bounds. Relation (4) shows in particular that the transparency order can be lower bounded by an expression only depending on the Walsh transforms of the coordinate functions of the S-box (recall that the Walsh transform plays also a central role in the evaluation of the nonlinearity of the S-box). In Section 4, we deduce a lower bound on the transparency order of the inverse function (in a finite field of characteristic 2), and in particular of the S-box of the AES. We deduce that it cannot contribute by itself to a resistance to DPA attacks. We show the same property for the Kasami functions (at least some of them). We also calculate, for n odd and for n even, the transparency order of the Gold functions and compare it with the lower bounds obtained in Section 3.

2 Preliminaries on S-boxes

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the field $\mathbb{F}_2$. We call *n-variable Boolean function* any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and *(n,m)-function* any function $F = (f_1, \ldots, f_m)$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ (the coordinate functions f_i of F are n-variable Boolean functions). (n,m)-functions are used as S-boxes (substitution boxes) in block ciphers, often with $n = m$. An (n,m)-function is called *balanced* if its output is uniformly distributed over $\mathbb{F}_2^m$, which permits to withstand statistical attacks.

For every n-variable Boolean function f, the character sum

$$\mathcal{F}(f) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)}$$

and the related *Walsh transform* $W_f(a) = \mathcal{F}(f + l_a)$, where l_a is the linear function $l_a(x) = a{\cdot}x = a_1x_1+\ldots+a_nx_n$ (this addition being obviously calculated mod 2), play an important cryptographic role. In particular, the *nonlinearity* N_f of f equals $2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} |W_f(a)|$. The number $\max_{a\in\mathbb{F}_2^n} |W_f(a)|$ is usually called the *linearity* of f and we shall denote it by L_f. It is lower bounded by $2^{n/2}$, because of Parseval's relation $\sum_{a\in\mathbb{F}_2^n} {W_f}^2(a) = 2^{2n}$.

An n-variable Boolean function is called *bent* if its nonlinearity equals $2^{n-1} - 2^{n/2-1}$.

Another important parameter related to a Boolean function f is the autocorrelation function $AC_f(a) = \mathcal{F}(D_af)$, where D_af is the derivative of f in the direction of a:

$$D_af(x) = f(x) + f(x+a).$$

The Fourier transform of the autocorrelation function, that is, by definition, the function $\widehat{AC_f}(b) = \sum_{a\in\mathbb{F}_2^n} AC_f(a)(-1)^{a\cdot b}$, equals the square of the Walsh transform of f:

$$\widehat{AC_f}(b) = {W_f}^2(b).$$

In particular, for $b = 0$, we have:

$$\sum_{a\in\mathbb{F}_2^n} \mathcal{F}(D_af) = {W_f}^2(0).$$

The following relation will be useful in the sequel: let f and g be two n-variable Boolean functions, then

$$\sum_{a\in\mathbb{F}_2^n} \mathcal{F}(D_af)\mathcal{F}(D_ag) = 2^{-n} \sum_{a\in\mathbb{F}_2^n} {W_f}^2(a){W_g}^2(a). \tag{1}$$

Indeed, $\sum_{a\in\mathbb{F}_2^n}\mathcal{F}(D_af)\mathcal{F}(D_ag)$ is the value at 0 of the Fourier transform of the function $a\rightarrow\mathcal{F}(D_af)\mathcal{F}(D_ag)$ and it is well-known that the Fourier transform of the Hadamard product of two functions equals 2^{-n} times the convolutional product of the Fourier transforms of the functions. Hence, since the Fourier transform of AC_f equals ${W_f}^2$, we have (1).

Any (n,m)-function F (and in particular, any Boolean function) can be uniquely represented as a polynomial on n variables with coefficients in $\mathbb{F}_2^m$ of the form:

$$F(x_1,...,x_n)=\sum_{u\in\mathbb{F}_2^n}c(u)\prod_{i=1}^{n}x_i^{u_i}.$$

This representation is called the *algebraic normal form* of F and its degree $d^\circ(F)$ the *algebraic degree* of the function F.
Besides, for $m=n$, F can be identified to a function from the field $\mathbb{F}_{2^n}$ of order 2^n to itself, and has then a unique representation as a univariate polynomial of degree smaller than 2^n over this field:

$$F(x)=\sum_{i=0}^{2^n-1}c_ix^i,\quad c_i\in\mathbb{F}_{2^n}.$$

For any k, $0\le k\le 2^n-1$, the number $w_2(k)$ of nonzero coefficients $k_s\in\{0,1\}$ in the binary expansion $\sum_{s=0}^{n-1}2^sk_s$ of k is called the 2-weight of k. The algebraic degree of F is equal to the maximum 2-weight of the exponents i of the polynomial $F(x)$ such that $c_i\neq 0$.

For a function $F:\mathbb{F}_2^n\rightarrow\mathbb{F}_2^n$ and any elements $a,b\in\mathbb{F}_2^n$ we denote

$$\begin{aligned}\delta_F(a,b)&=|\{x\in\mathbb{F}_2^n: F(x+a)+F(x)=b\}|,\\ \lambda_F(a,b)&=\sum_{x\in\mathbb{F}_2^n}(-1)^{b\cdot F(x)+a\cdot x}=W_{b\cdot F}(a).\end{aligned}$$

Note that, for any $a,b\in\mathbb{F}_2^n$, the number $\delta_F(a,b)$ is even. Indeed, if x_0 is a solution of $F(x+a)+F(x)=b$ then x_0+a is a solution too.
The function λ_F is often called the Walsh transform of F. The *nonlinearity* N_F of F is the minimum nonlinearity of all the nonzero linear combinations $b\cdot F$, $b\neq 0$, of its coordinate functions; hence it equals $2^{n-1}-\frac{1}{2}\max_{a,b\in\mathbb{F}_2^n;b\neq 0}|\lambda_F(a,b)|$. The multi-set of the values $\lambda_F(a,b)$, $a,b\in\mathbb{F}_2^n$ does not depend on a particular choice of the inner product in $\mathbb{F}_2^n$. If we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ then we can take $x\cdot y=tr(xy)$, where $tr(x)=x+x^2+...+x^{2^{n-1}}$ is the trace function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$.
We also denote

$$\begin{aligned}\Delta_F&=\{\delta_F(a,b):a,b\in\mathbb{F}_2^n,a\neq 0\},\\ \Lambda_F&=\{\lambda_F(a,b):a,b\in\mathbb{F}_2^n,b\neq 0\}.\end{aligned}$$

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called *almost perfect nonlinear* (APN) if $\varDelta_F = \{0, 2\}$. A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called *almost bent* (AB) or *maximum nonlinear* if $\varLambda_F = \{0, \pm 2^{\frac{n+1}{2}}\}$. Obviously, AB functions exist only for n odd.

