# Idempotents in the Neighbourhood of Patterson-Wiedemann Functions having Walsh Spectra Zeros*

Sumanta Sarkar and Subhamoy Maitra
Applied Statistics Unit, Indian Statistical Institute
203 B T Road, Kolkata 700 108, India
Email: {sumanta_r, subho}@isical.ac.in

**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. The PW functions have nonlinearity $2^{15-1} - 2^{\frac{15-1}{2}} + 20 = 16276$, which exceeds the bent concatenation bound $2^{15-1} - 2^{\frac{15-1}{2}} = 16256$ and these functions do not have zeros in the Walsh spectra. We exploit the idempotent structure of the PW functions and interpret them as Rotation Symmetric Boolean Functions (RSBFs). Then we modify these RSBFs to introduce zeros in the Walsh spectra of the modified functions with minimum reduction in nonlinearity. In the process, we construct 15-variable functions with nonlinearity $2^{15-1} - 2^{\frac{15-1}{2}} + 8 = 16264$ with 15 zeros in the Walsh spectrum of each functions. Moreover we modify these functions to achieve 15-variable balanced functions with nonlinearity $2^{15-1} - 2^{\frac{15-1}{2}} + 10 = 16266$, which is currently the best known. Next we present a method to increase the number of zeros further in the Walsh spectra of the functions with nonlinearity 16264. Applying linear transformation on these modified functions we achieve 1-resilient functions having nonlinearity 16264. This shows for the first time, the existence of the 15-variable 1-resilient Boolean functions with nonlinearity greater than the bent concatenation bound. 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.

## 1 Introduction

In [23], Patterson and Wiedemann presented Boolean functions on 15-variables with nonlinearity strictly greater than the bent concatenation bound. After more than two decades, in [15], 9-variable functions having nonlinearity exceeding the bent concatenation bound have been demonstrated. Most interestingly, both these constructions rely on the idempotent 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 [13, 15, 23] are such that $f(x^2) = f(x)$ for any $x \in GF(2^n)$. These functions were studied in [9–11] 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 a Rotation

*This is a revised and extended (Section 4 is a new addition) version of the paper that has been presented in WCC 2007, International Workshop on Coding and Cryptography, April 16-20, 2007, Versailles (France).

Symmetric Boolean Function (RSBF) from an idempotent by choosing a primitive polynomial of degree $n$ and a normal basis [9]. 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 [4, 6, 12–14, 18, 19, 25, 32, 33]. 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 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 [7, 27] 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, 21] and for odd $n > 7$, the maximum nonlinearity can exceed this bound [13, 15, 23].

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 $b$-variables by $nlb(b)$. Dobbertin conjectured in [8] 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 [31], 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 [17, 28], 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.

Before explaining our contribution in detail, we first present some preliminaries.

### 1.1 Basics of Boolean functions

An $n$-variable Boolean function $f$ is a mapping $f : GF(2^n) \to GF(2)$. Another representation of a Boolean function $f$ is a mapping $f : \{0,1\}^n \to \{0,1\}$. This representation is called the truth table representation. Using any basis of $GF(2^n)$, we can express each $x \in GF(2^n)$ as an $n$-tuple $(x_1 x_2 \dots x_n)$, $x_i \in GF(2)$, $i = 1, \dots, n$. Thus we can draw the truth table representation from the former representation.

We now concentrate on the truth table representation of a Boolean function which is a $2^n$ length binary string

$$f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), \dots, f(1,1,\cdots,1)].$$

The *Hamming weight* of a binary string $T$ is the number of 1's in $T$, denoted by $wt(T)$. An $n$-variable function $f$ is said to be *balanced* if its truth table contains an equal number of 0's and 1's, i.e., $wt(f) = 2^{n-1}$. Also, the *Hamming distance* between two equidimensional binary

strings $T_1$ and $T_2$ is defined by $d(T_1, T_2) = wt(T_1 \oplus T_2)$, where $\oplus$ denotes the addition over $GF(2)$.

An $n$-variable Boolean function $f(x_1, \ldots, x_n)$ can be considered to be a multivariate polynomial over $GF(2)$. This polynomial can be expressed as a sum of products representation of all distinct $k$-th order products ($0 \leq k \leq n$) of the variables. More precisely, $f(x_1, \ldots, x_n)$ can be written as

$$a_0 \oplus \bigoplus_{1 \leq i \leq n} a_i x_i \oplus \bigoplus_{1 \leq i < j \leq n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_i, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. This representation of $f$ is called the *algebraic normal form* (ANF) of $f$. The number of variables in the highest order product term with nonzero coefficient is called the *algebraic degree*, or simply the degree of $f$ and denoted by $deg(f)$.

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. The set of all $n$-variable affine (respectively linear) functions is denoted by $A(n)$ (respectively $L(n)$). The nonlinearity of an $n$-variable function $f$ is defined as

$$nl(f) = \min_{g \in A(n)} (d(f, g)),$$

i.e., the minimum distance from the set of all $n$-variable affine functions.

Let $x = (x_1, \ldots, x_n)$ and $\omega = (\omega_1, \ldots, \omega_n)$ both belong to $\{0, 1\}^n$ and $x \cdot \omega = x_1\omega_1 \oplus \ldots \oplus x_n\omega_n$. Let $f(x)$ be a Boolean function on $n$ variables. Then the *Walsh transform* of $f(x)$ is an integer valued function over $\{0, 1\}^n$ which is defined as

$$W_f(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot \omega}.$$

The Walsh spectrum of $f$ is the multiset $\{W_f(\omega) | \omega \in \{0, 1\}^n\}$. In terms of Walsh spectrum, the nonlinearity of $f$ is given by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \{0,1\}^n} |W_f(\omega)|.$$

In [34], an important characterization of correlation immune functions has been presented, which we use as the definition here. A function $f(x_1, \ldots, x_n)$ is $m$-th order correlation immune (respectively $m$-resilient) iff its Walsh spectrum satisfies $W_f(\omega) = 0$, for $1 \leq wt(\omega) \leq m$ (respectively $0 \leq wt(\omega) \leq m$).

