A Larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction

Claude Carlet

INRIA, Domaine de Voluceau, BP 105 – 78153, Le Chesnay Cedex, France
also member of GREYC-Caen and of University of Paris 8
claude.carlet@inria.fr

Abstract. Thanks to a new upper bound, we study more precisely the nonlinearities of Maiorana-McFarland's resilient functions. We characterize those functions with optimum nonlinearities and we give examples of functions with high nonlinearities. But these functions have a peculiarity which makes them potentially cryptographically weak. We study a natural super-class of Maiorana-McFarland's class whose elements do not have the same drawback and we give examples of such functions achieving high nonlinearities.

Keywords: resilient functions, nonlinearity, stream ciphers.

1 Introduction

The Boolean functions used in stream ciphers are functions from F_2^n to F_2, where n is a positive integer. In practice, n is often small (smaller than or equal to 10), but even for small values of n, searching for the best cryptographic functions by visiting all Boolean functions in n variables is computationally impossible since their number 2^{2^n} is too large (for instance, for $n = 7$, it would need billions of times the age of the universe on a work-station). Thus, we need constructions of Boolean functions satisfying all necessary cryptographic criteria. Before describing the known constructions, we recall what are these cryptographic criteria.

Any Boolean function f in n variables (i.e. any F_2-valued function defined on the set F_2^n of all binary vectors of length n) admits a unique algebraic normal form (A.N.F.):

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i,$$

where the additions are computed in F_2, i.e. modulo 2, and where the a_I's are in F_2. We call *algebraic degree* of a Boolean function f and we denote by $d^\circ f$ the degree of its algebraic normal form. The *affine functions* are those functions of degrees at most 1. They are the simplest functions, from cryptographic viewpoint. On the contrary, *cryptographic functions must have high degrees* (cf. [3, 16, 21, 27]).

M. Yung (Ed.): CRYPTO 2002, LNCS 2442, pp. 549–564, 2002.

The *Hamming weight* $w_H(f)$ of a Boolean function f in n variables is the size of its *support* $\{x \in F_2^n;\ f(x) = 1\}$. The *Hamming distance* $d_H(f, g)$ between two Boolean functions f and g is the Hamming weight of their difference, i.e. of $f + g$ (this sum is computed modulo 2). The *nonlinearity* of f is its minimum distance to all affine functions. We denote by N_f the nonlinearity of f. *Functions used in stream ciphers must have high nonlinearities* to resist the known attacks on these ciphers (correlation and linear attacks) [3]. A Boolean function f is called *bent* if its nonlinearity equals $2^{n-1} - 2^{n/2-1}$, which is the maximum possible value (obviously, n must be even). Then, its distance to every affine function equals $2^{n-1} \pm 2^{n/2-1}$. This property can also be stated in terms of the Walsh (i.e., discrete Fourier, or Hadamard) transform of f defined on F_2^n as $\widehat{f}(u) = \sum_{x \in F_2^n} f(x)\,(-1)^{x \cdot u}$ (where $x \cdot u$ denotes the usual inner product $x \cdot u = \sum_{i=1}^n x_i\,u_i$). But it is more easily stated in terms of the Walsh transform of the "sign" function $\chi_f(x) = (-1)^{f(x)}$, equal to $\widehat{\chi_f}(u) = \sum_{x \in F_2^n} (-1)^{f(x)+x \cdot u}$: f is bent if and only if $\widehat{\chi_f}(u)$ has constant magnitude $2^{n/2}$ (cf. [14, 20]). Indeed, the Hamming distances between f and the affine functions $u \cdot x$ and $u \cdot x + 1$ are equal to $2^{n-1} - \frac{1}{2}\widehat{\chi_f}(u)$ and $2^{n-1} + \frac{1}{2}\widehat{\chi_f}(u)$. Thus:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{u \in F_2^n} |\widehat{\chi_f}(u)|. \tag{1}$$

Bent functions have degrees upper bounded by $n/2$. They are characterized by the fact that their derivatives $D_a f(x) = f(x) + f(x + a)$, $a \neq 0$, are all *balanced*, i.e. have weight 2^{n-1}. But *cryptographic functions themselves must be balanced*, so that the systems using them resist statistical attacks [21]. Bent functions are not balanced.

The last (but not least) criterion considered in this paper is resiliency. It plays a central role in stream ciphers: in the standard model of these ciphers (cf. [26]), the outputs of n linear feedback shift registers are the inputs of a Boolean function, called combining function. The output of the function produces the keystream, which is then bitwisely xored with the message to produce the cipher. Some devide-and-conquer attacks exist on this method of encryption (cf. [3, 27]). To resist these attacks, the system must use a combining function whose output distribution probability is unaltered when any m of the inputs are fixed [27], with m as large as possible. This property, called *m-th order correlation-immunity* [26], is characterized by the set of zero values in the Walsh spectrum [30]: f is m-th order correlation-immune if and only if $\widehat{\chi}_f(u) = 0$, i.e. $\widehat{f}(u) = 0$, for all $u \in F_2^n$ such that $1 \leq w_H(u) \leq m$, where $w_H(u)$ denotes the Hamming weight of the n-bit vector u, (the number of its nonzero components). Balanced m-th order correlation-immune functions are called *m-resilient* functions. They are characterized by the fact that $\widehat{\chi}_f(u) = 0$ for all $u \in F_2^n$ such that $0 \leq w_H(u) \leq m$.

Siegenthaler's inequality [26] states that any m-th order correlation immune function in n variables has degree at most $n - m$, that any m-resilient function $(0 \leq m < n - 1)$ has algebraic degree smaller than or equal to $n - m - 1$ and that any $(n - 1)$-resilient function has algebraic degree 1. Sarkar and Maitra [23] have shown that the nonlinearity of any m-resilient function ($m \leq n-2$) is divisible by 2^{m+1} and is therefore upper bounded by $2^{n-1} - 2^{m+1}$. If a function achieves this bound (independently obtained by Tarannikov [28] and Zheng and Zhang [31]), then it also achieves Siegenthaler's bound (cf. [28]) and the Fourier spectrum of the function has then three values (such functions are often called "plateaued" or "three-valued"; cf. [2]), these values are 0 and $\pm 2^{m+2}$. More precisely, it has been shown by Carlet and Sarkar [7, 8] that if f is m-resilient and has degree d, then its nonlinearity is divisible by $2^{m+1+\lfloor \frac{n-m-2}{d} \rfloor}$ and can therefore equal $2^{n-1} - 2^{m+1}$ only if $d = n - m - 1$. We shall say that an m-resilient function achieves the best possible nonlinearity if its nonlinearity equals $2^{n-1} - 2^{m+1}$. If $2^{n-1} - 2^{m+1}$ is greater than the best possible nonlinearity of all balanced functions (and in particular if it is greater than the best possible nonlinearity of all Boolean functions) then the Sarkar-Maitra-Tarannikov-Zheng-Zhang's bound can obviously be improved. In the case n is even, the best possible nonlinearity of all Boolean functions being equal to $2^{n-1} - 2^{n/2-1}$ and the best possible nonlinearity of all balanced functions being smaller than $2^{n-1} - 2^{n/2-1}$, Sarkar and Maitra deduce from their divisibility result that $N_f \leq 2^{n-1} - 2^{n/2-1} - 2^{m+1}$ for every m-resilient function f with $m \leq n/2 - 2$. In the case n is odd, they state that N_f is smaller than or equal to the highest multiple of 2^{m+1} which is less than or equal to the best possible nonlinearity of all Boolean functions, which is smaller than $2^{n-1} - 2^{n/2-1}$ (see [17] for more details). For $m \leq n/2 - 2$, a potentially better upper bound can be given, whatever is the evenness of n: Sarkar-Maitra's divisibility bound shows that $\widehat{\chi_f}(a) = \varphi(a) \cdot 2^{m+2}$ where $\varphi(a)$ is integer-valued. But Parseval's relation $\sum_{a \in F_2^n} \widehat{\chi_f}^2(a) = 2^{2n}$ and the fact that $\widehat{\chi_f}(a)$ is null for every word a of weight $\leq m$ implies $\sum_{a;\, w_H(a) > m} \varphi^2(a) = 2^{2n-2m-4}$ and thus $\max_{a \in F_2^n} |\varphi(a)| \geq \sqrt{\frac{2^{2n-2m-4}}{2^n - \sum_{i=0}^m \binom{n}{i}}} = \frac{2^{n-m-2}}{\sqrt{2^n - \sum_{i=0}^m \binom{n}{i}}}$. Thus we have $\max_{a \in F_2^n} |\varphi(a)| \geq \left\lceil \frac{2^{n-m-2}}{\sqrt{2^n - \sum_{i=0}^m \binom{n}{i}}} \right\rceil$ (where $\lceil \lambda \rceil$ denotes the smallest integer greater than or equal to λ)) and this implies $N_f \leq 2^{n-1} - 2^{m+1} \left\lceil \frac{2^{n-m-2}}{\sqrt{2^n - \sum_{i=0}^m \binom{n}{i}}} \right\rceil$. We shall call "Sarkar et al.'s bounds" all these bounds, in the sequel.