APN and AB functions are used in cryptography in block ciphers because APN mappings possess the best resistance against the differential cryptanalysis [1] and AB mappings oppose an optimum resistance to both linear [23] and differential attacks.

For affinely equivalent functions F and $F' = L \circ F \circ L'$ (where L and L' are two affine isomorphisms), we have $\varDelta_F = \varDelta_{F'}$, $\varLambda_F = \varLambda_{F'}$ and if F is a permutation then $\varDelta_F = \varDelta_{F^{-1}}$, $\varLambda_F = \varLambda_{F^{-1}}$ [5]. Therefore, if F is APN (resp. AB) and F' is affinely equivalent to either F or F^{-1} (if F is a permutation), then F' is also APN (resp. AB).

Table 1 (resp. Table 2) gives all known values of exponents d (up to affine equivalence and up to taking the inverse when a function is a permutation) such that the power function x^d is APN (resp. AB).

Table 1
Known APN power functions on $\mathbb{F}_{2^n}$.

	Exponents d	Conditions	Proven in
Gold functions	$2^i + 1$	$gcd(i, n) = 1$, $1 \le i \le \frac{n-1}{2}$	[27]
Kasami functions	$2^{2i} - 2^i + 1$	$gcd(i, n) = 1$, $1 \le i \le \frac{n-1}{2}$	[20],[19]
Welch function	$2^t + 3$	$n = 2t + 1$	[11]
Niho function	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[14]
Inverse function	$2^{2t} - 1$	$n = 2t + 1$	[27]
Dobbertin function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	[12]

Table 2
Known AB power functions on $\mathbb{F}_{2^n}$, n odd.

	Exponents d	Conditions	Proven in
Gold functions	$2^i + 1$	$gcd(i, n) = 1$, $1 \le i \le \frac{n-1}{2}$	[27]
Kasami functions	$2^{2i} - 2^i + 1$	$gcd(i, n) = 1$, $1 \le i \le \frac{n-1}{2}$	[20]
Welch function	$2^t + 3$	$n = 2t + 1$	[3]
Niho function	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[18]

Every AB function is APN [6]. The converse is not true, even when n is odd. A counterexample is given by the inverse APN function, which has the algebraic degree $n - 1$ while the algebraic degree of any AB function is not greater than $(n + 1)/2$ [5].

The inverse function is not APN when n is even, but it is almost APN in the sense that $\varDelta_F = \{0, 2, 4\}$ (we say that it is differentially 4-uniform). It has been chosen (as elementary block) in the S-box of the AES, with $n = 8$. It has nonlinearity $2^{n-1} - 2^{n/2}$, see [22, 26]. This value is the best known nonlinearity when n is even (see [4] for a list of all known permutations with the same nonlinearity) and knowing whether there exist (n, n)-functions with nonlinearity strictly greater than this value is an open question (even for power functions).

Other APN and AB functions have been recently found, which are not equivalent to power functions, see [2].

3 The transparency order

In [28], E. Prouff introduced a new characteristic for S-boxes in block cryptosystems. The *transparency order* of an S-box $F=(f_1,\dots,f_n)$ on $\mathbb{F}_2^n$ is the number:

$$\mathcal{T}_F=\max_{b\in\mathbb{F}_2^n}\left(|n-2w_H(b)|-\frac{1}{2^{2n}-2^n}\sum_{a\in\mathbb{F}_2^{n\,*}}\left|\sum_{i=1}^{n}(-1)^{b_i}\mathcal{F}(D_af_i)\right|\right). \qquad (2)$$

In this definition (which also exists for (n,m)-functions, but we shall study here the case $m=n$ only), the expression inside the brackets is positive for $w_H(b)=0$ and for $w_H(b)=n$, and it is upper bounded by n for every b. Hence, as observed in [28], we have $0\le\mathcal{T}_F\le n$. As also observed by Prouff, if the coordinate functions f_i of F are bent, then F has obviously worst possible transparency order n. However, nothing more is said in [28] on the relationship between the transparency order and the (non)linearities of the f_i's (it seems quite logical that any non-linear S-box will be rather bad against this property, but this has to be proven). We show below four bounds relating the transparency order to the Walsh transforms of the coordinate functions. Bound (3) implies (4) which implies (5) which implies in its turn (6). Bound (5) (resp. bound (6)) shows in particular that, to have a chance of obtaining a good transparency order, two kinds of parameters play a role: the nonlinearities of the coordinate functions (resp. the nonlinearity of the S-box), which would better be not too high, and the sizes of the Walsh supports of these functions and the sizes of the pairwise intersections of these supports.

Theorem 1. *Let $F=(f_1,\dots,f_n)$ be any (n,n)-function. For every $i=1,\dots,n$, let S_i denote the support of the Walsh transform of f_i, that is, the set $\{a\in\mathbb{F}_2^n\,|\,W_{f_i}(a)\neq 0\}$, and let L_{f_i} denote the linearity of f_i (hence, its nonlinearity equals $2^{n-1}-\frac{1}{2}L_{f_i}$). Then, $\mathcal{T}_F$ is lower bounded by each of the following expressions:*

$$n-\frac{1}{2^n\sqrt{2^n-1}}\sqrt{\sum_{i=1}^{n}\sum_{a\in\mathbb{F}_2^{n\,*}}\mathcal{F}^2(D_af_i)+2\sum_{1\le i<j\le n}\sum_{a\in\mathbb{F}_2^{n\,*}}\mathcal{F}(D_af_i)\mathcal{F}(D_af_j)} \qquad (3)$$

$$n-\frac{1}{2^{\frac{3n}{2}}\sqrt{2^n-1}}\sqrt{\sum_{i=1}^{n}\sum_{a\in\mathbb{F}_2^{n}}W_{f_i}^4(a)+2\sum_{1\le i<j\le n}\sum_{a\in\mathbb{F}_2^{n}}W_{f_i}^2(a)W_{f_j}^2(a)-n^2\,2^{3n}} \qquad (4)$$

$$n-\frac{1}{2^{\frac{3n}{2}}\sqrt{2^n-1}}\sqrt{\sum_{i=1}^{n}(L_{f_i}^4\,|S_i|)+2\sum_{1\le i<j\le n}(L_{f_i}^2\,L_{f_j}^2\,|S_i\cap S_j|)-n^2\,2^{3n}}, \qquad (5)$$

where "$|\ |$" denotes the size. Consequently, denoting by N_F the nonlinearity of F, and by L_F its linearity (such that $N_F=2^{n-1}-\frac{1}{2}L_F$), $\mathcal{T}_F$ is lower bounded by:

$$n-\frac{1}{2^{3n/2}\sqrt{2^n-1}}\left(\left(\sum_{i=1}^{n}|S_i|+2\sum_{1\le i<j\le n}|S_i\cap S_j|\right)L_F^4-n^2\,2^{3n}\right)^{1/2}. \qquad (6)$$