Autocorrelation properties are also cryptographically important [26,35] for a Boolean function $f$. Let $\beta \in \{0, 1\}^n$. The autocorrelation value of the Boolean function $f$ with respect to the vector $\beta$ is $\Delta_f(\beta) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus f(x \oplus \beta)}$. Further we denote

$$\Delta_f = \max_{\beta \in \{0,1\}^n, \beta \neq (0,\ldots,0)} |\Delta_f(\beta)|$$

and $\Delta_f$ is called the absolute indicator. $f$ is said to satisfy PC($k$), if $\Delta_f(\beta) = 0$ $for$ $1 \leq wt(\beta) \leq k$.

Recently algebraic attack has received a lot of attention (see [2, 3, 20] and the references in these paper) in studying the security of the ciphers. One necessary condition to resist this attack is that the Boolean function used in the cryptosystem should have good algebraic immunity. An $n$-variable Boolean function $g$ is called an annihilator of an $n$-variable Boolean function $f$ if $fg = 0$. We denote the set of all nonzero annihilators of $f$ by $AN(f)$. Then algebraic immunity of $f$, denoted by $\mathcal{AI}_n(f)$, is defined [20] as the degree of the minimum degree annihilator among all the annihilators of $f$ and $1 + f$, i.e., $\mathcal{AI}_n(f) = \min\{\deg(g) : g \neq 0,\ g \in AN(f) \cup AN(1 + f)\}$. It is known [3,20] that $\mathcal{AI}_n(f) \leq \lceil \frac{n}{2} \rceil$.

### 1.2 Rotation Symmetric Boolean Function (RSBF)

Let $x_i \in \{0,1\}$ for $1 \le i \le n$. For some integer $k \ge 0$ we define $\rho_n^k(x_i)$ as $\rho_n^k(x_i) = x_{i+k \bmod n}$, with the exception that when $i + k \equiv 0 \bmod n$, then we will assign $i + k \bmod n$ by $n$ instead of 0. This is to cope up with the input variable indices $1, \ldots, n$ for $x_1, \ldots, x_n$. Let $(x_1, x_2, \ldots, x_{n-1}, x_n) \in \{0,1\}^n$. Then we extend the definition as $\rho_n^k(x_1, x_2, \ldots, x_{n-1}, x_n) = (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_{n-1}), \rho_n^k(x_n))$. Hence, $\rho_n^k$ acts as $k$-cyclic rotation on an $n$-bit vector.

A Boolean function $f$ is called *rotation symmetric* if for each input $(x_1, \ldots, x_n) \in \{0,1\}^n$,

$$f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n) \text{ for } 1 \le k \le n-1.$$

That is, the rotation symmetric Boolean functions are invariant under cyclic rotations of inputs. The inputs of a rotation symmetric Boolean function can be divided into *orbits* so that each orbit consists of all cyclic shifts of one input. An orbit generated by $(x_1, x_2, \ldots, x_n)$ is

$$G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 1 \le k \le n\}$$

and the number of such orbits is denoted by $g_n$. Thus the total number of distinct $n$-variable RSBFs is $2^{g_n}$. Let $\phi$ be Euler's *phi*-function, then it can be shown by Burnside's lemma that (see also [32])

$$g_n = \frac{1}{n} \sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}.$$

An *orbit* is completely determined by its *representative element* $\Lambda_{n,i}$, which is the lexicographically first element belonging to the orbit [33]. 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 [33] it was shown that the Walsh spectrum of an RSBF $f$ takes the same value for all elements belonging to the same orbit, i.e., $W_f(u) = W_f(v)$ if $u \in G_n(v)$. Therefore the Walsh spectrum of $f$ can be represented by the $g_n$ length vector $(wa_f[0], \ldots, wa_f[g_n - 1])$, where $wa_f[j] = W_f(\Lambda_{n,j})$. In analyzing the Walsh spectrum of an RSBF, the ${}_n\mathcal{A}$ matrix has been introduced [33]. 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 $g_n \times g_n$ matrix, the Walsh spectrum for an RSBF can be calculated as

$$W_f(\Lambda_{n,j}) = \sum_{i=0}^{g_n-1} (-1)^{f(\Lambda_{n,i})}\, {}_n\mathcal{A}_{i,j}.$$

The operation of multiplying by 2 divides the integers $\bmod (2^n - 1)$ into different sets called 2-cyclotomic cosets $\bmod (2^n - 1)$. The 2-cyclotomic coset containing $s$ consists of the elements $\{s, 2s, 2^2 s, \ldots, 2^{d_s-1} s\}$ where $d_s$ is the smallest positive integer such that $2^{d_s} \cdot s \equiv s \bmod (2^n - 1)$. The term $d_s$ is called the length of the cyclotomic coset $\bmod (2^n - 1)$. One may note that there are $(g_n - 1)$ many cyclotomic cosets.

### 1.3 Equivalence between RSBF and Idempotent

Let us consider a Boolean function $f : GF(2^n) \to GF(2)$. A Boolean function $f$ is called idempotent [9] iff $f(\gamma) = f(\gamma^2)$, for any $\gamma \in GF(2^n)$. Given a primitive element $\theta \in GF(2^n)$,

an idempotent function will have the same value corresponding to all elements $\theta^i$ where $i$ belongs to the same 2-cyclotomic coset, say $\{s, 2s, 2^2s, \ldots, 2^{d_s-1}s\}$.

We fix a primitive polynomial $P(X)$ of degree $n$ over GF(2) and let $\theta$ be a root of $P(X)$. Let us consider a normal basis $\{\theta^t, \theta^{2t}, \theta^{2^2t} \ldots, \theta^{2^{n-1}t}\}$ of $GF(2^n)$. We represent $\theta^t, \theta^{2t}, \theta^{2^2t}, \ldots, \theta^{2^{n-1}t}$ by the $n$-bit binary vectors $(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)$ (the order is $(x_1, x_2, \ldots, x_n)$) respectively. Then all the elements $\theta^j$ can be expressed as an $n$-bit binary vector with respect to the normal basis. Once the $n$-bit vector is decided, this is basically the assignment to the inputs of the Boolean function and we can refer back to the standard truth table (considering Boolean function as a mapping $\{0,1\}^n \to \{0,1\}$) to get the value of the function corresponding to the input pattern. In this representation all the $n$-bit binary vectors corresponding to the elements $\{\theta^s, \theta^{2s}, \theta^{2^2s} \ldots, \theta^{2^{d_s-1}s}\}$ will be cyclic rotation of each other [9]. That means the elements $\theta^i$ where $i$ runs over a 2-cyclotomic coset, form an orbit and as the idempotent $f$ has the same value corresponding to all these $\theta^i$'s, $f$ will have the same output in its truth table for all the elements in the orbit; i.e., in terms of truth table representation, $f$ becomes an RSBF.