High order resilient functions with high degrees and high nonlinearities are needed for applications in stream ciphers, but designing constructions of Boolean functions meeting these cryptographic criteria is still a crucial challenge nowadays in symmetric cryptography. We observe now some imbalance in the knowledge on cryptographic functions for stream ciphers, after the results recently obtained on the properties of resilient functions [7, 8, 22, 23]. Examples of m-resilient functions achieving the best possible nonlinearities have been obtained for small values of n [19, 22, 23] and for every $m \geq 0.6\ n$ [29] (n being then not limited). But these examples give very limited numbers of functions (they are often defined recursively or obtained after a computer search) and these functions often have cryptographic weaknesses such as linear structures. Designing constructions leading to large numbers of functions would permit to choose in applications cryptographic functions satisfying specific constraints. It would also make more efficient those cryptosystems in which the cryptographic functions themselves would be part of the secret keys.

The paper is organized as follows. At section 2, we study the known constructions of resilient functions and the nonlinearities of the functions they produce. We study the nonlinearities of Maiorana-McFarland's functions more efficiently than the previous papers on this subject could do, thanks to a new upper bound that we introduce. We characterize then those functions which reach Sarkar et al.'s bound and we exhibit functions achieving high nonlinearities. At section 3, we introduce a super-class of Maiorana-McFarland's class. We study the degrees, the nonlinearities and the resiliency orders of its elements and we give examples of functions in this class having good cryptographic parameters.

2 The Known Constructions of Reasonably Large Sets of Cryptographic Functions, and Their Properties

Only one reasonably large class of Boolean functions is known, whose elements can be cryptographically analyzed.

2.1 Maiorana-McFarland's Construction

In [1] is introduced a modification of Maiorana-McFarland's construction of bent functions (cf. [12]) whose elements, viewed as binary vectors of length 2^n, are the concatenations of affine functions[1]: let k and r be integers such that $n \geq r > k \geq 0$; denote $n-r$ by s; let g be any Boolean function on F_2^s and ϕ a mapping from F_2^s to F_2^r such that every element in $\phi(F_2^s)$ has Hamming weight strictly greater than k. Then the function:

$$f_{\phi,g}(x,y) = x \cdot \phi(y) + g(y) = \sum_{i=1}^{r} x_i \phi_i(y) + g(y),\ x \in F_2^r,\ y \in F_2^s \qquad (2)$$

where $\phi_i(y)$ is the ith coordinate of $\phi(y)$, is m-resilient with $m \geq k$. Indeed, for every $a \in F_2^r$ and every $b \in F_2^s$, we have

$$\widehat{\chi_{f_{\phi,g}}}(a,b) = 2^r \sum_{y \in \phi^{-1}(a)} (-1)^{g(y)+b\cdot y}, \qquad (3)$$

since every (affine) function $x \mapsto f_{\phi,g}(x,y) + a \cdot x + b \cdot y$ either is constant or is balanced and contributes then for 0 in the sum $\sum_{x \in F_2^r, y \in F_2^s} (-1)^{f_{\phi,g}(x,y)+x\cdot a+y\cdot b}$.

The degree of $f_{\phi,g}$ is $s+1 = n-r+1$ if and only if ϕ has degree s (i.e. if at least one of its coordinate functions has degree s), which is possible only if

[1] As noted e.g. in [22], concatenations of m-resilient functions produce also, more generally, m-resilient functions. But this observation has not permitted until now to produce larger classes of resilient functions.

$k \leq r-2$, since if $k = r-1$ then ϕ is constant. Otherwise, the degree of $f_{\phi,g}$ is at most s. Thus, if $m = k$ then the degree of $f_{\phi,g}$ reachs Siegenthaler's bound $n-m-1$ if and only if either $m = r-2$ and ϕ has degree $s = n-m-2$ or $m = r-1$ and g has degree $s = n-m-1$. There are cases where $m > k$ (see below).

The nonlinearity of Maiorana-McFarland's functions could not be determined in the literature in a precise and a general way: the lower bound $N_{f_{\phi,g}} \geq 2^{n-1} - 2^{r-1}\max_{a\in F_2^r}|\phi^{-1}(a)|$ (where $|\phi^{-1}(a)|$ denotes the size of $\phi^{-1}(a)$) obtained in [24] is rather precise, but the upper bound $N_{f_{\phi,g}} \leq 2^{n-1} - 2^{r-1}$ obtained in [9, 10] does not involve the size of $\phi^{-1}(a)$. This upper bound is efficient when ϕ is injective. Notice that in this case, $f_{\phi,g}$ is then exactly k-resilient, where $k+1$ is the minimum weight of $\phi(y)$, $y \in F_2^s$ and that g plays no role in the nonlinearity of $f_{\phi,g}$ or in its resiliency order. Thanks to these bounds, the nonlinearity of $f_{\phi,g}$ can also be precisely determined when g is null (as noted in [9, 10]) and more generally when g is affine, and also when $\max_{a\in F_2^r}|\phi^{-1}(a)| \leq 2$: according to relation (3), $N_{f_{\phi,g}}$ equals then $2^{n-1} - 2^{r-1}\max_{a\in F_2^r}|\phi^{-1}(a)|$. Notice that, ϕ being chosen, the case g affine is unfortunately not the most interesting one from nonlinearity viewpoint. Indeed, in relation (3), for a given a, the sum $\sum_{y\in\phi^{-1}(a)}(-1)^{g(y)+b\cdot y}$ has maximum magnitude when $g(y) + b\cdot y$ is constant on $\phi^{-1}(a)$ for some b.

In the next proposition, we improve upon the upper bound proved in [9, 10] and we deduce further information on the nonlinearities of Maiorana-McFarland's functions, which shows for instance why Sarkar and Maitra could not find 4-resilient Maiorana McFarland's functions in 10 variables with nonlinearity 480.