Proof: Applying Cauchy-Schwartz' inequality, we have:

$$\sum_{a\in\mathbb{F}_2^{n*}}\left|\sum_{i=1}^{n}(-1)^{b_i}\mathcal{F}(D_af_i)\right|\leq\left((2^n-1)\sum_{a\in\mathbb{F}_2^{n*}}\left(\sum_{i=1}^{n}(-1)^{b_i}\mathcal{F}(D_af_i)\right)^2\right)^{1/2}.$$

The sum:

$$\sum_{a\in\mathbb{F}_2^{n*}}\left(\sum_{i=1}^{n}(-1)^{b_i}\mathcal{F}(D_af_i)\right)^2$$

equals

$$\sum_{i=1}^{n}\sum_{a\in\mathbb{F}_2^{n*}}\mathcal{F}^2(D_af_i)+2\sum_{1\leq i<j\leq n}(-1)^{b_i+b_j}\sum_{a\in\mathbb{F}_2^{n*}}\mathcal{F}(D_af_i)\mathcal{F}(D_af_j).$$

Taking for b the null vector or the all-one vector, we get (3).
According to Relation (1), the sum $\sum_{a\in\mathbb{F}_2^{n*}}\left(\sum_{i=1}^{n}\mathcal{F}(D_af_i)\right)^2$, that is equal to the expression:
$\sum_{i=1}^{n}\sum_{a\in\mathbb{F}_2^n}\mathcal{F}^2(D_af_i)+2\sum_{1\leq i<j\leq n}\sum_{a\in\mathbb{F}_2^n}\mathcal{F}(D_af_i)\mathcal{F}(D_af_j)-n^2\,2^{2n}$, equals then:

$$2^{-n}\sum_{i=1}^{n}\sum_{a\in\mathbb{F}_2^n}{W_{f_i}}^4(a)+2^{-n+1}\sum_{1\leq i<j\leq n}\sum_{a\in\mathbb{F}_2^n}{W_{f_i}}^2(a){W_{f_j}}^2(a)-n^2\,2^{2n}.$$

This proves (4), and we deduce (5) and (6) since $W_{f_i}^2(a)\leq L_{f_i}^2$, for every a and for every i, and since $L_{f_i}\leq L_F$ for every i. ◇

Remarks:
1. When the f_i's are bent, all of the expressions (3) to (6) equal $\mathcal{T}_F=n$, since for every i, $|S_i|$ equals then 2^n, L_{f_i} equals $2^{n/2}$, and for every i,j, $|S_i\cap S_j|$ equals 2^n.
2. Relation (4) gives

$$\mathcal{T}_F\geq n-\frac{1}{2^{3n/2}\sqrt{2^n-1}}\left(\sum_{a\in\mathbb{F}_{2^n}}\left(\sum_{i=1}^{n}{W_{f_i}}^2(a)\right)^2-n^2\,2^{3n}\right)^{1/2}.\qquad(7)$$

4 Power permutations

Bounds (3), (4), (5) and (6) seem complicated and we can wonder whether they can ever be computed. We shall show that, in the case of power permutations, their complexity decreases and that their computation can be done at least in the cases of Gold functions and of inverse function (see Section 5).
The coordinate functions of a power function x^d have the form $f_i(x)=tr(b_ix^d)$, where the b_i's are linearly independent. Set $b\neq 0$. Assuming that d is co-prime

with 2^n-1 (i.e. that the power function is a permutation), the character sum $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr(bx^d+ax)}$ equals

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr\left(b\left(\frac{x}{b^{1/d}}\right)^d+a\left(\frac{x}{b^{1/d}}\right)\right)}=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr\left(x^d+\left(\frac{a}{b^{1/d}}\right)x\right)},$$

where $1/d$ denotes the inverse of d mod 2^n-1. Hence, denoting the function $tr(bx^d)$ by f_b, and the function $tr(x^d)$ by f, we have

$$W_{f_b}(a)=W_f\left(\frac{a}{b^{1/d}}\right), \tag{8}$$

and the support of W_{f_b} equals $b^{1/d}S$, where S is the support of W_f.

Hence $\sum_{b\in\mathbb{F}_{2^n}^*}\sum_{a\in\mathbb{F}_{2^n}}W_{f_b}^4(a)=(2^n-1)\sum_{a\in\mathbb{F}_{2^n}}W_f^4(a)$.

It is well-known that $\sum_{b\in\mathbb{F}_{2^n}}\sum_{a\in\mathbb{F}_{2^n}}W_{f_b}^4(a)$ equals 2^{2n} times the size of the set $\{(x,y,z)\in\mathbb{F}_{2^n}^3\,|\,x^d+y^d+z^d+(x+y+z)^d=0\}$. Indeed, we have

$$\sum_{b\in\mathbb{F}_{2^n}}\sum_{a\in\mathbb{F}_{2^n}}W_{f_b}^4(a)=$$

$$\sum_{b\in\mathbb{F}_{2^n}}\sum_{a\in\mathbb{F}_{2^n}}\sum_{x,y,z,t\in\mathbb{F}_{2^n}}(-1)^{tr(b(x^d+y^d+z^d+t^d)+a(x+y+z+t))}=$$

$$\sum_{x,y,z,t\in\mathbb{F}_{2^n}}\left(\sum_{b\in\mathbb{F}_{2^n}}(-1)^{tr(b(x^d+y^d+z^d+t^d))}\right)\left(\sum_{a\in\mathbb{F}_{2^n}}(-1)^{tr(a(x+y+z+t))}\right),$$