### 1.4 Contribution of this paper

Balancedness is an important property of a Boolean function from a cryptographic as well as a combinatorial point of view. A challenging question in this direction is to get balanced Boolean functions with high nonlinearity. One natural attempt for the 15-variable case is to use or modify the PW functions (which do not contain any zero in their Walsh spectra) to get balancedness, keeping in mind that the nonlinearity should not decrease much due to the modification.

The 15-variable PW functions were used as a black box in [31] to construct balanced functions on an odd number of input variables ($\geq 29$) having nonlinearity greater than the bent concatenation bound. However, the internal structure of the PW functions was not studied in [31]. In [17, 28] the internal structure of the PW functions has been modified to get improved results upon [31] in terms of nonlinearity for balanced functions on odd number ($\geq 15$) of input variables. The idea of [17, 28] was as follows.

Take $n = 15$. Consider the truth table of a PW function $f$ as a mapping from $\{0,1\}^n \to \{0,1\}$. One can easily check that there are 3255 many points $\omega \in \{0,1\}^n$ where the value of the Walsh spectrum $W_f(\omega) = 40$. Now consider a function $g = f \oplus \omega \cdot x$. Clearly $W_g(0) = 40$ and one needs to toggle 20 output bits from 0 to 1 to achieve balancedness. The idea of [17,28] was to divide the $2^n$-bit long truth table of $g$ in 20 (almost) equal contiguous parts and selecting a random 0 bit from each part and toggle that to 1. Thus the modified function from $g$ becomes balanced and in some of the cases the reduction in nonlinearity was less than 20. That provided the nonlinearity greater than the bent concatenation bound. Though the simple method provided nice results, it was only a heuristic and the idempotent structure of the PW functions was not exploited at all. In this paper we look at the idempotent structure of the PW functions and get better results over [17,28]. In this direction, first we interpret the PW functions as RSBFs in order to take the advantage of the matrix ${}_n\mathcal{A}$ associated with the Walsh transform of the functions. Then studying the distribution of the Walsh spectra values, we modify the PW functions to obtain new functions having high nonlinearity. Let us list the results we achieve in this paper that were not known earlier.

1. In Section 2.1, by modifying the two available PW functions from [23] we find 316 many RSBFs (idempotents) each having nonlinearity 16264 and 15 Walsh spectrum zeros. All these 316 functions have a different distribution in the Walsh spectra and they are not

affinely equivalent among themselves. These functions can be transformed to balanced functions and this nonlinearity 16264 is better than the nonlinearity 16262 presented in [17, 28]. Once more we like to point out that this study is a more disciplined one in terms of exploiting the structure of the idempotents rather than the simple heuristic presented in [17, 28]. Some of these functions have the maximum absolute value in the autocorrelation spectra as low as 192, which is better than 216 as presented in [17, 28]. Further we find functions having maximum possible algebraic immunity 8 where the maximum absolute value in the autocorrelation spectra is as low as 200. This is the first time a function on an odd number of variables having maximum possible algebraic immunity with nonlinearity greater than the bent concatenation bound is demonstrated. In [5], the functions of [17, 28] have been studied for their algebraic immunity and the value found was 7, which is not the maximum possible.

2. In Section 3, we further modify some of the 316 RSBFs (reported in Subsection 2.1) by toggling the outputs corresponding to two input points and could achieve balanced functions with nonlinearity 16266, algebraic immunity 8 and maximum absolute value in the autocorrelation spectra 208. Again, this is not done by randomly modifying two output points, but following a specific strategy examining the Walsh spectra of the functions. The nonlinearity presented here is the best known for 15-variable balanced functions and it provides the construction of $n$-variable ($n \geq 15$ and odd) balanced functions having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 10 \times 2^{\frac{n-15}{2}}$.

3. Each of the 15-variable functions presented in Section 2.1 and Section 3 (having nonlinearity either 16264 or 16266) has 15 many Walsh spectrum zeros. Unfortunately one needs at least 16 many zeros to have an attempt to get a 1-resilient function by the method of linear transformation on input variables. Thus we target some of the functions with certain distribution in the Walsh spectra having nonlinearity 16264 and modify each of them to increase the number of Walsh spectrum zeros keeping the rotation symmetric structure unchanged. We concentrate on the points where the Walsh spectrum values are close to zero and modify the function accordingly so that the values at those points can be changed to zero increasing the overall number of zeros in the Walsh spectrum. This technique has the risk that the nonlinearity will be reduced further, but we managed to control the reduction so that the resulting nonlinearity remains greater than the bent concatenation bound. In Section 4, we could modify the functions having nonlinearity 16264 from Section 2.1 to get functions with nonlinearity 16260 or 16264, each having 30 or more Walsh spectrum zeros. For example, we could get a function with nonlinearity 16264 with 135 many zeros in the Walsh spectrum that has then been suitably modified to 1-resilient function by linear transformation on input variables [16, 22]. This shows that it is possible to construct 1-resilient functions having nonlinearity greater than the bent concatenation bound for $(15 + 2i)$ variables ($i \geq 0$). The maximum absolute autocorrelation value of this function is 232. This shows for the first time the existence of a 1-resilient function exceeding the bent concatenation bound in nonlinearity with the maximum absolute value in the autocorrelation spectrum less than $2^{\frac{15+1}{2}}$.

Earlier 1-resilient 15-variable functions having nonlinearity greater than the bent concatenation bound were known for odd number of variables greater than or equal to 41 [28, 30]. In [28, 30], the 15-variable PW functions have been used in the construction of resilient functions but modification of the internal structure was not attempted to get resiliency. Thus 15-variable 1-resilient functions with nonlinearity more than the bent concatenation bound could not be

identified in [28, 30]. Our work is based on the modification of internal structure of PW functions and it shows the construction of 1-resilient functions on $n$ variables having nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for $n \geq 15$ and odd. Thus the gap from 15 to 39 variables is resolved by our work in terms of getting 1-resilient functions having nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$. Further our nonlinearity is better than what was presented for the 41-variable case in [28, 30].