Proposition 1. *Let $f_{\phi,g}$ be defined by (2). Then the nonlinearity $N_{f_{\phi,g}}$ of $f_{\phi,g}$ satisfies*

$$2^{n-1} - 2^{r-1}\max_{a\in F_2^r}|\phi^{-1}(a)| \leq N_{f_{\phi,g}} \leq 2^{n-1} - 2^{r-1}\left\lceil \sqrt{\max_{a\in F_2^r}|\phi^{-1}(a)|}\right\rceil. \qquad (4)$$

Assume that every element in $\phi(F_2^s)$ has Hamming weight strictly greater than k ($f_{\phi,g}$ is then m-resilient with $m \geq k$). Then $N_{f_{\phi,g}} \leq 2^{n-1} - 2^{r-1}\left\lceil \frac{2^{s/2}}{\sqrt{\sum_{i=k+1}^{r}\binom{r}{i}}}\right\rceil$.

Under this hypothesis, if $f_{\phi,g}$ achieves the best possible nonlinearity $2^{n-1} - 2^{k+1}$, then either $r = k+1$ or $r = k+2$.

If $r = k+1$ then ϕ takes constant value $(1,\cdots,1)$ and $n \leq k+3$. Either $s = 1$ and $g(y)$ is then any function in one variable or $s = 2$ and g is then any function of the form $y_1y_2 + l(y)$ where l is affine (thus, f is quadratic, i.e. has degree at most 2).

If $r = k+2$, then ϕ is injective, $n \leq k+2+\log_2(k+3)$, g is any function in $n-k-2$ variables and $d^\circ f_{\phi,g} \leq 1 + \log_2(k+3)$.

Proof: The inequality $N_{f_{\phi,g}} \geq 2^{n-1} - 2^{r-1}\max_{a\in F_2^r}|\phi^{-1}(a)|$ is a direct consequence of relations (1) and (3). Let us prove now the upper bound. The sum

$\sum_{b\in F_2^s}\left(\sum_{y\in\phi^{-1}(a)}(-1)^{g(y)+b\cdot y}\right)^2 = \sum_{b\in F_2^s}\left(\sum_{y,z\in\phi^{-1}(a)}(-1)^{g(y)+g(z)+b\cdot(y+z)}\right)$ equals: $2^s|\phi^{-1}(a)|$ (indeed, $\sum_{b\in F_2^s}(-1)^{b\cdot(y+z)}$ is null if $y\neq z$). The maximum of a set of values being always greater than or equal to its mean, we deduce $\max_{b\in F_2^s}|\sum_{y\in\phi^{-1}(a)}(-1)^{g(y)+b\cdot y}|\geq\sqrt{|\phi^{-1}(a)|}$ and thus

$$\max_{a\in F_2^r;b\in F_2^s}|\widehat{\chi_{f_{\phi,g}}}(a,b)|\geq 2^r\left\lceil\sqrt{\max_{a\in F_2^r}|\phi^{-1}(a)|}\right\rceil .$$

Hence, according to relation (1): $N_{f_{\phi,g}}\leq 2^{n-1}-2^{r-1}\left\lceil\sqrt{\max_{a\in F_2^r}|\phi^{-1}(a)|}\right\rceil$. If every element in $\phi(F_2^s)$ has Hamming weight strictly greater than k, we have $\max_{a\in F_2^r}|\phi^{-1}(a)|\left(\sum_{i=k+1}^r\binom{r}{i}\right)\geq 2^s$ and $N_{f_{\phi,g}}\leq 2^{n-1}-2^{r-1}\left\lceil\frac{2^{s/2}}{\sqrt{\sum_{i=k+1}^r\binom{r}{i}}}\right\rceil$.

If $N_{f_{\phi,g}}=2^{n-1}-2^{k+1}$, then according to (4), we have $\sqrt{\max_{a\in F_2^r}|\phi^{-1}(a)|}\leq 2^{k-r+2}$ and thus $k+1\leq r\leq k+2$ since $\max_{a\in F_2^r}|\phi^{-1}(a)|\geq 1$. If $r=k+1$, then since every element in $\phi(F_2^s)$ has Hamming weight strictly greater than k, ϕ must take constant value $(1,\cdots,1)$ and $\max_{a\in F_2^r}|\phi^{-1}(a)|$ is then equal to 2^s. Since $\sqrt{\max_{a\in F_2^r}|\phi^{-1}(a)|}\leq 2^{k-r+2}$, this implies $s\leq 2(k-r+2)=2$. Thus, $f_{\phi,g}$ is quadratic and of the form $f(x,y)=\sum_{i=1}^r x_i+g(y)$. Its nonlinearity being equal to $2^{n-1}-2^{k+1}$, we have $\max_{b\in F_2^s}\left|\sum_{y\in F_2^s}(-1)^{g(y)+b\cdot y}\right|=2$. Thus $s\geq 1$. If $s=1$ then $f(x,y_1)=\sum_{i=1}^r x_i+g(y_1)$ (if g is constant then f is $(n-2)$-resilient with null nonlinearity and if g is not constant, then f is $(n-1)$-resilient with null nonlinearity). If $s=2$ then g must be bent, i.e. equal to $y_1y_2+l(y)$ where l is affine. If $r=k+2$, then $\max_{a\in F_2^r}|\phi^{-1}(a)|=1$ and ϕ is injective. Since ϕ is injective and is valued in $\{a\in F_2^r;\ w_H(a)\geq k+1=r-1\}$ we deduce $2^s\leq\binom{r}{r-1}+\binom{r}{r}=r+1$ and thus $n-r\leq\log_2(r+1)$. Siegenthaler's inequality completes the proof. ◇

Examples of Optimum Functions. We give now examples of resilient Maiorana-McFarland's functions with high nonlinearities. The existence of some of these functions have been already shown in the literature. But this was often done by random search while a deterministic construction is provided here. We shall reduce our investigation to m-resilient functions with n even or with n odd and $m>n/2-2$, since in the case n is odd and $m\leq n/2-2$, we do not know what is the precise bound.

– We first complete Proposition 1 when $\phi(y)=(1,\cdots,1)$, $\forall y\in F_2^s$. Then $\phi^{-1}(a)$ is empty if $a\neq(1,\cdots,1)$ and equals F_2^s if $a=(1,\cdots,1)$, and the function $f_{\phi,g}$ is $(r-1)$-resilient if g is not balanced and it is $(r+k)$-resilient if g is k-resilient. $N_{f_{\phi,g}}$ equals $2^r\ N_g$ and is at most equal to $2^{n-1}-2^{r-1+s/2}=2^{n-1}-2^{n/2-1+r/2}$. If g is not balanced, the functions $f_{\phi,g}$ achieving Sarkar et al.'s bound have been studied in Proposition 1 for $m=r-1>n/2-2$. For $m=r-1\leq n/2-2$ (n even) the only possible cases for which we can obtain functions with nonlinearity

$2^{n-1}-2^{n/2-1}-2^r$ are clearly for $r \leq 2$. For $r = 1$, we have $N_g = 2^{n-2}-2^{n/2-2}-1$ which is possible for $n = 4$ only. For $r = 2$, the function $f_{\phi,g}$ achieves Sarkar et al.'s bound if and only if $r = n/2 - 1$, i.e. $n = 6$ and g is bent. If g is k-resilient, then if $r+k > n/2-2$, $f_{\phi,g}$ achieves Sarkar et al.'s bound if and only if $k > s/2-2$ and if g does; and if $r+k \leq n/2-2$ then $f_{\phi,g}$ cannot achieve Sarkar et al.'s bound (i.e. N_g cannot equal $2^{s-1}-2^{n/2-r-1}-2^{k+1}$) unless, maybe, $r = 1$ and $k = (s-5)/2$.