and the sum $\sum_{b\in\mathbb{F}_{2^n}}(-1)^{tr(b(x^d+y^d+z^d+t^d))}$ is null if $x^d+y^d+z^d+t^d\neq 0$ (resp. the sum $\sum_{a\in\mathbb{F}_{2^n}}(-1)^{tr(a(x+y+z+t))}$ is null if $x+y+z+t\neq 0$).
Since the condition $x^d+y^d+z^d+(x+y+z)^d=0$ is satisfied under the sufficient condition that two elements among x,y and z are equal (the number of such cases equals $3\cdot 2^{2n}-2^{n+1}$), $\sum_{a\in\mathbb{F}_{2^n}}W_f^4(a)$ is therefore lower bounded by $\frac{1}{2^n-1}\left(2^{2n}\cdot(3\cdot 2^{2n}-2^{n+1})-\sum_{a\in\mathbb{F}_{2^n}}W_0^4(a)\right)=\frac{1}{2^n-1}\left(2^{2n}\cdot(3\cdot 2^{2n}-2^{n+1})-2^{4n}\right)=2^{3n+1}$, as well as $\sum_{a\in\mathbb{F}_{2^n}}W_{f_b}^4(a)$, for every $b\neq 0$. We deduce:

Lemma 1. *If $F=(f_1,\ldots,f_n)$ is a power permutation, then*

$$\sum_{i=1}^{n}\sum_{a\in\mathbb{F}_{2^n}}W_{f_i}^4(a)=$$

$$\frac{n\,2^{2n}}{2^n-1}\left(|\{(x,y,z)\in\mathbb{F}_{2^n}^3\,|\,x^d+y^d+z^d+(x+y+z)^d=0\}|-2^{2n}\right)\geq$$

$$n\cdot 2^{3n+1}.$$

If x^d is APN, then the condition $x^d+y^d+z^d+(x+y+z)^d=0$ is satisfied if and only if two elements among x, y and z are equal, and $\sum_{a\in\mathbb{F}_{2^n}} W_f^4(a)$ equals 2^{3n+1}, as well as $\sum_{a\in\mathbb{F}_{2^n}} W_{f_b}^4(a)$, for every $b\neq 0$. Hence $\sum_{i=1}^n \sum_{a\in\mathbb{F}_{2^n}} W_{f_i}^4(a) = n\cdot 2^{3n+1}$.

Let us consider now, for $c\notin\mathbb{F}_2$, the sum $\sum_{a\in\mathbb{F}_{2^n}} {W_f}^2(a){W_{f_c}}^2(a)$ involved in (4). According to (8), it is equal to $\frac{1}{2^n-1}$ times

$$\sum_{b\in\mathbb{F}_{2^n}^*}\sum_{a\in\mathbb{F}_{2^n}} W_{f_b}^2(a)W_{f_b}^2\left(\frac{a}{c^{1/d}}\right)=$$

$$\sum_{b\in\mathbb{F}_{2^n}^*}\sum_{a\in\mathbb{F}_{2^n}} W_{f_b}^2(a)W_{f_{bc}}^2(a)=$$

$$\left(\sum_{b\in\mathbb{F}_{2^n}}\sum_{a\in\mathbb{F}_{2^n}}\sum_{x,y,z,t\in\mathbb{F}_{2^n}}(-1)^{tr(b(x^d+y^d+cz^d+ct^d)+a(x+y+z+t))}-2^{4n}\right).$$

Hence, we have:

Lemma 2. *If $F(x)=x^d$ is a power permutation and $f(x)=tr(F(x))$, $f_c(x)=tr(cF(x))$, $c\notin\mathbb{F}_2$, then*

$$\sum_{a\in\mathbb{F}_{2^n}} {W_f}^2(a){W_{f_c}}^2(a)= \tag{9}$$

$$\frac{2^{2n}}{2^n-1}\left(|\{(x,y,z)\in{\mathbb{F}_{2^n}}^3\,|\,x^d+y^d+cz^d+c(x+y+z)^d=0\}|-2^{2n}\right).$$

There does not seem to exist a nice general lower bound on this expression, even when x^d is APN (taking $x=y$ only leads only to the positivity of $\sum_{a\in\mathbb{F}_{2^n}} {W_f}^2(a){W_{f_c}}^2(a)$). We first consider the particular case of the inverse function.

5 The inverse function and the S-box of the AES

Let $d=2^n-2=-1$ [mod 2^n-1] (x^d equals $1/x$ if $x\neq 0$ and equals 0 if $x=0$). We know that x^d is APN when n is odd, and is not APN but is differentially 4-uniform when n is even. Its nonlinearity equals $2^{n-1}-2^{n/2}$ when n is even and it equals the highest multiple of 2 upper bounded by this number, when n is odd. Recall that this function is used with $n=8$ as the basic S-box in the AES.

In Appendix 1, we show why it seems impossible to calculate the exact value of the transparency order of the inverse function. So we must use the method initiated in the introduction of Section 4 (see Lemmas 1 and 2).

We study in Appendix 2, for any $c\neq 0$, the solutions of the equation $x^d+y^d+cz^d+c(x+y+z)^d=0$. We obtain:

- if $c=1$, then:

  - if n is odd, the number of solutions of the equation $x^d + y^d + z^d + (x + y + z)^d = 0$ equals $2^{2n} + 4(2^n - 1) + 2(2^n - 1)(2^n - 2) = 3 \cdot 2^{2n} - 2^{n+1}$; we calculated already this number (the function is APN);
  - if n is even, the number of solutions of the equation $x^d + y^d + z^d + (x + y + z)^d = 0$ equals $2^{2n} + 8(2^n - 1) + 2(2^n - 1)(2^n - 2) = 3 \cdot 2^{2n} + 2^{n+1} - 4$, since $tr(1) = 0$; this number could have also been calculated by using the results of Nyberg [27].
- if $c \neq 1$, then
  - if $tr(c) = tr(1/c) = 0$, the number of solutions of the equation $x^d + y^d + cz^d + c(x + y + z)^d = 0$ equals $2^{2n} + 4(2^n - 1) + 4(2^n - 1) + 2(2^n - 1)(2^{n-1} - 2) = 2 \cdot 2^{2n} + 3 \cdot 2^n - 4$
  - if $tr(c) = 0$ and $tr(1/c) = 1$ or if $tr(c) = 1$ and $tr(1/c) = 0$, the number of solutions of the equation $x^d + y^d + cz^d + c(x + y + z)^d = 0$ equals $2^{2n} + 4(2^n - 1) + 2(2^n - 1)(2^{n-1} - 2) = 2 \cdot 2^{2n} - 2^n$
  - if $tr(c) = tr(1/c) = 1$, the number of solutions of the equation $x^d + y^d + cz^d + c(x+y+z)^d = 0$ equals $2^{2n} + 2(2^n - 1)(2^{n-1} - 2) = 2 \cdot 2^{2n} - 5 \cdot 2^n + 4$.