## 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 [23]. 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 $\alpha$ 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 $\{0,1\}^n \to \{0,1\}$ by $f$.*
*$f$ 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 Walsh spectra of both the functions are the same (presented in Table 1).

For $n = 15$, the number of orbits is $g_n = 2192$, 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.

Table 1: Distribution of Walsh spectrum for 15-variable PW function.

| Weight $w$ | Number of Vectors (number of input points) | Walsh Spectra Value $2^{15} - 2w$ | How it comes (# of orbits of size 15, 5, 3, 1) |
|---|---|---|---|
| 16492 | 13021 | -216 | 868, 0, 0, 1 |
| 16428 | 217 | -88 | 12, 6, 2, 1 |
| 16364 | 3255 | 40 | 217, 0, 0, 0 |
| 16300 | 16275 | 168 | 1085, 0, 0, 0 |

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. A random strategy has been presented in [28] that we have briefly explained in the previous section. 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

We first start with a theoretical result.

**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*

$$(-1)^{f(\Lambda_{n,q})}\,{}_n\mathcal{A}_{q,j} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathcal{A}_{r,j} = 20,$$

*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 $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathcal{A}_{q,s} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathcal{A}_{r,s} < 20$ for all $s$, then $nl(g) > 2^{n-1} - 2^{\frac{n-1}{2}}$.*

**Proof:** Since, $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathcal{A}_{q,j} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathcal{A}_{r,j} = 20$, and $g = 1 \oplus f$ for the input points corresponding to the orbits represented by $\Lambda_{n,q}, \Lambda_{n,r}$, we have,

$$(-1)^{g(\Lambda_{n,q})}\,{}_n\mathcal{A}_{q,j} + (-1)^{g(\Lambda_{n,r})}\,{}_n\mathcal{A}_{r,j} = -20.$$

Also since $W_f(\Lambda_{n,j}) = 40$ and $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathcal{A}_{q,j} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathcal{A}_{r,j} = 20$, therefore we have $\sum_{i \notin \{q,r\}} (-1)^{f(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,j} = 20$. Thus,

$$W_g(\Lambda_{n,j}) = \Big((-1)^{g(\Lambda_{n,q})}\,{}_n\mathcal{A}_{q,j} + (-1)^{g(\Lambda_{n,r})}\,{}_n\mathcal{A}_{r,j}\Big) + \sum_{i \notin \{q,r\}} (-1)^{g(\Lambda_{n,i})}\,{}_n\mathcal{A}_{i,j} = -20 + 20 = 0.$$

This proves the first part of the theorem.

Now refer to Table 1 and note that for any $\omega$, 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, i.e., referring to Table 1, we have $W_f(\Lambda_{n,s}) = -216$ as $s$ varies. Let $(-1)^{f(\Lambda_{n,q})}\,{}_n\mathcal{A}_{q,s} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathcal{A}_{r,s} = 20 - \delta_s$, where $\delta_s > 0$. Thus,

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

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

Using the idea of the above theorem, we design an algorithm 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 $\omega$. 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 $W_f(\Lambda_{n,j}) = 40$. Next we choose one orbit $G_n(\Lambda_{n,q})$ of size 15 and another orbit $G_n(\Lambda_{n,r})$ of size 5 such that

$$(-1)^{f(\Lambda_{n,q})}\,{}_n\mathcal{A}_{q,j} + (-1)^{f(\Lambda_{n,r})}\,{}_n\mathcal{A}_{r,j} = 20.$$

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.

Now we present the actual algorithm.

**Algorithm 1**

$maxnl = 0$;
for each of the representative elements $\lambda$ such that $W_f(\lambda) = 40$
    for each pair of the representative elements $\delta, \gamma$ with $|G_n(\delta)| = 15, |G_n(\gamma)| = 5$
        sum $= (-1)^{f(\delta)} \sum_{x \in G_n(\delta)} (-1)^{x \cdot \lambda} + (-1)^{f(\gamma)} \sum_{x \in G_n(\gamma)} (-1)^{x \cdot \lambda}$;
        if sum $= 20$
            $g(x) = f(x)$ for $x \in \{0,1\}^n \setminus (G_n(\delta) \cup G_n(\gamma))$;
            $g(x) = 1 \oplus f(x)$ for $x \in G_n(\delta) \cup G_n(\gamma)$;
            if $maxnl < nl(g)$, then $maxnl = nl(g)$
                store $\delta$, $\gamma$ and $nl(g)$ in a file F;
for each $\delta$, $\gamma$, $nl(g)$ tuple in a file F
    if $nl(g) < maxnl$
        remove the tuple from file F;
file F provides the RSBFs with nonlinearity $maxnl$ with at least 15 Walsh zeros;

**Complexity of Algorithm 1**

We define the following sets.

$$S_1 = \{\Lambda_{n,d} : W_f(\Lambda_{n,d}) = 40\}, S_2 = \{\Lambda_{n,d} : |G_n(\Lambda_{n,d})| = 15\} \text{ and } S_3 = \{\Lambda_{n,d} : |G_n(\Lambda_{n,d})| = 5\}.$$

Then we need to check $|S_1| \times |S_2| \times |S_3|$, i.e., $217 \times 2182 \times 6 < 2^{22}$ many options. For each of the options, we need to calculate the nonlinearity of $g$, requiring $O(n2^n)$ time using the Fast Walsh Transform which is around $2^{19}$. Thus the total time complexity is around $2^{41}$, which is negligible compared to any search in the space of 15-variable Boolean functions.

**Outcome of Algorithm 1**

Running Algorithm 1 we get 253 and 63 RSBFs $g$ respectively from degree 8 and degree 9 PW functions with nonlinearity $maxnl = 16264$ 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.

Refer to Appendix A to get the list of these 316 functions with nonlinearity 16264. We studied these functions and the distribution of the functions $g$ with respect to $\Delta_g$ is given in the following table.

