Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros

Sumanta Sarkar · Subhamoy Maitra

Abstract In this paper we study the neighbourhood of 15-variable Patterson-Wiedemann (PW) functions, i.e., the functions that differ by a small Hamming distance from the PW functions in terms of truth table representation. We exploit the idempotent structure of the PW functions and interpret them as Rotation Symmetric Boolean Functions (RSBFs). We present techniques to modify these RSBFs to introduce zeros in the Walsh spectra of the modified functions with minimum reduction in nonlinearity. Our technique demonstrates 15-variable balanced and 1-resilient functions with currently best known nonlinearities 16272 and 16264 respectively. In the process, we find functions for which the autocorrelation spectra and algebraic immunity parameters are best known till date.

Keywords Algebraic immunity · Autocorrelation · Balancedness · Nonlinearity · Rotation Symmetric Boolean functions · Resiliency

AMS Classification O6E30

1 Introduction

In [15], Patterson and Wiedemann presented Boolean functions on 15-variables with nonlinearity strictly greater than the bent concatenation bound. After more than two decades, in [9], 9-variable functions having nonlinearity exceeding the bent concatenation bound have been demonstrated. Most interestingly, both of these constructions rely on a specific structure of the Boolean functions. Under the interpretation that a Boolean function is a mapping $f : GF(2^n) \rightarrow GF(2)$, the functions presented in [8,9,15] are such that $f(x^2) = f(x)$ for any $x \in GF(2^n)$, i.e., these functions are invariant under the action of the group of Frobenius automorphisms. These functions were studied in [5–7] and referred as idempotents. By fixing any irreducible polynomial of degree n over GF(2), one may interpret the mapping $f : GF(2^n) \rightarrow GF(2)$ as $f : \{0, 1\}^n \rightarrow \{0, 1\}$. One can use this interpretation to get an RSBF from an idempotent by choosing a primitive polynomial of degree n and a normal basis [5]. The RSBFs are studied in great detail recently and it has been found that this sub class of Boolean functions is extremely rich in terms of cryptographic and combinatorial properties (see [8,9] and the references in these papers). Motivated by these results, we concentrate on PW functions in this paper and exploit the rotation symmetric structure of such functions to get best known nonlinearity results in terms of balanced and 1-resilient functions.

High nonlinearity of a Boolean function is important when it is used as a building block in any cryptographic system. On the other hand nonlinearity of a Boolean function is directly related to the covering radius of the first order Reed-Muller codes. It is well known that the maximum possible nonlinearity of an n-variable Boolean function is $2^{n-1} - 2^{\frac{n}{2}-1}$ for n even [3,16] and functions with this nonlinearity are called bent functions. The bound $2^{n-1} - \lceil 2^{\frac{n}{2}-1} \rceil$ is in general not known to be achieved when n is odd. For odd n, one can easily get (balanced) Boolean functions having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ by suitably concatenating two bent functions on $(n-1)$ variables. That is the reason the nonlinearity value $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd n is called the bent concatenation bound. For odd $n \leq 7$, the maximum nonlinearity of n-variable functions is $2^{n-1} - 2^{\frac{n-1}{2}}$ [1,13] and for odd $n > 7$, the maximum nonlinearity can exceed this bound [8,9,15].

Since balancedness is a useful cryptographic property for a Boolean function, the question of getting balanced Boolean function with high nonlinearity is an important issue. Further it is also combinatorially very interesting. As the bent functions are not balanced, the maximum nonlinearity for n-variable balanced functions for even n must be less than $2^{n-1} - 2^{\frac{n}{2}-1}$. Denote the maximum nonlinearity for any balanced Boolean function on n-variables by $nlb(n)$. Dobbertin conjectured in [4] that for n even, $nlb(n) \not> 2^{n-1} - 2^{\frac{n}{2}} + nlb(\frac{n}{2})$. This conjecture still remains unsettled.

For odd n, the challenge is to get balanced Boolean functions having nonlinearity greater than the bent concatenation bound. The first attempt in this direction was in [21], where 15-variable PW functions were used as a black box to construct balanced functions on odd number of input variables ($\geq$29) having nonlinearity greater than the bent concatenation bound. Later, in [12,17], the truth tables of the PW functions were modified to get 15-variable balanced functions having nonlinearity 16262 and that shows the existence of balanced Boolean functions exceeding the bent concatenation bound for odd number of input variables greater than or equal to 15.