Note that, in the case $c \neq 1$, the greatest number that we have obtained is $2 \cdot 2^{2n} + 3 \cdot 2^n - 4$. According to Relation (9), we deduce that Bound (4) gives, if n is odd:

$$\mathcal{T}_{\mathcal{F}} \geq$$

$$n - \left(\frac{n(2 \cdot 2^{2n} - 2^{n+1}) + n(n-1)(2^{2n} + 3 \cdot 2^n - 4)}{2^n(2^n - 1)^2} - \frac{n^2}{(2^n - 1)} \right)^{1/2} =$$

$$n - \frac{1}{2^{n/2}(2^n - 1)} \left(4n^2(2^n - 1) + n(2^{2n} - 5 \cdot 2^n + 4) \right)^{1/2} \approx n - \sqrt{\frac{n}{2^n}}$$

and if n is even:

$$\mathcal{T}_{\mathcal{F}} \geq$$

$$n - \left(\frac{n(2 \cdot 2^{2n} + 2^{n+1} - 4) + n(n-1)(2^{2n} + 3 \cdot 2^n - 4)}{2^n(2^n - 1)^2} - \frac{n^2}{(2^n - 1)} \right)^{1/2} =$$

$$n - \frac{1}{2^{n/2}(2^n - 1)} \left(4n^2(2^n - 1) + n(2^{2n} - 2^n) \right)^{1/2} \approx n - \sqrt{\frac{n}{2^n}}.$$

Hence, the inverse function has bad transparency order! In particular, in the case of the S-box of the AES ($n = 8$), our bound gives that $\mathcal{T}_{\mathcal{F}} \geq 7.8$, which is close to $n = 8$.

6 The Gold functions

The exact value of the transparency order of the Gold functions can be calculated. For $F(x) = x^{2^i+1}$ ($\gcd(i,n)$=1), taking $b \neq 0$ and $a \neq 0$, we have $f_b(x) = tr(bx^{2^i+1})$, $D_a f_b(x) = tr(bax^{2^i} + ba^{2^i}x + ba^{2^i+1}) = tr(((ba)^{2^{n-i}} + ba^{2^i})x + ba^{2^i+1})$ and $\mathcal{F}(D_a f_b)$ equals $\pm 2^n$ if $(ba)^{2^{n-i}} + ba^{2^i} = 0$ and is null otherwise. We have $(ba)^{2^{-i}} + ba^{2^i} = 0$ if and only if $ba + b^{2^i} a^{2^{2i}} = 0$, that is, if and only if $b^{2^i-1}a^{2^{2i}-1} = 1$, or equivalently $ba^{2^i+1} = 1$, since $\gcd(i,n)$=1. Hence, for every $a \neq 0$, there exists exactly one $b \neq 0$ such that $\mathcal{F}(D_a f_b) \neq 0$, and therefore at most one i such that $\mathcal{F}(D_a f_i) \neq 0$. We deduce that $\mathcal{T}_F$ equals in fact $n - \frac{1}{2^{2n}-2^n} \sum_{a \in \mathbb{F}_2^{n\,*}} \sum_{i=1}^n |\mathcal{F}(D_a f_i)| = n - \frac{1}{2^{2n}-2^n} \sum_{i=1}^n \Big(\sum_{a \in \mathbb{F}_2^{n\,*}} |\mathcal{F}(D_a f_i)| \Big)$. Note that this observation is valid whatever is the evenness of n. When n is odd, F is a permutation. For every $b \neq 0$, there exists then a unique $a \neq 0$ such that $ba^{2^i+1} = 1$ and we deduce

$$\mathcal{T}_F = n - \frac{n2^n}{2^{2n}-2^n} = n - \frac{n}{2^n-1}.$$

When n is even, there exists $a \in \mathbb{F}_2^{n\,*}$ such that $ba^{2^i+1} = 1$ if and only if $b \in \{y^{2^i+1};\, y \in \mathbb{F}_2^{n\,*}\}$. We have $\gcd(2^i+1, 2^n-1) = \gcd((2^i+1)(2^i-1), 2^n-1) = \gcd(2^{2i}-1, 2^n-1) = 3$. Hence, there exists $a \in \mathbb{F}_2^{n\,*}$ such that $ba^{2^i+1} = 1$ if and only if $b \in \{y^3;\, y \in \mathbb{F}_2^{n\,*}\}$. In such case, given a solution a_0 of the equation $ba^{2^i+1} = 1$, the other solutions are those elements a such that $\left(\frac{a}{a_0}\right)^{2^i+1} = 1$, that is $\left(\frac{a}{a_0}\right)^3 = 1$, i.e. $\frac{a}{a_0} \in F_4^*$. We deduce that $\mathcal{T}_F$ equals $n - \frac{3n \cdot 2^n}{2^{2n}-2^n} = n - \frac{3n}{2^n-1}$ when all the b_i chosen for defining the coordinate functions of F belong to $\{y^3;\, y \in \mathbb{F}_2^{n\,*}\}$ and equals n when none of them is in this case (i.e. when all the coordinate functions are bent). We see that the transparency order of Gold functions is bad too. These functions had already the drawback of having low degree.