– We show now that for every even $n \leq 10$, Sarkar et al.'s bound with $m = n/2 - 2$ can be acheived by Maiorana-McFarland's functions. The nonlinearity the function $f_{\phi,g}$ must reach is $2^{n-1} - 2^{n/2}$ (this number is often called the quadratic bound, see next paragraph). Take $r = n/2 + 1$ and $s = n/2 - 1$. For $n \leq 10$, we have $1 + r + \binom{r}{2} \geq 2^s$ and we deduce that there exist injective mappings $\phi : F_2^s \mapsto \{x \in F_2^r;\ w_H(x) > r - 3 = m\}$. For every such ϕ and for every $g : F_2^s \mapsto F_2$, the function $f_{\phi,g}$ is $(n/2-2)$-resilient and its nonlinearity is $2^{n-1} - 2^{r-1} = 2^{n-1} - 2^{n/2}$.

– We describe now a general situation in which Maiorana-McFarland's functions can have high nonlinearities (but do not achieve in general Sarkar et al.'s bound, which is not known to be tight in these ranges except for small values of n). Let r, k and s be three positive integers such that $k \leq r-1$ and $\sum_{i=k+1}^{r} \binom{r}{i} \geq 2^s$. Set $n = r + s$. Let ϕ be any one-to-one mapping from F_2^s to the set $\{x \in F_2^r; w_H(x) > k\}$ (such mapping ϕ exists thanks to the inequality above). Then for every Boolean function g on F_2^s, the function $f_{\phi,g}$ is a k-resilient function on F_2^n and has nonlinearity $2^{n-1} - 2^{r-1}$. Examples of such situation are the following:

• For any $k > 0$, choose $r = 2k + 1$ and $s = 2k$; then the nonlinearity of $f_{\phi,g}$ equals $2^{n-1} - 2^{2k} = 2^{n-1} - 2^{\frac{n-1}{2}}$ which is known as the best possible nonlinearity of all Boolean functions on F_2^n for odd $n \leq 7$ and the best possible nonlinearity of quadratic functions on F_2^n for every odd n (it is often called the quadratic bound). There exist only few known examples of functions on F_2^n (n odd) with nonlinearities strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ (these examples are known for odd $n \geq 15$, cf. [17]) and of balanced such functions (cf. [15, 22, 25]); here we have an example, for every $n \equiv 1 \bmod 4$, of $\frac{n-1}{4}$-resilient functions on F_2^n with nonlinearity equal to $2^{n-1} - 2^{\frac{n-1}{2}}$. This nonlinearity is the best known nonlinearity for k-resilient functions; moreover, for $k = 1, 2$ ($n = 5, 9$) it achieves Sarkar et al.'s bound (this does not imply, in the case $n = 9$, that $f_{\phi,g}$ achieves Siegenthaler's bound because $2^{n-1} - 2^{2k} > 2^{n-1} - 2^{k+1}$; in fact, the maximum possible degree of $f_{\phi,g}$ is $2k+1$). For $n = 9$, this optimal function can be obtained by Sarkar and Maitra's algorithm A given in [22]. We have here its precise description.

Notice that it is impossible to obtain nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ with a quadratic $\frac{n-1}{4}$-resilient function (or even more generally with a partially-bent function): recall that such function has this nonlinearity if and only if its kernel has dimension 1 (see [5]) and that it can then be $\frac{n-1}{4}$-resilient only if there exists an affine hyperplane with minimum weight strictly greater than $\frac{n-1}{4}$. This is clearly impossible for $n \geq 9$.

- For any $s > 0$, choose $r \geq 2^s - 1$ and set $k = r - 2$. The nonlinearity of $f_{\phi,g}$ equals then $2^{n-1} - 2^{r-1} = 2^{n-1} - 2^{k+1}$ and $f_{\phi,g}$ achieves Sarkar et al.'s bound and Siegenthaler's bound.
- There exist other examples of r, k, s leading to good functions.

Improved Resiliency Orders. The functions satisfying the hypothesis of Proposition 1 are not the only ones in Maiorana-McFarland's class which can achieve Sarkar et al.'s bound. We describe below two other cases. The first one has also been considered by Cusick in [11], but in a more complex way and without looking for the best possible nonlinearity.

Proposition 2. *Let $f_{\phi,g}$ be defined by (2).*

1. Assume that every element in $\phi(F_2^s)$ has Hamming weight strictly greater than k and that, for every $a \in F_2^r$ of weight $k+1$, either the set $\phi^{-1}(a)$ is empty or it has an even size and the restriction of g to this set is balanced. Then $f_{\phi,g}$ is m-resilient with $m \geq k+1$. Under this hypothesis, if $f_{\phi,g}$ achieves the best possible nonlinearity $2^{n-1} - 2^{k+2}$, then $r \leq k+2$.
If $r = k+1$ then either $s = 2$ and g and f are affine or $s = 3$ and g is balanced and has nonlinearity 4.
If $r = k+2$ then $n \leq k + 4 + \log_2(k+3)$ and $d^\circ f \leq 2 + \log_2(k+3)$.

2. Assume in addition that:
a. for every $a \in F_2^r$ of weight $k+1$ and every $i \in \{1, \cdots, s\}$, denoting by H_i the linear hyperplane of equation $y_i = 0$ in F_2^s, either the set $\phi^{-1}(a) \cap H_i$ is empty or it has an even size and the restriction of g to this set is balanced;
b. for every $a \in F_2^r$ of weight $k+2$, either the set $\phi^{-1}(a)$ is empty or it has an even size and the restriction of g to this set is balanced. Then $f_{\phi,g}$ is m-resilient with $m \geq k+2$. Under this hypothesis, if $f_{\phi,g}$ achieves the best possible nonlinearity $2^{n-1} - 2^{k+3}$, then $r \leq k+3$.
If $r = k+1$, then $3 \leq s \leq 5$ and ϕ takes constant value $(1, \cdots, 1)$. If $s = 3$ then g and f are affine. If $s = 4$, then g has nonlinearity 4. If $s = 5$ then g has nonlinearity 12.
If $r = k+2$ then $n \leq k + 6 + \log_2(k+3)$ and $d^\circ f \leq 3 + \log_2(k+3)$.
If $r = k+3$ then $n \leq k+5+\log_2(\binom{k+3}{2}+k+3)$ and $d^\circ f \leq 2+\log_2(\binom{k+3}{2}+k+3)$.

The proof has to be omitted because of length constraints.

Other Examples of Optimum Functions. Choose again three positive integers r, k and s such that $\sum_{i=k+1}^{r} \binom{r}{i} \geq 2^s$ and a one-to-one mapping ϕ from F_2^s to the set $\{x \in F_2^r; w_H(x) > k\}$. Set $s' = s + 1$ and modify ϕ into a two-to-one mapping $\phi' : F_2^{s'} \mapsto \{x \in F_2^r;\ w_H(x) > k\}$. For any $x \in F_2^r$ such that $w_H(x) > k$, let $g' : F_2^{s'} \mapsto F_2$ take each value 0 and 1 once on the pair $\phi'^{-1}(x)$. Then, according to Proposition 2, the function $f_{\phi',g'}$ is $(k+1)$-resilient on $F_2^{n'}$ with $n' = s' + r = n + 1$ and its nonlinearity is twice that of $f_{\phi,g}$ for every $g : F_2^s \mapsto F_2$ (thus, $f_{\phi',g'}$ achieves Sarkar et al.'s bound if $f_{\phi,g}$ does).