We like to refer to [2,8,12,20] for the basics related to a Boolean function f and the definitions of Walsh spectrum $W_f(\cdot)$, nonlinearity $nl(f)$, autocorrelation spectrum, maximum absolute value in the autocorrelation spectrum Δ_f and algebraic immunity.

A Boolean function f is called *rotation symmetric* (RSBF) if it is invariant under the action of the cyclic group C_n acting on $\{0, 1\}^n$. Under this action, the orbit generated by $(x_1, x_2, \ldots, x_n)$ is $G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 1 \leq k \leq n\}$, where $\rho_n^k(x_1, \ldots, x_n)$ is the k-cyclic shift of $(x_1, \ldots, x_n)$. That means for an RSBF f, $f(y) = f(x)$, for all $y \in G_n(x)$. The number of such orbits is denoted by g_n. Thus the total number of distinct n-variable RSBFs is 2^{g_n}. Let ϕ be the Euler's *phi*-function, then it is known that $g_n = \frac{1}{n}\sum_{k|n}\phi(k)\,2^{\frac{n}{k}}$.

An *orbit* is completely determined by its *representative element* $\Lambda_{n,i}$, which is the lexicographically first element belonging to the orbit [22]. These representative elements are again arranged lexicographically as $\Lambda_{n,0},\ldots,\Lambda_{n,g_n-1}$. Thus an n-variable RSBF f can be represented by the g_n length string $[f(\Lambda_{n,0}),\ldots,f(\Lambda_{n,g_n-1})]$. In [22], it was also shown that the Walsh spectrum of an RSBF f can take only g_n many different values. To analyze the Walsh spectrum of an RSBF, the matrix ${}_n\mathcal{A}$ was introduced [22]. The matrix ${}_n\mathcal{A} = ({}_n\mathcal{A}_{i,j})_{g_n\times g_n}$ is defined as ${}_n\mathcal{A}_{i,j} = \sum_{x\in G_n(\Lambda_{n,i})}(-1)^{x\cdot\Lambda_{n,j}}$, for an n-variable RSBF. Using this matrix, the Walsh spectrum for an RSBF can be calculated as $W_f(\Lambda_{n,j}) = \sum_{i=0}^{g_n-1}(-1)^{f(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,j}$.

In this paper we present a deterministic technique that searches the neighbourhood of PW functions. The PW functions are interpreted as RSBFs and our motivation is to introduce Walsh spectrum zeros by modifying these functions with very little reduction in nonlinearity. In the process we get examples of balanced and 1-resilient functions with currently best known nonlinearities and Δ_f values. Our results improve upon the results available in [10,12,17,19]. Further, for the first time we demonstrate Boolean functions with maximum possible algebraic immunity having nonlinearity greater than bent concatenation bound.

Our technique is not a heuristic search, but an exhaustive search in a restricted domain based on the theoretical results presented in Theorems 1 and 2. We work on the rotation symmetric implementation instead of idempotents as the matrix structure of $({}_n\mathcal{A}_{i,j})_{g_n\times g_n}$ can be exploited nicely for implementation purpose.

A more general study of Boolean functions invariant under the action of some finite groups has been presented in [11] that demonstrated 15-variable functions with nonlinearity greater than the bent concatenation bound (but not exceeding the nonlinearity reported in [15]). Our study can be considered as looking into a particular case where the functions are invariant under the action of the group of Frobenius automorphisms.

2 Studying the Walsh spectrum of PW functions as RSBF

We first present the construction of RSBFs from the two PW functions on $(n = 15)$-variables given in [15]. Each of these functions is idempotent when we consider them as a mapping from $GF(2^n)$ to $GF(2)$. Let f_{PW} denotes one such function.