The fact that we could calculate the exact value of $\mathcal{T}_F$ in the case of Gold functions is an opportunity of seeing whether, at least in this case, our bound (6) is good or not. Let us consider for instance the case when n is odd. It is well known that the support of the Walsh transform of the function $tr(x^{2^i+1})$ (n odd, $\gcd(i,n) = 1$) equals $H = \{a \in \mathbb{F}_{2^n} \,|\, tr(a) = 1\}$. Indeed, since function $tr(x^{2^i+1})$ is quadratic (i.e. has degree 2), for every $a \in \mathbb{F}_{2^n}$, the function $tr(x^{2^i+1}) + tr(ax)$ is unbalanced if and only if its restriction to the kernel of its associated symplectic form, that is, the vectorspace $E = \{x \in \mathbb{F}_{2^n} \,|\, \forall y \in \mathbb{F}_{2^n}, tr(x^{2^i+1}) + tr(y^{2^i+1}) + tr((x+y)^{2^i+1}) = 0\}$, is constant. We have $E = \{x \in \mathbb{F}_{2^n} \,|\, x^{2^i} + x^{2^{n-i}} = 0\} = \{x \in \mathbb{F}_{2^n} \,|\, x^{2^{2i}} + x = 0\} = \{0\} \cup \{x \in \mathbb{F}_{2^n}{}^* \,|\, x^{2^{2i}-1} = 1\} = \{0,1\}$. Hence, $W_f(a)$ is null if and only if $tr(a) = 0$. It is a simple matter to see that, for every $k \neq j$, we have $|b_j^{1/(2^i+1)}\, H \cap b_k^{1/(2^i+1)}\, H| = 2^{n-2}$, since the b_j's are nonzero and pairwise distinct. We deduce that Relation (6) gives

$$\begin{aligned}\mathcal{T}_F &\geq n - \frac{1}{2^{3n/2}\sqrt{2^n-1}} \left(\left(n\, 2^{n-1} + n(n-1)\, 2^{n-2} \right) 2^{2n+2} - n^2\, 2^{3n} \right)^{1/2} \\ &= n - \sqrt{\frac{n}{2^n-1}}.\end{aligned}$$

The difference between $\mathcal{T}_F = n - \frac{n}{2^n-1}$ and $n - \sqrt{\frac{n}{2^n-1}}$ is negligible with respect to $\mathcal{T}_F$.

7 The Kasami functions

It has been proved by Dillon and Dobbertin in [10] that, if $3i$ is congruent with 1 mod n, then the Walsh support of the Kasami Boolean function $tr(x^{2^{2i}-2^i+1})$, that we shall denote in this subsection by $f(x)$, equals $\{x \in F_{2^n} \,|\, tr(x^{2^i+1}) = 1\}$ (that is, equals the support of the Gold function) if n is odd and equals the set $\{x \in F_{2^n} \,|\, Tr_{n/2}(x^{2^i+1}) = 0\}$ if n is even, where $Tr_{n/2}$ is the trace function from F_{2^n} to the field F_{2^2}: $Tr_{n/2}(x) = x + x^4 + x^{4^2} + \ldots + x^{4^{n/2-1}}$. We shall show (see the next remark) that, when n is odd, that is, when the Kasami function is a permutation (and is almost bent), this permits to calculate the magnitude of the auto-correlation of f and to deduce a lower bound on its transparency order. But, since we do not know the sign of the auto-correlation of f, this does not seem to allow the exact calculation of its transparency order, and it leads in fact to a weak bound! A better bound is obtained by using Relation (6).

Case n odd : the Walsh support of f being equal to the support of the Gold function, and the Kasami and the Gold functions being both permutations, Relation (8) implies that, for every i, we have $|S_i| = 2^{n-1}$, and for every $i < j$, we have $|S_i \cap S_j| = 2^{n-2}$ (as also mentioned by Dillon and Dobbertin). So, Bound (6) gives the same result as for the Gold function: $\mathcal{T}_F \geq n - \sqrt{\frac{n}{2^n-1}}$.

Case n even : as also mentioned in [10], if $b_i^{2^{2i}-2^i+1} \neq 1$, $b_j^{2^{2i}-2^i+1} \neq 1$ and $i < j$, then we have $|S_i| = 2^{n-2}$ and $|S_i \cap S_j| = 2^{n-4}$. We know also that the Kasami function has linearity $2^{\frac{n}{2}+1}$. So, Bound (6) gives, if $b_i^{2^{2i}-2^i+1} \neq 1$ for every i: $\mathcal{T}_F \geq n - \sqrt{\frac{3n}{2^n-1}}$.

Remark: As recalled in the introduction, the Fourier transform of the function $AC_f : a \to \mathcal{F}(D_a f)$ equals the square of the Walsh transform of f: $\widehat{AC_f}(b) = {W_f}^2(b)$. According to Dillon's and Dobbertin's result recalled above, and since we know that the Kasami function is almost bent, ${W_f}^2(b)$ equals 2^{n+1} if $tr(b^{2^i+1}) = 1$ and equals zero otherwise. That is, ${W_f}^2(b) = 2^{n+1} tr(b^{2^i+1})$. Hence, by applying the inverse Fourier transform (that is, by applying the Fourier transform again and dividing by 2^n), AC_f equals twice the Fourier transform of the function $tr(x^{2^i+1})$. We deduce that, except at the zero vector, $AC_f(a)$ equals the opposite of the Walsh transform of the function $tr(x^{2^i+1})$. We have seen that this Walsh transform has support $H = \{a \in \mathbb{F}_{2^n} \,|\, tr(a) = 1\}$. It is well-known and easy to check that the value of this Walsh transform at every element of its support equals $\pm 2^{\frac{n+1}{2}}$. Unfortunately, we do not know what is the sign, and this leads only to an upper bound which is weaker than above: we have, for every nonzero a, we have

$$|\mathcal{F}(D_a f)| = 2^{\frac{n+1}{2}} \text{ if } tr(a) = 1;\ \mathcal{F}(D_a f) = 0 \text{ otherwise.}$$

This implies that, for every $b \neq 0$, we have $|\mathcal{F}(D_a f_b)| = 2^{\frac{n+1}{2}}$ if $tr\left(\frac{a}{b^{1/d}}\right) = 1$, where $d = 2^{2i} - 2^i + 1$; $\mathcal{F}(D_a f_b) = 0$ otherwise. We deduce:

$$\mathcal{T}_F \geq n - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{i=1}^{n} |\mathcal{F}(D_a f_i)| = n - \frac{1}{2^{2n} - 2^n} \sum_{i=1}^{n} \sum_{a \in \mathbb{F}_2^{n*}} |\mathcal{F}(D_a f_i)| =$$

$$n - \frac{2^{\frac{n+1}{2}}}{2^{2n} - 2^n} \sum_{i=1}^{n} card\left\{ a \in \mathbb{F}_2^{n*} \,|\, tr\left(\frac{a}{b_i^{1/d}}\right) = 1 \right\} = n - \frac{2^{\frac{n+1}{2}} 2^{n-1}}{2^{2n} - 2^n} n$$

$$\approx n\left(1 - 2^{-\frac{n+1}{2}}\right).$$

Conclusion

We were able to show that the transparency orders of three highly nonlinear S-boxes (including the S-box of the AES) are bad. This confirms the intuition that nonlinear mappings used as S-boxes may be unable to avoid using heavy countermeasures to DPA attacks (and the resulting penalties on efficiency). But it remains to show that the other functions included in tables 1 and 2 (for instance) have also bad transparency orders.