Table 2: Number of RSBFs $g$ with nonlinearity 16264 with corresponding $\Delta_g$ values.

| $\Delta_g$ | 192 | 200 | 208 | 216 | 224 | 232 | 240 | 248 | 256 | 280 |
|---|---|---|---|---|---|---|---|---|---|---|
| Number of functions $g$ | 1 | 21 | 87 | 101 | 60 | 34 | 8 | 2 | 1 | 1 |

Now consider $\omega \in \{0,1\}^n$ such that $W_g(\omega) = 0$. Then it is clear that the function $g'(x) = g(x) \oplus \omega \cdot x$ will be balanced and $nl(g') = nl(g) = 16264$, $\Delta_{g'} = \Delta_g = 192$. Thus we get balanced functions $g'$ having better nonlinearity and autocorrelation values than presented in [28]. Note that, though $g$ is an RSBF, the rotational symmetric property may be lost in $g'$.

*In all the following examples of this paper, we express any element $x \in \{0,1\}^n$ as the $n$-bit binary vector $(x_n, x_{n-1}, \ldots, x_1)$, where $x_n$ is the most significant bit.*

**Example 1** Now we provide the exact specification of a function $g$ having nonlinearity 16264 and $\Delta_g = 192$. First we construct the RSBF $f$ from the PW function of degree 9 by using

Construction 1. Then we toggle the outputs of $f$ corresponding to the orbits represented by $(0,0,0,0,1,1,1,0,0,1,1,0,0,1,1)$ (of size 15) and $(0,0,0,0,1,0,0,0,0,1,0,0,0,0,1)$ (of size 5) to get $g$. The function $g$ has the Walsh spectrum values zero corresponding to the orbit represented by $(0,0,0,0,1,1,1,0,1,1,0,0,1,0,1)$ (of size 15). The algebraic degree of $g$ is 13. If we consider $\omega = (0,0,0,0,1,1,1,0,1,1,0,0,1,0,1)$, then $g'(x) = g(x) \oplus \omega \cdot x$ will be balanced. We have also noted that the algebraic immunity of $g'$ is 7, which is not the maximum possible.

**Example 2** Next we present a function with the maximum possible algebraic immunity 8. We take the RSBF $f$ obtained from the 9-degree PW function using Construction 1. Then we toggle the outputs of $f$ corresponding to the orbits represented respectively by the elements $(0,0,0,0,1,1,0,0,1,1,0,1,0,1,1)$ (of size 15) and $(0,1,0,1,1,0,1,0,1,1,0,0,1,0,1,1)$ (of size 5) to get $g$. This function has the Walsh spectrum values zero for the orbit represented by $(0,0,0,0,1,1,1,0,1,1,0,0,1,0,1)$ (of size 15). For this function $g$, we have nonlinearity 16264, $\Delta_g = 200$ and algebraic degree 13. Let $\omega = (0,0,0,0,1,1,1,0,1,1,0,0,1,0,1)$, then $g'(x) = g(x) \oplus \omega \cdot x$ will be balanced and $g'$ possesses maximum possible algebraic immunity 8. This is the first demonstration of a Boolean function on an odd number of variables having nonlinearity greater than the bent concatenation bound and maximum possible algebraic immunity.

## 3 Further improvement of nonlinearity

Now we study the functions which are the outputs of Algorithm 1. We modify these functions to get 15-variable balanced functions with nonlinearity better than 16264. Let us first explain the theoretical idea behind this.

*For this section, by $g$, we denote any function which is an output of Algorithm 1.*

**Theorem 2** *Consider a function $g$. Let both of the maximum and second maximum absolute values in the Walsh spectrum of $g$ be negative in sign and let the values be $-v$ and $-v+\delta$, where $v, \delta > 0$. Let $W_g(\omega) = -v$ for $\omega \in \{\omega^{(1)}, \ldots, \omega^{(t)}\}$. Consider the set $\{x^{(1)}, \ldots, x^{(s)}\}$ such that for any $x \in \{x^{(1)}, \ldots, x^{(s)}\}$, the values $\omega \cdot x$ are the same and $g(x) = 1 \oplus \omega \cdot x$ for all $\omega \in \{\omega^{(1)}, \ldots, \omega^{(t)}\}$.*

*Consider $|\{x^{(1)}, \ldots, x^{(s)}\}| \geq \frac{\delta}{4}$ and let $Q$ be a $\frac{\delta}{4}$ size subset of $\{x^{(1)}, \ldots, x^{(s)}\}$. Construct*

$$\begin{aligned} g'(x) &= g(x) \text{ for } x \in \{0,1\}^n \setminus Q, \\ &= 1 \oplus g(x) \text{ for } x \in Q. \end{aligned}$$

*Then the maximum Walsh spectrum value of $g'$ at the points $\omega \in \{\omega^{(1)}, \ldots, \omega^{(t)}\}$ will be the absolute value of $-v + \frac{\delta}{2}$ and the maximum absolute value of Walsh spectrum of $g'$ will be $v - \frac{\delta}{2}$.*

*If there exists an input point $\zeta$ with $W_g(\zeta) = 0$ and $\sum_{x \in Q} (-1)^{g(x) \oplus \zeta \cdot x} = 0$, then $W_{g'}(\zeta) = 0$.*

**Proof:** For any $\omega \in \{\omega^{(1)}, \ldots, \omega^{(t)}\}$ and any $x \in Q$, we have

$$(-1)^{g(x) \oplus \omega \cdot x} = (-1)^{1 \oplus \omega \cdot x \oplus \omega \cdot x} = -1.$$

Thus, $\sum_{x \in Q} (-1)^{g(x) \oplus \omega \cdot x} = -\frac{\delta}{4}$. Then,

$$\begin{aligned} W_{g'}(\omega) &= \textstyle\sum_{x \in \{0,1\}^n \setminus Q} (-1)^{g'(x) \oplus \omega \cdot x} + \sum_{x \in Q} (-1)^{g'(x) \oplus \omega \cdot x} \\ &= \textstyle\sum_{x \in \{0,1\}^n \setminus Q} (-1)^{g(x) \oplus \omega \cdot x} - \left( \sum_{x \in Q} (-1)^{g(x) \oplus \omega \cdot x} \right) \\ &= W_g(\omega) - 2 \left( \textstyle\sum_{x \in Q} (-1)^{g(x) \oplus \omega \cdot x} \right) \\ &= W_g(\omega) - 2 \cdot (-\tfrac{\delta}{4}) = -v + \tfrac{\delta}{2}. \end{aligned}$$

Due to the toggling of $\frac{\delta}{4}$ output bits of $g$ to get $g'$, other Walsh spectrum values ($-v+\delta$, the next maximum Walsh spectrum value in absolute terms) can be modified to $-v+\frac{\delta}{2}$ in $g'$ (at most in absolute terms).