Construction 1 *Take $n = 15$. Consider a PW function f_{PW} on n-variables. Take the primitive polynomial $P(X) = X^{15} + X + 1$ over $GF(2)$. Consider a root α of $P(X)$. Take the normal basis $\mathcal{N} = \{\alpha^{(2^i\cdot 29) \bmod (2^{15}-1)} : i = 0,\ldots,14\}$. Represent each $x \in GF(2^n)$ as an n-bit binary vector with respect to $\mathcal{N}$. Denote the corresponding mapping $\{0,1\}^n \rightarrow \{0,1\}$ by f. The function f is an RSBF with $nl(f) = 2^{n-1} - 2^{\frac{n-1}{2}} + 20 = 16276$.*

In the rest of the paper we will consider f as the RSBF obtained from a PW function using Construction 1. We get two distinct (the first one is of algebraic degree 8 and the second one is of algebraic degree 9) RSBFs up to affine equivalence from Construction 1. Each of them are of nonlinearity 16276 and the distribution of the Walsh spectra of both the functions are the same. The Walsh spectrum of each of these functions consists of the distinct values $\{-216, -88, 40, 168\}$.

Henceforth we consider $n = 15$. Then $g_n = 2192$, out of them there are 2182 orbits of size 15, 6 orbits of size 5, 2 orbits of size 3 and 2 orbits of size 1.

We are interested in modifying each of the PW functions such that we can get zeros in the Walsh spectrum with minimum number of toggles at the output bits. In [17], authors adopted a random heuristic to achieve the similar goal. Here our motivation is to toggle the outputs of f corresponding to one or more orbits. It means that after the modification, the function will remain RSBF.

2.1 Modification with respect to one orbit of size 15 and another of size 5

Theorem 1 *Refer to the function f as in Construction 1. Let $G_n(\Lambda_{n,j})$ be an orbit such that $W_f(\Lambda_{n,j}) = 40$ and $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,j} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,j} = 20$, for some q, r, where $\Lambda_{n,q}$ is the representative element of an orbit of size 15 and $\Lambda_{n,r}$ is the representative element of an orbit of size 5. Construct*

$$\begin{aligned} g(x) &= f(x) \text{ for } x \in \{0,1\}^n \setminus (G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r})), \\ &= 1 \oplus f(x) \text{ for } x \in G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r}). \end{aligned}$$

Then $W_g(\Lambda_{n,j}) = 0$.

Further, let $\Lambda_{n,s}$ be the representative elements such that $W_f(\Lambda_{n,s}) = -216$ as s varies. If $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,s} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,s} < 20$ for all s, then $nl(g) > 2^{n-1} - 2^{\frac{n-1}{2}}$.

Proof Since, $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,j} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,j} = 20$, and $g = 1 \oplus f$ for the inputs belonging to $G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r})$, we have, $(-1)^{g(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,j} + (-1)^{g(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,j} = -20$. Also since $W_f(\Lambda_{n,j}) = 40$ and $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,j} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,j} = 20$, therefore we have

$$\sum_{i \notin \{q,r\}} (-1)^{f(\Lambda_{n,i})}\,{}_n\mathscr{A}_{i,j} = 20.$$

Thus,

$$\begin{aligned} W_g(\Lambda_{n,j}) &= \left((-1)^{g(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,j} + (-1)^{g(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,j}\right) + \sum_{i \notin \{q,r\}} (-1)^{g(\Lambda_{n,i})}\,{}_n\mathscr{A}_{i,j} \\ &= -20 + 20 = 0. \end{aligned}$$

This proves the first part of the theorem.

Note that for any ω, such that $W_f(\omega) = -88, 40, 168$, $|W_g(\omega)| \leq 168 + 40 = 208$. Further, consider the points $\Lambda_{n,s}$ where the Walsh spectrum values of f are maximum in absolute terms, we have $W_f(\Lambda_{n,s}) = -216$ as s varies. Let $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,s} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,s} = 20 - \delta_s$, where $\delta_s > 0$. Thus,

$$\begin{aligned} W_g(\Lambda_{n,s}) &= (-1)^{g(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,s} + (-1)^{g(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,s} + \sum_{i \notin \{q,r\}} (-1)^{g(\Lambda_{n,i})}\,{}_n\mathscr{A}_{i,s} \\ &= -\left((-1)^{f(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,s} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,s}\right) + \sum_{i \notin \{q,r\}} (-1)^{f(\Lambda_{n,i})}\,{}_n\mathscr{A}_{i,s} \\ &= -20 + \delta_s + (-216 - 20 + \delta_s) = -256 + 2\delta_s. \end{aligned}$$