Acknowledgement

We wish to thank E. Prouff for useful discussions.

References

1. E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, vol. 4, No.1, pp. 3-72, 1991.
2. L. Budaghyan, C. Carlet and A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials. Proceedings of the Workshop on Coding and Cryptography 2005, Bergen, pp. 306-315, 2005.
3. A. Canteaut, P. Charpin and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture. *IEEE Trans. Inform. Theory*, 46 (1), pp. 4-8, 2000.
4. A. Canteaut, P. Charpin, and H. Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on GF(2^m) and crosscorrelation of maximum-length sequences. *SIAM Journal on Discrete Mathematics*, 13(1), pp. 105–138, 2000.
5. C. Carlet, P. Charpin and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2), pp. 125-156, 1998.
6. F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis, *Advances in Cryptology -EUROCRYPT'94, Lecture Notes in Computer Science*, Springer-Verlag, New York, 950, pp. 356-365, 1995.
7. S. Chari, C. Jutla, J. Rao and P. Rohatgi. Towards sound approaches to counteract power analysis attacks. CRYPTO'99, *Advances in Cryptology, Lecture Notes in Computer Science* 1666, pp. 398-412, 1999.

8. C. Clavier, J.-S. Coron and N. Dabbous. Differential power analysis in the presence of hardware countermeasures. CHES 2000, *Lecture Notes in Computer Science* 1965, pp. 252-263, 2000.
9. J.-S. Coron and L. Goubin. On Boolean and Arithmetic Masking against Differential Power Analysis. CHES00, pp. 231–237, 2000.
10. J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. Finite Fields and Their Applications 10, pp. 342-389, 2004.
11. H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case, *IEEE Trans. Inform. Theory*, 45, pp. 1271-1275, 1999.
12. H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5. D. Jungnickel and H. Niederreiter Eds. *Proceedings of Finite Fields and Applications FQ5*, Augsburg, Germany, Springer, pp. 113-121, 2000.
13. J. Golic and C. Tymen. Multiplicative masking and power analysis of AES. CHES02, pp. 198–212, 2002
14. H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case, *Inform. and Comput.*, 151, 57-72, 1999.
15. L. Goubin and J. Patarin. DES and differential power analysis - the duplication method. CHES'99, *Lecture Notes in Computer Science* 1717, pp. 158-172, 1999.
16. S. Guilley, P. Hoogvorst and R. Pascalet. Differential power analysis model and some results. Smart Card Research ann Advanced Applications VI - Cardis 2004, *Kluwer Academic Publishers*, pp. 127-142, 2004.
17. A. A. Hasan. Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz cryptosystems. CHES 2000, *Lecture Notes in Computer Science* 1965, pp. 93-108, 2000.
18. H. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences. *Finite Fields and Their Applications 7*, pp. 253-286, 2001.
19. H. Janwa and R. Wilson. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. *Proceedings of AAECC-10, Lecture Notes in Computer Science*, vol. 673, Berlin, Springer-Verlag, pp. 180-194, 1993.
20. T. Kasami. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. *Inform. and Control*, 18, pp. 369-394, 1971.
21. P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems. CRYPTO'96, *Advances in cryptology, Lecture Notes in Computer Science* 1109, pp. 104-113, 1996.
22. G. Lachaud and J. Wolfmann. The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. *IEEE Trans. Inform. Theory*, vol. 36, pp. 686-692, 1990.
23. M. Matsui. Linear cryptanalysis method for DES cipher. *Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science*, Springer-Verlag, pp.386-397, 1994.
24. R. Mayer Sommer. Smartly analysing the simplicity and the power of simple power analysis on smartcards. CHES 2000, *Lecture Notes in Computer Science* 1965, pp. 78-92, 2000.
25. T. Messerges, E. Dabbish and R. Sloan. Power analysis attacks on smartcards. CHES'99, *Lecture Notes in Computer Science* 1717, pp. 144-157, 1999.
26. K. Nyberg. On the construction of highly nonlinear permutations. *Advances in Cryptology, EUROCRYPT' 92, Springer Verlag, Lecture Notes in Computer Science* 658, pp. 92-98, 1993.

27. K. Nyberg. Differentially uniform mappings for cryptography, *Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science*, Springer-Verlag, New York, 765, pp. 55-64, 1994.
28. E. Prouff. DPA attacks and S-boxes. FSE 2005, *Lecture Notes in Computer Science* 3557, pp. 424-441, 2005.
29. E. Trichina and D. DeSeta and L. Germani. Simplified Adaptive Multiplicative Masking for AES. CHES'02, pp. 187–197, 2002.

Appendix 1

In this appendix, we see whether it is possible to calculate the exact value of $\mathcal{T}_F$ when $F(x)$ is the inverse function x^{-1}, equal to $\frac{1}{x}$ if $x \neq 0$ and to 0 if $x = 0$. For every $a, b \neq 0$, we have $D_a f_b(x) = tr\left(\frac{ab}{x(x+a)}\right)$ if $x \neq 0, x \neq a$ and $D_a f_b(x) = tr\left(\frac{b}{a}\right)$ if $x = 0$ and if $x = a$.
Hence, $\mathcal{F}(D_a f_b)$ equals $\sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr\left(abx^{-1}(x+a)^{-1}\right)} - 2 + 2(-1)^{tr(b/a)}$, that is, by changing variable x into ax: $\sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr\left(a^{-1}b(x^2+x)^{-1}\right)} - 2 + 2(-1)^{tr(a^{-1}b)}$. Since $x^2 + x$ ranges uniformly over the hyperplane $\{u \in \mathbb{F}_{2^n} \,|\, tr(u) = 0\}$ when x ranges over $\mathbb{F}_{2^n}$, we deduce that $\mathcal{F}(D_a f_b)$ equals $2 \sum_{u \in \mathbb{F}_{2^n} \,|\, tr(u)=0} (-1)^{tr\left(a^{-1}bu^{-1}\right)} - 2 + 2(-1)^{tr(a^{-1}b)}$, that is, equals $\sum_{u \in \mathbb{F}_{2^n}} [(-1)^{tr\left(a^{-1}bu^{-1}\right)} + (-1)^{tr\left(u+a^{-1}bu^{-1}\right)}] - 2 + 2(-1)^{tr(a^{-1}b)}$, that is, changing u into $ab^{-1}u$:

$$\mathcal{F}(D_a f_b) = \sum_{u \in \mathbb{F}_{2^n}} (-1)^{tr\left(u^{-1}\right)} + \sum_{u \in \mathbb{F}_{2^n}} (-1)^{tr\left(ab^{-1}u + u^{-1}\right)} - 2 + 2(-1)^{tr(a^{-1}b)}.$$

Since x^{-1} is a permutation, the first of these two sums is null. The second one is known under the name of *Kloosterman* sum. It is proved in [22] that, when ab^{-1} ranges over $\mathbb{F}_{2^n}$, the set of the values of this sum equals the set of all the integers congruent with -1 modulo 4, in the range $[-2^{\frac{n}{2}+1}, 2^{\frac{n}{2}+1}]$. But the distribution of these values is not known and this gives therefore no information on the possible value of the expression inside the brackets in (2).