Another way of modifying $f_{\phi,g}$ into a function with the same number of variables and the same parameters as the function $f_{\phi',g'}$ above would be to take $f'(x, x_{r+1}, y) = f_{\phi,g}(x, y) + x_{r+1}$. But this kind of function having a linear term, it is less suited for cryptographic use (for instance, it has a linear structure, i.e. the derivative $f'(x, x_{r+1}, y) + f'(x, x_{r+1} + 1, y)$ is a constant).

Remark: In the case that every non-empty set $\phi^{-1}(a)$ is an affine set, then more can be said: assume that $\phi^{-1}(a)$ is either the empty set or a flat for every a, that it is empty for every word a of weight $\leq k$, and that, for some positive integer l, the restriction of g to every non-empty set $\phi^{-1}(a)$ such that $w_H(a) = k + i$, $i \leq l$, is $(l - i)$-resilient. Then according to relation 3, $f_{\phi,g}$ is $(k + l)$-resilient. ⋄

A drawback of Maiorana-McFarland's functions is that their restrictions obtained by fixing y in their input are affine. Affine functions being cryptographically weak functions, there is a risk that this property be used in attacks. Also, Maiorana-McFarland's functions have high divisibilities of their Fourier spectra, and there is also a risk that this property be used in attacks as it is used in [4] to attack block ciphers. A purpose of this paper is to produce a construction having not this drawback and leading to a larger class of cryptographic functions. Before that, we study the other known constructions.

2.2 Dillon's Construction

In [6] is used an idea of Dillon (cf. [12]) to obtain a construction of resilient functions. Similar observations as for Maiorana-McFarland's construction can be made on the ability of these functions to have nonlinearities near Sarkar et al.'s bound. But this class has few elements.

2.3 Dobbertin's Construction

In [13], Hans Dobbertin studies an interesting method for modifying bent functions into balanced functions with high nonlinearities. Unfortunately:

Proposition 3. *Dobbertin's construction cannot produce m-resilient functions with $m > 0$.*

3 Maiorana-McFarland's Super-class

The functions of the super-class of Maiorana-McFarland's class that we introduce now are concatenations of quadratic functions (i.e. functions of degrees at most 2).

3.1 Quadratic Functions

It is shown in [14] that any quadratic function $f(x)$ is linearly equivalent to a function of the form

$$x_1x_2 + \cdots + x_{2i-1}x_{2i} + \cdots + x_{2t-1}x_{2t} + l(x) \tag{5}$$

where $2t$ is smaller than or equal to the number of variables and where l is affine. The functions we shall concatenate below are not general quadratic functions, because the parameters of the functions could then not be evaluated, but they have a slightly more general form than (5). They are defined on F_2^{2t} and have the form

$$f(x) = \sum_{i=1}^{t} u_i x_{2i-1} x_{2i} + l(x) = \sum_{i=1}^{t} u_i x_{2i-1} x_{2i} + \sum_{j=1}^{2t} v_i x_i + c, \tag{6}$$

where $u = (u_1, \cdots, u_t)$ is an element of F_2^t, $v = (v_1, \cdots, v_{2t})$ is an element of F_2^{2t} and c is an element of F_2. We shall need in the sequel to compute sums $\sum_{x \in F_2^{2t}} (-1)^{f(x)}$. We know (and it is a simple matter to check) that if there exists $i = 1, \cdots, t$ such that u_i is null and v_{2i-1} or v_{2i} is not null, then f is balanced and thus $\sum_{x \in F_2^{2t}} (-1)^{f(x)} = 0$. We consider now the case where such an i does not exist. Then we have $f(x) = \sum_{i=1}^{t} u_i (x_{2i-1} + v_{2i})(x_{2i} + v_{2i-1}) + \sum_{i=1}^{t} v_{2i-1} v_{2i} + c$. Changing x_{2i-1} into $x_{2i-1} + v_{2i}$ and x_{2i} into $x_{2i} + v_{2i-1}$ does not change the value of $\sum_{x \in F_2^{2t}} (-1)^{f(x)}$. Hence: $\sum_{x \in F_2^{2t}} (-1)^{f(x)} = \sum_{x \in F_2^{2t}} (-1)^{\sum_{i=1}^{t} u_i x_{2i-1} x_{2i} + \sum_{i=1}^{t} v_{2i-1} v_{2i} + c}$. It is a simple matter to check that $\sum_{x_{2i-1}, x_{2i} \in F_2} (-1)^{u_i x_{2i-1} x_{2i}}$ equals 4 if $u_i = 0$ and equals 2 if $u_i = 1$. Thus $\sum_{x \in F_2^{2t}} (-1)^{f(x)} = 2^{2t - w_H(u)} (-1)^{\sum_{i=1}^{t} v_{2i-1} v_{2i} + c}$. Applying this to the function $f(x) + \sum_{j=1}^{2t} a_j x_j$, we deduce:

Proposition 4. *Let $u = (u_1, \cdots, u_t) \in F_2^t$, $v = (v_1, \cdots, v_{2t}) \in F_2^{2t}$, $c \in F_2$ and set $f(x) = \sum_{i=1}^{t} u_i x_{2i-1} x_{2i} + \sum_{j=1}^{2t} v_j x_j + c$. Let a be any element of F_2^{2t}. If there exists $i = 1, \cdots, t$ such that $u_i = 0$ and $v_{2i-1} \neq a_{2i-1}$ or $v_{2i} \neq a_{2i}$, then $\widehat{\chi_f}(a)$ is null. Otherwise, $\widehat{\chi_f}(a)$ equals $2^{2t - w_H(u)} (-1)^{\sum_{i=1}^{t} (v_{2i-1} + a_{2i-1})(v_{2i} + a_{2i}) + c}$.*

3.2 The Maiorana-McFarland's Super-class

Definition 1. *Let n and r be positive integers such that $r < n$. Denote the integer part $\lfloor \frac{r}{2} \rfloor$ by t and $n - r$ by s. Let ψ be a mapping from F_2^s to F_2^t and let $\psi_1, \cdots, \psi_t$ be its coordinate functions. Let ϕ be a mapping from F_2^s to F_2^r and let $\phi_1, \cdots, \phi_r$ be its coordinate functions. Let g be a Boolean function on F_2^s. The function $f_{\psi,\phi,g}$ is defined on $F_2^n = F_2^r \times F_2^s$ as*

$$f_{\psi,\phi,g}(x, y) = \sum_{i=1}^{t} x_{2i-1} x_{2i} \psi_i(y) + x \cdot \phi(y) + g(y) =$$

$$\sum_{i=1}^{t} x_{2i-1} x_{2i} \psi_i(y) + \sum_{j=1}^{r} x_i\, \phi_i(y) + g(y);\ x \in F_2^r,\ y \in F_2^s.$$

The restrictions of $f_{\psi,\phi,g}$ obtained by fixing y in its input are quadratic functions of the form (6) or their extensions with one linear variable (r odd), and

$f_{\psi,\phi,g}(x,y)$, viewed as a binary vector of length 2^n, equals the concatenation of quadratic functions. Maiorana-McFarland's functions correspond to the case where ψ is the null mapping. As a direct consequence of Proposition 4, we have:

Theorem 1. *Let $f_{\psi,\phi,g}$ be defined as in Definition 1. Then for every $a \in F_2^r$ and every $b \in F_2^s$ we have*

$$\widehat{\chi_{f_{\psi,\phi,g}}}(a,b) = \sum_{y \in E_a} 2^{r-w_H(\psi(y))}(-1)^{\sum_{i=1}^{t}(\phi_{2i-1}(y)+a_{2i-1})(\phi_{2i}(y)+a_{2i})+g(y)+y\cdot b},$$

where E_a is the superset of $\phi^{-1}(a)$ equal if r is even to

$$\{y \in F_2^s / \ \forall i \leq t,\ \psi_i(y) = 0 \Rightarrow (\phi_{2i-1}(y) = a_{2i-1} \text{ and } \phi_{2i}(y) = a_{2i})\},$$

and if r is odd to

$$\left\{ y \in F_2^s / \begin{cases} \forall i \leq t,\ \psi_i(y) = 0 \Rightarrow (\phi_{2i-1}(y) = a_{2i-1} \text{ and } \phi_{2i}(y) = a_{2i}) \\ \phi_r(y) = a_r \end{cases} \right\}.$$

Remark: let y be an element of F_2^s. Denote the weight of $\psi(y)$ by l. Then y belongs to 4^l sets E_a. One of them is $E_{\phi(y)}$. The others correspond to the vectors $a \neq \phi(y)$ such that $a_{2i-1} = \phi_{2i-1}(y)$ and $a_{2i} = \phi_{2i}(y)$ for every index i outside the support of the vector $\psi(y)$.

4 Cryptographic Properties of the Constructed Functions

4.1 Algebraic Degree

Let $f_{\psi,\phi,g}$ be defined as in Definition 1. The degree of $f_{\psi,\phi,g}$ clearly equals $\max(2 + d^\circ\psi_1, \cdots, 2 + d^\circ\psi_t, 1 + d^\circ\phi_1, \cdots, 1 + d^\circ\phi_r, d^\circ g)$. It is upper bounded by $2 + s$.

4.2 Nonlinearity

Theorem 2. *Let $f_{\psi,\phi,g}$ be defined as in Definition 1. Denote by M the maximum weight of $\psi(y)$ for $y \in F_2^s$, and by M' its minimum weight. Then the nonlinearity $N_{f_{\psi,\phi,g}}$ of $f_{\psi,\phi,g}$ satisfies*

$$2^{n-1} - 2^{r-M'-1} \max_{a \in F_2^r} |E_a| \leq 2^{n-1} - \max_{a \in F_2^r} \sum_{y \in E_a} 2^{r-w_H(\psi(y))-1} \leq N_{f_{\psi,\phi,g}} \leq$$

$$2^{n-1} - \max_{a \in F_2^r} \sqrt{\sum_{y \in E_a} 2^{2r-2w_H(\psi(y))-2}} \leq 2^{n-1} - 2^{r-M-1} \max_{a \in F_2^r} \sqrt{|E_a|}$$

where $|E_a|$ denotes the size of the set E_a defined in Theorem 1.

The proof is similar to that of Proposition 1 and is omitted because of length constraints.

We have seen above that the nonlinearity of a Maiorana-McFarland's function $f_{\phi,g}$ can be more easily determined when ϕ is injective. The function is then "three-valued". The nonlinearity of $f_{\psi,\phi,g}$ can similarly be more precisely determined when all the sets E_a have size at most 1, i.e. when the quadratic functions whose concatenation is $f_{\psi,\phi,g}$ have disjoint spectra.

Proposition 5. *Let $f_{\psi,\phi,g}$ be defined as in Definition 1. Every set E_a has at most one element if and only if, for every two distinct elements y and y' of F_2^s, denoting by J_y the set of indices equal to $\{j \leq 2t/\ \psi_{\lceil \frac{j}{2} \rceil}(y) = 0\}$ if r is even and to $\{j \leq 2t/\ \psi_{\lceil \frac{j}{2} \rceil}(y) = 0\} \cup \{r\}$ if r is odd, there exists $i \in J_y \cap J_{y'}$ such that $\phi_j(y) \neq \phi_j(y')$.*

Notice that, even in this case, $f_{\psi,\phi,g}$ is not necessarily three-valued: the magnitude of $\widehat{\chi_{f_{\psi,\phi,g}}}$ being bounded between 2^{r-M} and $2^{r-M'}$ where M (resp. M') is the maximum (resp. minimum) weight of $\psi(y)$, $y \in F_2^s$, the function $f_{\psi,\phi,g}$ is three-valued if $M' = M$. We study below a situation in which the hypothesis of Proposition 5 is satisfied.

Corollary 1. *Let $f_{\psi,\phi,g}$ be defined as in Definition 1 and let M be the maximum weight of $\psi(y)$, $y \in F_2^s$. Suppose that ϕ is injective and that for every two distinct elements y and y' of F_2^s, the set $\{i \leq t;\ \phi_{2i-1}(y) \neq \phi_{2i-1}(y')$ or $\phi_{2i}(y) \neq \phi_{2i}(y')\}$ has size strictly greater than $2M$ (this condition is satisfied in particular if the set $\phi(F_2^s)$ has minimum Hamming distance strictly greater than $4M$). Then, every set E_a has size at most 1, and $N_{f_{\psi,\phi,g}} = 2^{n-1} - 2^j$ where $r - M - 1 \leq j \leq r - M' - 1$.*

Proof. For every two elements $y \neq y'$ of F_2^s, since $\psi(y)$ and $\psi(y')$ have weights smaller than or equal to M, at most $2M$ indices $i \leq t$ satisfy $\psi_i(y) = 1$ or $\psi_i(y') = 1$. The condition satisfied by ϕ implies that there exists $i \leq t$ such that $\psi_i(y) = \psi_i(y') = 0$ and $\phi_{2i-1}(y) \neq \phi_{2i-1}(y')$ or $\phi_{2i}(y) \neq \phi_{2i}(y')$, and the hypothesis of Proposition 5 is satisfied. Thus every set E_a contains at most one element. Theorem 2 completes the proof. ◇

4.3 Balancedness and Resiliency

Theorem 3. *Let $f_{\psi,\phi,g}$ be defined as in Definition 1 and let k be non-negative. For every $y \in F_2^s$, denote by I_y the set of indices equal to $\{j \leq 2t/\ \psi_{\lceil \frac{j}{2} \rceil}(y) = 0$ and $\phi_j(y) = 1\}$ if r is even or if r is odd and $\phi_r(y) = 0$, and to $\{j \leq 2t/\ \psi_{\lceil \frac{j}{2} \rceil}(y) = 0$ and $\phi_j(y) = 1\} \cup \{r\}$ if r is odd and $\phi_r(y) = 1$. Assume that for every $y \in F_2^s$, I_y has size strictly greater than k. Then $f_{\psi,\phi,g}$ is m-resilient with $m \geq k$.*
In particular, if for every $y \in F_2^s$, the set I_y is not empty, then $f_{\psi,\phi,g}$ is balanced.

Proof: Let $a \in F_2^r$ and $b \in F_2^s$. Assume that (a, b) has weight smaller than or equal to k. Then a has weight smaller than or equal to k. Let y be an element of the set E_a (defined in Theorem 1), then for every index j in I_y, we must have $a_j = 1$. According to the hypothesis on I_y, the word a must then have weight strictly greater than k, a contradiction. We deduce that the set E_a is empty and, thus, that $\widehat{\chi_f}(a,b) = 0$. $\diamond$

In the case of Maiorana-McFarland's functions, the condition of Theorem 3 reduces to the fact that every element in $\phi(F_2^s)$ has Hamming weight strictly greater than k, since all coordinate functions of ψ are null. Let us translate the condition similarly in the general case.