Thus $nl(g) > 2^{n-1} - 2^{\frac{n-1}{2}}$. □

Using the idea of the above theorem, we describe a strategy to get 15-variable RSBFs g such that $nl(g) > 2^{n-1} - 2^{\frac{n-1}{2}}$ with $W_g(\omega) = 0$ for some point ω. There are 217 orbits (each of size 15) at which the Walsh spectrum value of f is 40. We take an orbit $G_n(\Lambda_{n,j})$ such that $W_f(\Lambda_{n,j}) = 40$. Then for each pair of orbits $G_n(\Lambda_{n,q})$ and $G_n(\Lambda_{n,r})$ of size 15 and 5 respectively such that $(-1)^{f(\Lambda_{n,q})}\, {}_n\mathscr{A}_{q,j} + (-1)^{f(\Lambda_{n,r})}\, {}_n\mathscr{A}_{r,j} = 20$, we construct

$$\begin{aligned} g(x) &= f(x) \text{ for } x \in \{0,1\}^n \setminus (G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r})), \\ &= 1 \oplus f(x) \text{ for } x \in G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r}). \end{aligned}$$

Then by Theorem 1, we have $W_g(\Lambda_{n,j}) = 0$, i.e., $W_g(\omega) = 0$ for each $\omega \in G_n(\Lambda_{n,j})$. As $|G_n(\Lambda_{n,j})| = 15$, number of the zeros in the Walsh spectrum of g will be 15. We store the tuple $(\Lambda_{n,j}, \Lambda_{n,q}, \Lambda_{n,r}, nl(g))$ in a file F. We repeat these steps for all the 217 orbits where W_f takes the value zero. At the end, we see that 16264 is the maximum nonlinearity that has been achieved by some functions in F. We get 253 and 63 RSBFs g respectively from degree 9 and degree 8 PW functions with nonlinearity 16264 and for each of these functions the Walsh spectrum contains 15 many zeros which occur exactly at an orbit of size 15. We further check these functions and find that they are all affinely non-equivalent as their Walsh distributions are different. We find that some of these functions have the maximum absolute value in the autocorrelation spectrum as low as 192. In the rest of the paper, we express a binary pattern $(x_1, \ldots, x_n) \in \{0,1\}^{15}$ by its equivalent decimal number, where x_1 is taken as the most significant bit.

For example, we take the RSBF f from the PW function of degree 8 and we take the function g from F represented by (1893, 1843, 1057, 16264), where $\Delta_g = 192$. Now consider the input $\omega = 1893$, then $g'(x) = g(x) \oplus \omega \cdot x$ will be balanced. Also $nl(g') = nl(g) = 16264$ and $\Delta_{g'} = \Delta_g = 192$. This improves the result of [12,17] in terms of nonlinearity as well as autocorrelation.

Closer studies to these functions provide further improvement in nonlinearity. Note that the maximum absolute value in the Walsh spectrum of g is 240 and the sign is negative. If for any of these functions, the second maximum absolute value in the Walsh spectrum corresponds to 232 and the sign is negative, then one may increase the nonlinearity by 2 by modifying the output of the functions at two points. There are plenty of such functions among the 316 functions reported above. Thus one gets balanced functions having nonlinearity 16266. We skip the details of this technique (which is available in [20]) as later to the conference version of this paper in WCC 2007, further search in this domain has produced better nonlinearity 16268 [10] for 15-variable balanced functions. In [10], the PW functions having nonlinearity 16268 [15] are studied. Directed search has been exploited in [10] to toggle the outputs corresponding to 20 orbits (13 of size 15, 5 of size 5, 2 of size 1) to get a balanced function without any reduction in nonlinearity. Note that, in our technique we motivate the exhaustive search in the neighbourhood of the PW functions. Exhaustive search considering 20 orbits is computationally infeasible, but the kind of directed search [10] motivated by our technique may provide more improved results.