Again since, $W_g(\zeta) = 0$ and $\sum_{x\in Q}(-1)^{g(x)\oplus\zeta\cdot x} = 0$, then $\sum_{x\in\{0,1\}^n\setminus Q}(-1)^{g(x)\oplus\zeta\cdot x} = 0$. Therefore

$$\begin{aligned} W_{g'}(\zeta) &= \sum_{x\in\{0,1\}^n\setminus Q}(-1)^{g'(x)\oplus\zeta\cdot x} + \sum_{x\in Q}(-1)^{g'(x)\oplus\zeta\cdot x} \\ &= \sum_{x\in\{0,1\}^n\setminus Q}(-1)^{g(x)\oplus\zeta\cdot x} - \left(\sum_{x\in Q}(-1)^{g(x)\oplus\zeta\cdot x}\right) \\ &= 0-0=0. \end{aligned}$$

■

Note that the maximum absolute value in the Walsh spectrum of $g$ is 240 and the sign is negative. While modifying $g$ we will keep in mind the following points.

1. We attempt to toggle two output points of $g$ to get an increment of 2 in nonlinearity having one or more zeros in the Walsh spectrum. We refer to this modified function as $g'$. The function $g'$ is not an RSBF as this function will have two input orbits of size $> 1$ where the outputs are not constant.

2. The points $\omega$ for which $W_g(\omega) = -240$ should provide $W_{g'}(\omega) = -236$.

3. The points $\omega$ for which $W_g(\omega) = -236$ should provide $W_{g'}(\omega) = -236$ or $W_{g'}(\omega) = -232$. After toggling two points in the output of $g$, if we get $W_{g'}(\omega) = -240$ for any such $\omega$, then the increment in nonlinearity will not be possible. Note that this issue can be avoided if there is no $\omega$ for which $W_g(\omega) = -236$. This is the reason we only consider the functions $g$ where there is no $\omega$ such that $W_g(\omega) = -236$. That is for each of these functions, the second maximum absolute value in the Walsh spectrum corresponds to -232. We find that there are plenty of such functions among the 316 functions reported in the previous section.

4. For each of the functions $g$, the Walsh spectrum values are in the range $[-240, 208]$. The points $\omega$ for which $-232 \le W_g(\omega) \le 208$ will provide $-236 \le W_{g'}(\omega) \le 212$ and they will not create any trouble if we want to have an increment in nonlinearity by 2 by toggling two output bits of $g$.

We select a function $g$ such that the second maximum absolute Walsh spectrum value of $g$ corresponds to $-232$. Referring to Appendix A will provide a handful of such functions. From the above argument it is clear that we need to concentrate on the $\omega$'s for which $W_g(\omega) = -240$. Let us consider that there are $t$ such $\omega$'s denoted by $\omega^{(1)}, \ldots, \omega^{(t)}$. We would like to get input points $x$ such that for all $\omega \in \{\omega^{(1)}, \ldots, \omega^{(t)}\}$ the values $\omega \cdot x$ are the same and also $g(x) = 1 \oplus \omega \cdot x$. Say there are $s$ such input points $x^{(1)}, \ldots, x^{(s)}$. We choose two input points $x^{(i)}, x^{(j)}$, $1 \le i \ne j \le s$ such that $(-1)^{g(x^{(i)})\oplus\zeta\cdot x^{(i)}} + (-1)^{g(x^{(j)})\oplus\zeta\cdot x^{(j)}} = 0$ where $W_g(\zeta) = 0$ and prepare $g'$ as follows:

$$\begin{aligned} g'(x) &= g(x) && \text{when } x \in \{0,1\}^n \setminus \{x^{(i)}, x^{(j)}\} \\ &= 1 \oplus g(x) && \text{when } x \in \{x^{(i)}, x^{(j)}\}. \end{aligned}$$

Then following Theorem 2, $g'$ will have nonlinearity increased by 2 over that of $g$ as $W_{g'}(\omega) = -236$ for $\omega \in \{\omega^{(1)}, \ldots, \omega^{(t)}\}$ and for all other $\omega$'s the maximum absolute value of $W_{g'}(\omega)$ cannot exceed 236. Moreover the fact that $(-1)^{g(x^{(i)})\oplus\zeta\cdot x^{(i)}} + (-1)^{g(x^{(j)})\oplus\zeta\cdot x^{(j)}} = 0$ will ensure that $W_{g'}(\zeta) = 0$.

*Construct the set $S$ of 15-variable functions $g$ with nonlinearity 16264 obtained by running Algorithm 1 such that the second maximum absolute value in the Walsh spectrum of each of them corresponds to $-232$.* We present the algorithm which takes a function $g \in S$ and returns a function with nonlinearity 16266 with some Walsh spectrum values equal to zero.

**Algorithm 2**

*choose a function $g \in S$*
*form the set $\{\omega^{(1)}, \ldots, \omega^{(t)}\}$ which is the set of all $\omega$ such that $W_g(\omega) = -240$;*
*form the set $\{x^{(1)}, \ldots, x^{(s)}\}$ such that*
*for all $\omega \in \{\omega^{(1)}, \ldots, \omega^{(t)}\}$*
*(i) the values of $\omega \cdot x$, are the same and*
*$g(x) = 1 \oplus \omega \cdot x$ for all $x \in \{x^{(1)}, \ldots, x^{(s)}\}$;*
*for any pair $x^{(i)}, x^{(j)} \in \{x^{(1)}, \ldots, x^{(s)}\}$, $(i \neq j)$ if*
*$(-1)^{g(x^{(i)}) \oplus \zeta \cdot x^{(i)}} + (-1)^{g(x^{(j)}) \oplus \zeta \cdot x^{(j)}} = 0$, for some $\zeta$ with $W_g(\zeta) = 0$*
*construct*
$g'(x) = g(x)$ *when* $x \in \{0,1\}^n \setminus \{x^{(i)}, x^{(j)}\}$
$= 1 \oplus g(x)$ *when* $x \in \{x^{(i)}, x^{(j)}\}$
*report $g'(x)$ as a function having nonlinearity 16266 and $W_{g'}(\zeta) = 0$;*