Corollary 2. *Let $f_{\psi,\phi,g}$ be defined as in Definition 1 and let k be a non-negative integer. Consider the mapping Φ from F_2^s to F_2^r whose jth coordinate function for $j \leq 2t$ equals the product of the Boolean functions ϕ_j and $1+\psi_{\lceil \frac{j}{2} \rceil}$ and whose rth coordinate function equals ϕ_r if r is odd. If the image of every element in F_2^s by Φ has Hamming weight strictly greater than k, then $f_{\psi,\phi,g}$ is m-resilient with $m \geq k$.*

In particular, if the image of every element in F_2^s by Φ is nonzero, then $f_{\psi,\phi,g}$ is balanced.

Proof: For every $y \in F_2^s$, the set I_y introduced in Theorem 3 equals the support of $\Phi(y)$. Thus, it has size strictly greater than k if and only if $\Phi(y)$ has Hamming weight strictly greater than k. Theorem 3 completes the proof. $\diamond$

Remark:

- If the mapping ϕ satisfies $w_H(\phi(y)) > k$ for every $y \in F_2^s$, then the mapping Φ satisfies $w_H(\Phi(y)) > k - 2M$ for every y, since the vectors $\phi(y)$ and $\Phi(y)$ lie at distance at most $2M$ from each other.
- The results of Theorem 3 and Corollary 2 can be refined the same way as in Proposition 2.

Constructions of Highly Nonlinear Resilient Functions from the Super-class

– Let n be even and $\phi : F_2^{n/2} \mapsto F_2^{n/2} \setminus \{0\}$ be chosen such that every vector different from $(1, \cdots, 1)$ has one reverse image by ϕ and $(1, \cdots, 1)$ has two reverse images by ϕ. For every $g : F_2^{n/2} \mapsto F_2$, the function $f_{\phi,g}$ is then balanced, since ϕ does not take the zero value; but it has nonlinearity $2^{n-1} - 2^r = 2^{n-1} - 2^{n/2}$ only. We shall increase this nonlinearity by considering, instead of $f_{\phi,g}$, a function $f_{\psi,\phi,g}$ where ψ is chosen such that $f_{\psi,\phi,g}$ is still balanced. Choose $\psi(y)$ equal to the zero vector, except at one element u of $\phi^{-1}(1, \cdots, 1)$. If $n/2$ is odd or if it is even and if we choose as value of $\psi(u)$ a vector of F_2^t different from $(1, \cdots, 1)$, then for every $g : F_2^{n/2} \mapsto F_2$, the function $f_{\psi,\phi,g}$ is balanced since $E_{(0,\cdots,0)} = \emptyset$. According to Theorem 1, its nonlinearity equals $2^{n-1} - 2^{n/2-1} - 2^{n/2-w_H(\psi(u))-1}$. So let us choose for $\psi(u)$ a vector of highest possible weight: $\lceil \frac{n}{4} \rceil - 1$. Then $f_{\psi,\phi,g}$ has nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{n/2-\lceil \frac{n}{4} \rceil} = 2^{n-1} - 2^{n/2-1} - 2^{\lfloor \frac{n}{4} \rfloor}$. If $n/2$ is odd, then $f_{\psi,\phi,g}$ has nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{(n/2-1)/2}$, which is the best known nonlinearity for balanced functions if $n \leq 26$ (this same nonlinearity can be also reached with Dobbertin's method; the other methods do not work here: it can be checked that extending Patterson-Wiedemann's functions [17] or their modifications by Maitra-Sarkar [15] to even numbers of variables gives worse nonlinearities). Notice that this nonlinearity is impossible to exceed with a Maiorana-McFarland's function with $\phi : F_2^{n-r} \mapsto F_2^r \setminus \{0\}$. Indeed, if $r \geq n/2$ then $f_{\phi,g}$ has nonlinearity at most $2^{n-1} - 2^{n/2}$ (since ϕ cannot be injective if $r = n/2$) and if $r < n/2$ then there exists $a \in F_2^r$ such that $|\phi^{-1}(a)| \geq \frac{2^{n-r}}{2^r-1}$ and thus, according to Proposition 1, $N_{f_{\phi,g}} \leq 2^{n-1} - 2^{r-1} \left\lceil \sqrt{\frac{2^{n-r}}{2^r-1}} \right\rceil = 2^{n-1} - 2^{r-1} \left\lceil 2^{n/2-r} \sqrt{\frac{2^r}{2^r-1}} \right\rceil$. We have $\sqrt{\frac{2^r}{2^r-1}} > 1 + 2^{-r-1}$. Thus $N_{f_{\phi,g}} \leq 2^{n-1} - 2^{n/2-1} - 2^{r-1} \left\lceil 2^{n/2-2r-1} + \epsilon \right\rceil$ where $\epsilon > 0$. We checked that $N_{f_{\phi,g}}$ cannot then exceed $2^{n-1} - 2^{n/2-1} - 2^{(n/2-1)/2}$. It seems impossible that $N_{f_{\phi,g}}$ equals $2^{n-1} - 2^{n/2-1} - 2^{(n/2-1)/2}$, but we could not prove it.

– Let n be even and and let k be an integer such that $\sum_{i=0}^{k} \binom{n/2-2}{i} \leq \frac{2^{n/2-2}}{5}$. Then we have $2^{n/2-2} - \sum_{i=k+1}^{n/2-2} \binom{n/2-2}{i} \leq \frac{1}{5} 2^{n/2-2}$, thus $2^{n/2} \leq 5 \sum_{i=k+1}^{n/2-2} \binom{n/2-2}{i}$ and there can exist $\phi : F_2^{n/2} \mapsto \{x \in F_2^{n/2};\ w_H(x_3, \cdots, x_{n/2}) > k\}$ such that for every $u \in F_2^{n/2-2}$, at most one element of $F_2^2 \times \{u\}$ has two reverse images by ϕ and the three others have at most one reverse image. For every element $a \in F_2^{n/2}$ which has two reverse images, choose $y \in \phi^{-1}(a)$ and take $\psi(y) = (1, 0, \cdots, 0)$. Take $\psi(y) = (0, \cdots, 0)$ for every other element. Then $f_{\psi,\phi,g}$ is at least k-resilient and has nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{n/2-2}$, while $f_{\phi,g}$ is also at least k-resilient but has nonlinearity $2^{n-1} - 2^{n/2}$.

– *A general method:* Let $\phi : F_2^s \mapsto F_2^r$ be injective and such that $\phi^{-1}(a) = \emptyset$ for every a of Hamming weight at most k ($f_{\phi,g}$ is then k-resilient for every g; we have seen that such functions can achieve high nonlinearities). Choose a subset I of $\{1, \cdots, t\}$, where $t = \left\lfloor \frac{r}{2} \right\rfloor$ and denote its size by M. In our choice of the values taken by ψ, some of the vectors in $\psi(F_2^t)$ will have I as support and the others will be null. To ensure that $f_{\psi,\phi,g}$ is k-resilient, we need that for every $y \in F_2^s$ such that $\psi(y) \neq 0$, the word obtained from $\phi(y)$ by erasing all its coordinates of indices $j \leq 2t$ such that $\left\lceil \frac{j}{2} \right\rceil \in I$ has weight strictly greater than k. So we choose a subset U of F_2^{r-2M} of minimum weight at least $k+1$, we denote by $\tilde{U}$ the set of all $y \in F_2^s$ such that the word $\tilde{\phi}(y)$ obtained from $\phi(y)$ by erasing all these coordinates belongs to U, and we set ψ such that $\psi_i(y) = 1$ if $y \in \tilde{U}$ and $i \in I$ and $\psi_i(y) = 0$ otherwise. Assume that every non-empty set E_a is a flat and that, for every a such that $\phi^{-1}(a) \in \tilde{U}$, the restriction of g to E_a is bent. Then the upper bound of Theorem 2 is achieved. We have $E_a = \emptyset$ for every a of Hamming weight at most k, $|E_a| = 1$ for every a such that $w_H(a) > k$ and $\phi^{-1}(a) \notin \tilde{U}$ and $|E_a| = 2^{2M}$ for every a such that. $w_H(a) > k$ and $\phi^{-1}(a) \in \tilde{U}$. Then $f_{\psi,\phi,g}$ has same resiliency order and nonlinearity as $f_{\phi,g}$.