The next challenge is to get 15-variable balanced functions with nonlinearity more than 16268 (by searching the neighbourhood of PW functions, but not by some heuristic search). So far we have considered the neighbourhood of the PW functions by modifying the outputs corresponding to the inputs containing one orbit of size 5 and another of size 15. The next motivation is to extend the neighbourhood further and we study the neighbourhood considering three orbits of size 15. Thus there are $\binom{2182}{3} < 2^{31}$ many options. We study this space and find unbalanced functions with nonlinearity 16271, having 2 as the minimum absolute value in the Walsh spectrum. We need to modify one more point at the output to get zeros in the Walsh spectrum. We try any one of the two size 1 orbits for this. In the process the nonlinearity is increased further to 16272[1]. For example, an RSBF g_1 is obtained by toggling the outputs of f (degree 8 PW function having nonlinearity 16276) at the orbits 315, 2275, 8183 (of size 15) and 0 (of size 1). The function g_1 has 7 zeros in its Walsh spectrum with $\Delta_{g_1} = 248$ and algebraic degree 11. Consider the input $\omega = 4681$ as one of the points such that $W_{g_1}(\omega) = 0$. Construct the function $g_2(x) = g_1(x) \oplus \omega \cdot x$. Then g_2 is balanced with $nl(g_2) = 16272$ and $\Delta_{g_2} = 248$. We have checked that the algebraic immunity of g_2 is equal to 8. This demonstrates a Boolean function on an odd number of variables having nonlinearity greater than the bent concatenation bound and maximum possible algebraic immunity.

For general case, construct the balanced function F on odd number of variables $m > 15$ as $F(x_1, \ldots, x_{15}, x_{16}, \ldots, x_m) = g_2(x_1, \ldots, x_{15}) + b(x_{16}, \ldots, x_m)$, where b is a bent function. Then $nl(F) = 2^{m-1} - 2^{\frac{m-1}{2}} + 16 \times 2^{\frac{m-15}{2}}$.

3 Strategy to get 1-resilient functions

Any 15-variable RSBF g with nonlinearity 16264 has 15 many zeros and all of these 15 input points with Walsh spectrum zeros belong to one orbit of size 15. Now one may note that for an n-variable 1-resilient function, the number of Walsh spectrum zeros is at least $n + 1$. Thus the functions g cannot be affinely transformed to 1-resilient functions. To get more Walsh spectrum zeros, we need to modify the functions further. We consider the additional points where the Walsh spectrum values are close to zero. We observe that the value in the Walsh spectrum closest to zero is 16 which occurs for some functions g, also for each of these functions the Walsh spectrum value 16 occurs at one or more orbits of size 15 only. *We construct the set S which consists of the functions g such that the second minimum Walsh spectrum value is* 16. We would like to modify any function from S such that

1. the existing orbit with Walsh spectrum value zero stays at zero and
2. one or more of the existing orbits with Walsh spectrum value 16 drop to zero.

This strategy will indeed increase the Walsh spectrum zeros in the modified function. The only issue that has to be noted is the drop in nonlinearity after this modification. As the nonlinearity of 1-resilient functions must be divisible by four [18] and we are interested in nonlinearities greater than the bent concatenation bound 16256, the nonlinearities of the modified functions should be 16260 or 16264 (or even more, but we actually did not get more than that in the experimentation we did).

Theorem 2 *Consider a function $g \in S$ such that $W_g(\Lambda_{n,p}) = 0$ and $W_g(\Lambda_{n,j}) = 16$. Let*

1. $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,j} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,j} = 8$, *and*
2. $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathscr{A}_{q,p} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathscr{A}_{r,p} = 0$,

where $\Lambda_{n,q}, \Lambda_{n,r}$ are two orbit representative elements. Construct

$$\begin{aligned} h(x) &= g(x) \text{ for } x \in \{0,1\}^n \setminus G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r}), \\ &= 1 \oplus g(x) \text{ for } x \in G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r}), \end{aligned}$$

then $W_h(\Lambda_{n,j}) = W_h(\Lambda_{n,p}) = 0$.

[1] One of the reviewers has also pointed out this neighbourhood by identifying a nonlinearity 16268 function with the Walsh spectrum zeros.