**Complexity of Algorithm 2**

Let $N = \{\omega^{(1)}, \ldots, \omega^{(t)}\}$. While forming the set $M = \{x^{(1)}, \ldots, x^{(s)}\}$, we require $N$ checks for each $x^{(i)} \in M$, i.e., in total $M \cdot N$ checks. Also to get the points $\zeta$ and $\omega$ such that $W_g(\zeta) = 0$ and $W_g(\omega) = -240$, we require $O(n2^n)$ time using the Fast Walsh Transform which is around $2^{19}$. Now for any pair $x^{(i)}, x^{(j)} \in \{x^{(1)}, \ldots, x^{(s)}\}$, the checking for $(-1)^{g(x^{(i)}) \oplus \zeta \cdot x^{(i)}} + (-1)^{g(x^{(j)}) \oplus \zeta \cdot x^{(j)}} = 0$, for $\zeta$ with $W_g(\zeta) = 0$ requires constant time. Thus the total time complexity for Algorithm 2 is $(2^{19} + |M| \cdot |N|) < 2^{19} + (2192)^2 < 2^{23}$. There are 232 functions $g$ in $S$. Therefore if we run Algorithm 2 for all the 232 functions $g$, the complexity will be around $2^{31}$.

**Example 3** It is clear that the possibility of getting a larger set $\{x^{(1)}, \ldots, x^{(s)}\}$ increases when the size of the set $\{\omega^{(1)}, \ldots, \omega^{(t)}\}$ becomes smaller. In this manner we found functions $g$ such that $W_g(\omega) = -240$ is at only 30 points. We choose such a function $g$ with the following description. We consider the PW function having degree 9 and the function is transformed to an RSBF $f$ as described in Construction 1. The outputs of $f$ are toggled corresponding to the orbits represented by $(0,0,1,1,1,1,1,1,1,1,1,0,1,0,1)$ (of size 15) and $(0,1,0,1,1,0,1,0,1,1,0,1,0,1,1)$ (of size 5) to get $g$. Note that $nl(g) = 16264$ and $\Delta_g = 200$.

As per our description, we get $t = 30$ points $\omega^{(1)}, \ldots, \omega^{(t)}$, for which the Walsh spectrum value of $g$ is -240. Based on these we get $s = 82$ many $x^{(1)}, \ldots, x^{(s)}$ and toggling the outputs of $g$ at any two of these 82 points increases the nonlinearity by 2. As example we take the two input points $(0,0,0,0,0,1,1,0,0,1,1,1,0,0,1)$ and $(0,0,0,1,0,0,0,1,0,1,1,1,0,0,0)$ and toggle the outputs of $g$ at these two points to obtain $g'$. The function $g'$ has nonlinearity 16266 having 15 Walsh spectrum zeros, $\Delta_{g'} = 208$ and algebraic degree 14. Next we construct the balanced functions $g''$, such that $g''(x) = g'(x) \oplus \omega \cdot x$, where, $W_{g'}(\omega) = 0$. We choose such an $\omega = (0,0,0,1,1,1,0,1,1,0,0,1,0,1,0)$, and for this the function $g''(x)$ has maximum possible algebraic immunity equal to 8.

Once we have $g''$, we can construct a balanced function on $n$-variables (odd $n > 15$) as $b(x_{16}, \ldots, x_n) \oplus g''(x_1, \ldots, x_{15})$ with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 10 \times 2^{\frac{n-15}{2}}$, where $b$ is a bent function.

## 4 Strategy to get 1-resilient functions

Any 15-variable RSBF $g$ with nonlinearity 16264 from the list of Appendix A (i.e., output of Algorithm 1) 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 from Appendix A 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 of Appendix A, 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 constitutes 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 [29] 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 3** *Consider a function $g \in S'$ such that $W_g(\Lambda_{n,p}) = 0$ and $W_g(\Lambda_{n,j}) = 16$. Let*

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

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

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

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

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

We consider a function $g \in S'$. Then the orbit $G_n(\Lambda_{n,p})$ such that $W_g(\Lambda_{n,p}) = 0$ is of size 15 and also the orbits $G_n(\Lambda_{n,j})$ such that $W_g(\Lambda_{n,j}) = 16$ are of size 15. Now we form the sets $\{q_1, \ldots, q_t\}$ and $\{r_1, \ldots, r_l\}$ such that for each $q \in \{q_1, \ldots, q_t\}$ and $r \in \{r_1, \ldots, r_l\}$, we have, $|{}_n\mathcal{A}_{q,j}| = 5$ and $|{}_n\mathcal{A}_{r,j}| = 3$. Then we consider those pairs for which

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

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

Then by Theorem 3, 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). Based on this discussion we present the following algorithm.

**Algorithm 3**

$n = 15$;
choose a function $g \in S'$;
  find an orbit representative $\Lambda_{n,j}$ such that $W_g(\Lambda_{n,j}) = 16$;
  find the orbit representative $\Lambda_{n,p}$ such that $W_g(\Lambda_{n,p}) = 0$;
  form the set $\{q_1, \ldots, q_t\}$ and $\{r_1, \ldots, r_l\}$ such that
    $|{}_n\mathcal{A}_{q,j}| = 5$ and $|{}_n\mathcal{A}_{r,j}| = 3$ for all $q \in \{q_1, \ldots, q_t\}$ and $r \in \{r_1, \ldots, r_l\}$
  for each $q \in \{q_1, \ldots, q_t\}$ and for each $r \in \{r_1, \ldots, r_l\}$ if
    1. $(-1)^{g(\Lambda_{n,q})}\,{}_n\mathcal{A}_{q,j} + (-1)^{g(\Lambda_{n,r})}\,{}_n\mathcal{A}_{r,j} = 8$
    2. $(-1)^{g(\Lambda_{n,q})}\,{}_n\mathcal{A}_{q,p} + (-1)^{g(\Lambda_{n,r})}\,{}_n\mathcal{A}_{r,p} = 0$
    Construct
      $h(x) = g(x)$ for $x \in \{0,1\}^n \setminus G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r})$,
        $= 1 \oplus g(x)$ for $x \in G_n(\Lambda_{n,q}) \cup G_n(\Lambda_{n,r})$;
    if $nl(h) \geq 16260$ and 4 divides $nl(g)$
      store $h$ in file $F$;
file $F$ provides 15-variable functions with nonlinearity $\geq 16260$
  and having Walsh spectrum zeros in at least 30 points for each of the functions;