Appendix 2

Let us consider the equation $x^d + y^d + cz^d + c(x+y+z)^d = 0$ for any $c \neq 0$. If $x = y$, then it is satisfied. *This makes* 2^{2n} *solutions.* We study now the solutions such that $x \neq y$.
Case 1: if $z = 0$ or $z = x+y$, then the equation reduces to $x^d + y^d + c(x+y)^d = 0$.
- If $x = 0$ (and $y \neq 0$) or $y = 0$ (and $x \neq 0$), then it is satisfied if $c = 1$ and it is not satisfied if $c \neq 1$.
- If $x \neq 0$ and $y \neq 0$, it is equivalent to $\frac{1}{x} + \frac{1}{y} + \frac{c}{x+y} = 0$, that is, $x^2 + y^2 + cxy = 0$, or equivalently $\left(\frac{x}{cy}\right)^2 + \frac{x}{cy} + \frac{1}{c^2} = 0$. Thus, if $tr\left(\frac{1}{c^2}\right) = 0$, that is, if $tr\left(\frac{1}{c}\right) = 0$, then the equation admits two solutions in x, for every $y \neq 0$; note that these two solutions satisfy $x \neq 0$ and $x \neq y$, since c is nonzero. *This makes altogether* $2\ [2\ (2^n - 1) + 2\ (2^n - 1)] = 8\ (2^n - 1)$ *solutions if* $c = 1$ *and* $tr\left(\frac{1}{c}\right) = 0$ *(that*

is, if n is even), $2\ [2\ (2^n-1)] = 4\ (2^n-1)$ *if* $c=1$ *and* $tr\left(\frac{1}{c}\right)=1$ *(that is, if* n *is odd) or if* $c\neq 1$ *and* $tr\left(\frac{1}{c}\right)=0$ *and none if* $c\neq 1$ *and* $tr\left(\frac{1}{c}\right)=1$.

Case 2: if $z\neq 0$, $z\neq x+y$ and $x=0$ or $y=0$ - say $y=0$ (and $x\neq 0$), then the equation reduces to $\frac{1}{x}+\frac{c}{z}+\frac{c}{x+z}=0$, or equivalently $xz+z^2+cx^2=0$, that is, $\left(\frac{z}{x}\right)^2+\frac{z}{x}+c=0$. This last equation admits two solutions z, for every $x\neq 0$, if $tr(c)=0$ and none otherwise. Note that the two solutions, if they exist, satisfy $z\neq 0$ and $z\neq x+y=x$, since c is nonzero. *This makes altogether* $2\ (2\ (2^n-1))=4\ (2^n-1)$ *solutions if* $tr(c)=0$ *and none otherwise.*

Case 3: if $z\neq 0$, $z\neq x+y$, $x\neq 0$ and $y\neq 0$, then the equation is equivalent to $\frac{1}{x}+\frac{1}{y}+\frac{c}{z}+\frac{c}{x+y+z}=0$, that is, $(x+y+z)(yz+xz+cxy)+cxyz=0$, that is, $(x+y)(cxy+(x+y)z+z^2)=0$. Since $x\neq y$, this is equivalent to

$$\left(\frac{z}{x+y}\right)^2+\frac{z}{x+y}+\frac{cxy}{x^2+y^2}=0. \tag{10}$$

Two cases concerning x and y can occur:

- if $tr\left(\frac{cxy}{x^2+y^2}\right)=1$, then Equation (10) has no solution.

- if $tr\left(\frac{cxy}{x^2+y^2}\right)=0$, then Equation (10) has two solutions z. Note that, since x and y are distinct and nonzero, and since c is nonzero, these two solutions satisfy $z\neq 0$ and $z\neq x+y$.

Let us determine the number of ordered pairs (x,y), with x and y distinct and nonzero, such that $tr\left(\frac{cxy}{x^2+y^2}\right)=0$. We have $\frac{xy}{x^2+y^2}=\frac{x}{x+y}+\left(\frac{x}{x+y}\right)^2$, and $\frac{x}{x+y}$ ranges uniformly over $\mathbb{F}_{2^n}\setminus\mathbb{F}_2$ when (x,y) ranges over ${\mathbb{F}_{2^n}^*}^2\setminus\{(x,x); x\in\mathbb{F}_{2^n}^*\}$; hence $\frac{xy}{x^2+y^2}$ ranges uniformly over $\{u\in\mathbb{F}_{2^n}^*\,|\,tr(u)=0\}$ when (x,y) ranges over ${\mathbb{F}_{2^n}^*}^2\setminus\{(x,x); x\in\mathbb{F}_{2^n}^*\}$ (more precisely, every element $\{u\in\mathbb{F}_{2^n}^*\,|\,tr(u)=0\}$ equals $\frac{xy}{x^2+y^2}$ for $\frac{(2^n-1)(2^n-2)}{2^{n-1}-1}=2^{n+1}-2$ ordered pairs (x,y)). Thus, if $c=1$ then the condition $tr\left(\frac{cxy}{x^2+y^2}\right)=0$ is satisfied for all of the $(2^n-1)(2^n-2)$ ordered pairs (x,y), and if $c\not\in\mathbb{F}_2$, it is satisfied for $(2^{n+1}-2)(2^{n-2}-1)=(2^n-1)(2^{n-1}-2)$ ordered pairs. *This makes altogether* $2(2^n-1)(2^n-2)$ *solutions if* $c=1$ *and* $2(2^n-1)(2^{n-1}-2)$ *if* $c\not\in\mathbb{F}_2$.

Summarizing, this gives what is stated at Section 5.