Proof Since, $W_g(\Lambda_{n,j}) = 16$ and $(-1)^{g(\Lambda_{n,q})}\,{}_{n}\mathscr{A}_{q,j} + (-1)^{g(\Lambda_{n,r})}\,{}_{n}\mathscr{A}_{r,j} = 8$, therefore, $\sum_{i \notin \{q,r\}} (-1)^{g(\Lambda_{n,i})}\,{}_{n}\mathscr{A}_{i,j} = 8$. Now,

$$\begin{aligned} W_h(\Lambda_{n,j}) &= \sum_{i \notin \{q,r\}} (-1)^{h(\Lambda_{n,i})}\,{}_{n}\mathscr{A}_{i,j} + (-1)^{h(\Lambda_{n,q})}\,{}_{n}\mathscr{A}_{q,j} + (-1)^{h(\Lambda_{n,r})}\,{}_{n}\mathscr{A}_{r,j} \\ &= \sum_{i \notin \{q,r\}} (-1)^{g(\Lambda_{n,i})}\,{}_{n}\mathscr{A}_{i,j} - (-1)^{g(\Lambda_{n,q})}\,{}_{n}\mathscr{A}_{q,j} - (-1)^{g(\Lambda_{n,r})}\,{}_{n}\mathscr{A}_{r,j} \\ &= 8 - 8 = 0. \end{aligned}$$

Again since, $W_g(\Lambda_{n,p}) = 0$ and $(-1)^{f(\Lambda_{n,q})}\,{}_{n}\mathscr{A}_{q,p} + (-1)^{f(\Lambda_{n,r})}\,{}_{n}\mathscr{A}_{r,p} = 0$, the proof that $W_h(\Lambda_{n,p}) = 0$ follows easily by the similar argument as given above. □

We take a function $g \in S$. Then choose the orbit $G_n(\Lambda_{n,p})$ (size 15) such that $W_g(\Lambda_{n,p}) = 0$ and also an orbit $G_n(\Lambda_{n,j})$ (size 15) such that $W_g(\Lambda_{n,j}) = 16$. Now we form the sets $\{q_1, \ldots, q_t\}$ and $\{r_1, \ldots, r_t\}$ such that for each $q \in \{q_1, \ldots, q_t\}$ and $r \in \{r_1, \ldots, r_t\}$, we have, $|{}_{n}\mathscr{A}_{q,j}| = 5$ and $|{}_{n}\mathscr{A}_{r,j}| = 3$. Then we consider those pairs for which (i) $(-1)^{f(\Lambda_{n,q})}\,{}_{n}\mathscr{A}_{q,j} + (-1)^{f(\Lambda_{n,r})}\,{}_{n}\mathscr{A}_{r,j} = 8$, and (ii) $(-1)^{f(\Lambda_{n,q})}\,{}_{n}\mathscr{A}_{q,p} + (-1)^{f(\Lambda_{n,r})}\,{}_{n}\mathscr{A}_{r,p} = 0$. Construct

$$\begin{aligned} h(x) &= g(x) \text{ for } x \in \{0,1\}^n \setminus G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r}), \\ &= 1 \oplus g(x) \text{ for } x \in G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r}), \end{aligned}$$

Then by Theorem 2, we have $W_h(\Lambda_{n,j}) = W_h(\Lambda_{n,p}) = 0$. Thus the modified function h will have at least 30 zeros in its Walsh spectrum. Due to this modification, nonlinearity may fall. However we intend to keep functions h which have nonlinearity more than the bent concatenation bound 16256 and divisible by 4 (as a 1-resilient function must have its nonlinearity divisible by 4). We represent such a function h by the tuple $(st(g), \Lambda_{n,q}, \Lambda_{n,r}, nl(h))$, where $st(g)$ points to the PW function f and the tuple which represents g.

Given an m-variable Boolean function ϕ, let us define $S_\phi = \{\omega \in \{0,1\}^m \mid W_\phi(\omega) = 0\}$. If there exist n linearly independent vectors in S_ϕ, then one can construct a nonsingular $m \times m$ matrix B_ϕ whose rows are linearly independent vectors from S_ϕ. Let, $C_\phi = B_\phi^{-1}$. Now one can define $\phi'(x) = \phi(C_\phi x)$. Both ϕ' and ϕ *have the same weight, nonlinearity and algebraic degree*. Moreover, $W_{\phi'}(\omega) = 0$ for $wt(\omega) = 1$. This ensures that ϕ' is correlation immune of order 1. Further if ϕ is balanced then ϕ' is 1-resilient. This technique has been used in [14].