Acknowledgement

The author thanks one of the anonymous referees for his (her) useful observations.

References

1. P. Camion, C. Carlet, P. Charpin, N. Sendrier, "On correlation-immune functions", *Advances in Cryptology-CRYPTO'91*, Lecture Notes in Computer Science 576, pp. 86–100 (1991).
2. A. Canteaut, C. Carlet, P. Charpin et C. Fontaine. "On cryptographic properties of the cosets of $R(1, m)$". *IEEE Transactions on Information Theory* Vol. 47, no 4, pp. 1494-1513 (2001)
3. A. Canteaut and M. Trabbia. "Improved fast correlation attacks using parity-check equations of weight 4 and 5", *Advanced in Cryptology-EUROCRYPT 2000.* Lecture notes in computer science 1807, pp. 573-588 (2000).
4. A. Canteaut and M. Videau. "Degree of Composition of Highly Nonlinear Functions and Applications to Higher Order Differential Cryptanalysis", *Advances in Cryptology, EUROCRYPT2002*, Lecture Notes in Computer Science 2332, Springer Verlag, pp. 518-533 (2002)
5. C. Carlet. "Partially-bent functions", *Designs Codes and Cryptography*, 3, pp. 135-145 (1993) and *Advances in Cryptology-CRYPTO'92* Lecture Notes in Computer Science 740, pp. 280-291 (1993).
6. C. Carlet. "More correlation-immune and resilient functions over Galois fields and Galois rings". *Advances in Cryptology, EUROCRYPT' 97*, Lecture Notes in Computer Science 1233, Springer Verlag, pp. 422-433 (1997).
7. C. Carlet. "On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions", *Proceedings of SETA'01* (Sequences and their Applications 2001), *Discrete Mathematics and Theoretical Computer Science*, Springer, pp. 131-144 (2001).
8. C. Carlet and P. Sarkar. "Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions". *Finite fields and Applications* 8, pp. 120-130 (2002).
9. S. Chee, S. Lee, K. Kim and D. Kim. "Correlation immune functions with controlable nonlinearity". *ETRI Journal*, vol 19, no 4, pp. 389-401 (1997).
10. S. Chee, S. Lee, D. Lee and S. H. Sung. "On the correlation immune functions and their nonlinearity" *proceedings of Asiacrypt'96*, LNCS 1163, pp. 232-243 (1997).
11. T. W. Cusick. "On constructing balanced correlation immune functions". *Proceedings of SETA'98* (Sequences and their Applications 1998), *Discrete Mathematics and Theoretical Computer Science*, Springer, pp. 184-190 (1999).
12. J. F. Dillon. Elementary Hadamard Difference sets. Ph. D. Thesis, Univ. of Maryland (1974).
13. H. Dobbertin, " Construction of bent functions and balanced Boolean functions with high nonlinearity", *Fast Software Encryption* (Proceedings of the 1994 Leuven Workshop on Cryptographic Algorithms), Lecture Notes in Computer Science 1008, pp. 61-74 (1995).
14. Mac Williams, F. J. and N. J. Sloane (1977). *The theory of error-correcting codes*, Amsterdam, North Holland.
15. S. Maitra and P. Sarkar. "Modifications of Patterson-Wiedemann functions for cryptographic applications". *IEEE Trans. Inform. Theory*, Vol. 48, pp. 278-284, 2002.

16. W. Meier and O. Staffelbach. “ Nonlinearity Criteria for Cryptographic Functions”, *Advances in Cryptology*, EUROCRYPT’ 89, Lecture Notes in Computer Science 434, Springer Verlag, pp. 549-562 (1990).
17. N.J. Patterson and D.H. Wiedemann. “ The covering radius of the $[2^{15}, 16]$ Reed-Muller code is at least 16276”. *IEEE Trans. Inform. Theory*, IT-29, pp. 354-356 (1983).
18. N.J. Patterson and D.H. Wiedemann. “ Correction to [17]”. *IEEE Trans. Inform. Theory*, IT-36(2), pp. 443 (1990).
19. E. Pasalic, S. Maitra, T. Johansson and P. Sarkar. “New constructions of resilient functions and correlation immune Boolean functions achieving upper bound on nonlinearity”. Proceedings of the *Workshop on Coding and Cryptography 2001*, pp. 425–434 (2001).
20. O. S. Rothaus. “ On bent functions”, *J. Comb. Theory*, 20A, 300-305 (1976).
21. R. A. Rueppel *Analysis and design of stream ciphers* Com. and Contr. Eng. Series, Berlin, Heidelberg, NY, London, Paris, Tokyo 1986
22. P. Sarkar and S. Maitra. “Construction of nonlinear Boolean functions with important cryptographic properties”. *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, Springer Verlag, pp. 485–506 (2000).
23. P. Sarkar and S. Maitra. “Nonlinearity Bounds and Constructions of Resilient Boolean Functions”. *CRYPTO 2000, LNCS* Vol. 1880, ed. Mihir Bellare, pp. 515-532 (2000).
24. J. Seberry, X.M. Zhang and Y. Zheng. “On constructions and nonlinearity of correlation immune Boolean functions.” *Advances in Cryptology - EUROCRYPT’93*, LNCS 765, pp. 181-199 (1994).
25. J. Seberry, X.M. Zhang and Y. Zheng. “Nonlinearly balanced Boolean functions and their propagation characteristics.” *Advances in Cryptology - CRYPTO’93*, pp. 49–60 (1994).
26. T. Siegenthaler. “Correlation-immunity of nonlinear combining functions for cryptographic applications”. *IEEE Transactions on Information theory*, V. IT-30, No 5, pp. 776-780 (1984).
27. T. Siegenthaler. “Decrypting a Class of Stream Ciphers Using Ciphertext Only”. *IEEE Transactions on Computer, V. C-34*, No 1, pp. 81-85 (1985).
28. Y. V. Tarannikov. “ On resilient Boolean functions with maximum possible nonlinearity”. *Proceedings of INDOCRYPT 2000*, Lecture Notes in Computer Science 1977, pp. 19-30 (2000).
29. Y. V. Tarannikov. “New constructions of resilient Boolean functions with maximum nonlinearity”. *Proceedings of FSE 2001*, to appear in the Lecture Notes in Computer Science Series (2002).
30. Xiao Guo-Zhen and J. L. Massey. “A Spectral Characterization of Correlation-Immune Combining Functions”. *IEEE Trans. Inf. Theory*, Vol IT 34, n° 3, pp. 569-571 (1988).
31. Y. Zheng, X.-M. Zhang. “ Improved upper bound on the nonlinearity of high order correlation immune functions”. *Proceedings of Selected Areas in Cryptography 2000*, Lecture Notes in Computer Science 2012, pp. 262-274 (2001)