We use the above mentioned strategy for a few functions $g \in S$. Consider the RSBF f obtained from the 8-degree PW function using Construction 1. We take functions $g \in S$ obtained from f such that the value 16 occurs exactly at 15 points in the Walsh spectrum. For these functions we find 32066 functions with nonlinearity either 16260 or 16264 and having at least 30 Walsh zeros. For example, we take a function $g \in S$ obtained from f and represented by $st(g) = (1893, 935, 11627, 16264)$. We present the function h which is represented by $(st(g), 6895, 1971, 16264)$. We note that $W_h(\omega) = 0$ for the input $\omega = 539$. Thus the function $\phi = h \oplus \omega \cdot x$ will be balanced. Then as described above, we find 15 linearly independent vectors from S_ϕ and hence a 1-resilient function ϕ' having nonlinearity 16264 is found. We note that for ϕ', $\Delta_{\phi'} = 232$ with algebraic degree 12 and algebraic immunity 7. This shows for the first time the existence of a 1-resilient function exceeding the bent concatenation bound in nonlinearity with maximum absolute autocorrelation value less than $2^{\frac{15+1}{2}}$.

In [9], existence of 1-resilient functions having the maximum absolute value in the autocorrelation spectra $< 2^{\frac{m+1}{2}}$ has been demonstrated for $m = 9, 11$. However, the nonlinearity in those cases did not exceed the bent concatenation bound.

In [17,19], a method to construct resilient functions on odd numbers of variables, having nonlinearity greater than the bent concatenation bound, has been proposed. The construction used the PW functions as a part of it. In the process, a 41-variable 1-resilient function ψ_1 has been designed with $nl(\psi_1) > 2^{40} - 2^{20} + 51 \times 2^{10}$. Thus so far, the resilient functions, having nonlinearity greater than the bent concatenation bound, had been known for 41 or more variables. Our example shows the existence of a 15-variable function with nonlinearity that exceeds the bent concatenation bound. Again for odd $m > 15$, the function $b(x_{16}, \ldots, x_m) \oplus \phi'(x_1, \ldots, x_{15})$ will be 1-resilient with nonlinearity $2^{m-1} - 2^{\frac{m-1}{2}} + 8 \times 2^{\frac{m-15}{2}}$. This shows that 1-resilient functions are available for 15 or more variables with nonlinearity more than the bent concatenation bound. Thus the gap between 15 and 39 variables is now settled. Further we show that using the function ϕ' we can construct a 41-variable 1-resilient function with nonlinearity that exceeds the lower bound of $nl(\psi_1)$. Let $\psi_2 = b(x_{16}, \ldots, x_{41}) \oplus \phi'(x_1, \ldots, x_{15})$, then $nl(\psi_2) = 2^{40} - 2^{20} + 8 \times 2^{\frac{41-15}{2}} = 2^{40} - 2^{20} + 64 \times 2^{10}$ which is greater than $2^{40} - 2^{20} + 51 \times 2^{10}$, the lower bound of $nl(\psi_1)$.

4 Conclusion

In this paper we successfully modify the two 15-variable PW functions [15] to construct balanced functions f with currently best known nonlinearity and autocorrelation parameters. Some of these functions provide the maximum algebraic immunity 8. These results improve the parameters presented in [10,12,17]. Further we could also construct 1-resilient functions on 15-variables having nonlinearity 16264 that were not known earlier. The 1-resilient functions on odd number of variables having nonlinearity greater than the bent concatenation bound were earlier known for 41 or more variables [17,19]. Apart from the improvements in the parameter values, the theoretical contribution of this paper is to modify any of the PW functions keeping their idempotent structure unchanged and inducing Walsh spectrum zeros in the modified function. Given balancedness, 1-resiliency, maximum possible algebraic immunity, very good nonlinearity and nice autocorrelation properties, we recommend use of these functions in cipher design.

Acknowledgments The authors would like to thank the anonymous reviewers whose valuable comments have improved the editorial and technical quality of this paper a lot.

References

1. Berlekamp E.R., Welch L.R.: Weight distributions of the cosets of the (32, 6) Reed-Muller code. IEEE Trans. Inform. Theory **18**(1), 203–207 (1972).
2. Carlet C., Dalai D.K., Gupta K.C., Maitra S.: Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans. Inform. Theory **527**, 3105–3121 (2006).
3. Dillon J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland (1974).
4. Dobbertin H.: Construction of bent functions and balanced Boolean functions with high nonlinearity. In: Preneel B. (ed.) Fast Software Encryption, Lecture Notes in Computer Science, vol. 1008, pp. 61–74. Springer (1994).

5. Filiol E., Fontaine C.: Highly nonlinear balanced Boolean functions with a good correlation-immunity. In: Nyberg K. (ed.) EUROCRYPT, Lecture Notes in Computer Science, vol. 1403, pp. 475–488. Springer (1998).
6. Fontaine C.: The nonlinearity of a class of Boolean functions with short representation. In: Přibyl J. (ed.) PRAGOCRYPT'96, pp. 129–144. CTU Publishing House (1996).
7. Fontaine C.: On some cosets of the first-order Reed-Muller code with high minimum weight. IEEE Trans. Inform. Theory **45**(4), 1237–1243 (1999).
8. Kavut S., Maitra S., Sarkar S., Yücel M.D.: Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity > 240. In: Barua R., Lange T. (eds.) INDOCRYPT, Lecture Notes in Computer Science, vol. 4329, pp. 266–279. Springer (2006).
9. Kavut S., Maitra S., Yücel M.D.: Search for Boolean functions with excellent profiles in the rotation symmetric class. IEEE Trans. Inform. Theory **53**(5), 1743–1751 (2007).
10. Kavut S., Yücel M.D.: Balanced Boolean functions with nonlinearity > $2^{n-1} - 2^{\frac{n-1}{2}}$. Cryptology ePrint Archive, http://eprint.iacr.org/, Report 2007/321, 15 August (2007).
11. Langevin P., Zanotti J.-P.: Nonlinearity of some invariant Boolean functions. Des. Codes Cryptogr. **36**(2), 131–146 (2005).
12. Maitra S., Sarkar P.: Modifications of Patterson-Wiedemann functions for cryptographic applications. IEEE Trans. Inform. Theory **48**(1), 278–284 (2002).
13. Mykkeltveit J.J.: The covering radius of the (128, 8) Reed-Muller code is 56. IEEE Trans. Inform. Theory **26**(3), 359–362 (1980).
14. Pasalic E., Johansson T.: Further results on the relation between nonlinearity and resiliency for Boolean functions. In: Walker M. (ed.) IMA International Conference, Lecture Notes in Computer Science, vol. 1746, pp. 35–44. Springer (1999).
15. Patterson N.J., Wiedemann D.H.: The covering radius of the (2^{15}, 16) Reed-Muller code is at least 16276. IEEE Trans. Inform. Theory **29**(3), 354–356 (1983). See also the correction in **36**(2), 443 (1990).
16. Rothaus O.S.: On "bent" functions. J. Combin. Theory Ser. A **20**(3), 300–305 (1976).
17. Sarkar P., Maitra S.: Construction of nonlinear Boolean functions with important cryptographic properties. In: Advances in Cryptology-EUROCRYPT, Lecture Notes in Computer Science, vol. 1807, pp. 485–506 (2000).
18. Sarkar P., Maitra S.: Nonlinearity bounds and constructions of resilient Boolean functions. In: Bellare M. (ed.) CRYPTO, Lecture Notes in Computer Science, vol. 1880, pp. 515–532. Springer (2000).
19. Sarkar P., Maitra S.: Construction of nonlinear resilient Boolean functions using "small" affine functions. IEEE Trans. Inform. Theory **50**(9), 2185–2193 (2004).
20. Sarkar S., Maitra S.: Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros. In: WCC 2007, International Workshop on Coding and Cryptography, pp. 351–360, April 16-20, 2007, Versailles (France). A detailed version is available at Cryptology ePrint Archive, http://eprint.iacr.org/, Report 2007/427, 19 November, 2007.
21. Seberry J., Zhang X., Zheng Y.: Nonlinearly balanced Boolean functions and their propagation characteristics (extended abstract). In: Stinson D.R. (ed.) CRYPTO, Lecture Notes in Computer Science, vol. 773, pp. 49–60. Springer (1993).
22. Stănică P., Maitra S., Clark J.: Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. Fast Software Encryption Workshop (FSE 2004). Lecture Notes in Computer Science, vol. 3017, pp. 161–177. Springer Verlag (2004).