**Complexity of Algorithm 3**

The computational effort of this algorithm depends on the number of orbits $G_n(\Lambda_{n,q})$ and $G_n(\Lambda_{n,r})$ such that $|{}_n\mathcal{A}_{q,j}| = 5$ and $|{}_n\mathcal{A}_{r,j}| = 3$, i.e., we have to check $t \times l$ many options which can attain the maximum value $(\frac{2192}{2})^2$. Also within the loop, determination of the nonlinearity of the modified function $h$ requires $O(n2^n)$, i.e., around $2^{19}$ time by using Fast Walsh Transform. Thus total complexity for Algorithm 2 is $t \times l \times 2^{19} < (\frac{2192}{2})^2 \times 2^{19} < 2^{40}$. There are 292 functions $g \in S'$. Therefore if one wishes to run Algorithm 3 for all these functions, the time complexity will be less than $2^{49}$.

Given an $n$-variable Boolean function $\phi$, let us define

$$S_\phi = \{\omega \in \{0,1\}^n \mid W_\phi(\omega) = 0\}.$$

If there exist $n$ linearly independent vectors in $S_\phi$, then one can construct a nonsingular $n \times n$ matrix $B_\phi$ whose rows are linearly independent vectors from $S_\phi$. Let, $C_\phi = B_\phi^{-1}$. Now one can define $\phi'(x) = \phi(C_\phi x)$. Both $\phi'$ and $\phi$ *have the same weight, nonlinearity and algebraic degree.* Moreover, $W_{\phi'}(\omega) = 0$ for $wt(\omega) = 1$. This ensures that $\phi'$ is correlation immune of order 1. Further if $\phi$ is balanced then $\phi'$ is 1-resilient. This technique has been used in [16, 22].

We run Algorithm 3 for few functions $g \in S'$. In the following example we describe it.

**Example 4** Let $n = 15$. We consider the RSBF $f$ obtained from the 9-degree PW function using Construction 1. We run Algorithm 3 for a small subset of $S'$. 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 $g \in S'$ which is obtained by toggling

the outputs of $f$ corresponding to the orbits of size 15 and 5 having representative elements respectively $(0,0,0,0,0,1,1,1,0,1,0,0,1,1,1)$ and $(0,1,0,1,1,0,1,0,1,1,0,1,0,1,1)$. We have $nl(g) = 16264$ and $W_g$ contains 15 many zeros. We apply Algorithm 3 over the function $g$ to get $h$ such that $nl(h) = 16264$ and $W_h$ contains 135 many zeros. The function $h$ is obtained by toggling the outputs of $g$ corresponding to the orbits represented by the tuples $(0,0,1,1,0,1,0,1,1,1,0,1,1,1,1)$ and $(0,0,0,0,1,1,1,1,0,1,1,0,0,1,1)$ each of size 15. We note that $W_h(\omega) = 0$ for $\omega = (0,0,0,0,0,1,0,0,0,0,1,1,0,1,1)$. Thus the function $\phi = h \oplus \omega \cdot x$ will be balanced. Then as described above, we find 15 linearly independent vectors from $S_\phi$ and hence a 1-resilient function $\phi'$ having nonlinearity 16264 is found. We note that for $\phi'$, $\Delta_{\phi'} = 232$ with algebraic degree 12 and algebraic immunity 7. See Appendix B for the truth table of this function. 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 [15], existence of 1-resilient functions having the maximum absolute value in the autocorrelation spectra $< 2^{\frac{n+1}{2}}$ has been demonstrated for $n = 9, 11$. However, the nonlinearity in those cases did not exceed the bent concatenation bound.

In [28, 30], 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 $\psi_1$ 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. Example 4 above shows the existence of a 15-variable function with nonlinearity that exceeds the bent concatenation bound. Again for odd $n > 15$, the function $b(x_{16}, \ldots, x_n) \oplus \phi'(x_1, \ldots, x_{15})$, where $b(x_{16}, \ldots, x_n)$ is a bent function, will be 1-resilient with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 8 \times 2^{\frac{n-15}{2}}$. This shows that 1-resilient functions are available for 15 or more variables. Thus the gap between 15 to 39 variables is now settled. Further we show that using the function $\phi'$ we can construct a 41-variable 1-resilient function with nonlinearity that exceeds the lower bound of $nl(\psi_1)$. Let $\psi_2 = b(x_{16}, \ldots, x_{41}) \oplus \phi'(x_1, \ldots, x_{15})$, where $b(x_{16}, \ldots, x_{41})$ is a bent function, 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 $nl(\psi_1)$.

# 5 Conclusion

In this paper we successfully modify the two 15-variable PW functions [23] to construct balanced functions $f$ with nonlinearities 16264 and 16266. Corresponding to these nonlinearities, we get the $\Delta_f$ values as low as 192 and 208 respectively. Some of these functions provide the maximum algebraic immunity 8. All these parameters are the best known till date and clearly improve the parameters reported in [17, 28]. 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 [28, 30].

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.

## References


[1] Berlekamp, E.R., Welch, L.R.: Weight distributions of the cosets of the $(32, 6)$ Reed-Muller code. IEEE Transactions on Information 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 Transactions on Information Theory **52**(7), 3105–3121 (2006)

[3] Courtois, N., Meier, W.: Algebraic attacks on stream ciphers with linear feedback. In: E. Biham (ed.) EUROCRYPT, *Lecture Notes in Computer Science*, vol. 2656, pp. 345–359. Springer (2003)

[4] Cusick, T.W., Stănică, P.: Fast evaluation, weights and nonlinearity of rotation-symmetric functions. Discrete Mathematics **258**(1-3), 289–301 (2002)

[5] Dalai, D.K., Gupta, K.C., Maitra, S.: Results on rotation symmetric bent functions. In: Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA'06, pp. 107–124. Publications of Universities of Rouen and Havre (2006)

[6] Dalai, D.K., Maitra, S., Sarkar, S.: Results on rotation symmetric bent functions. In: Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA'06, pp. 137–156. Publicaions of Universities of Rouen and Havre (2006)

[7] Dillon, J.F.: Elementary hadamard difference sets. Ph.D. thesis, University of Maryland (1974)

[8] Dobbertin, H.: Construction of bent functions and balanced Boolean functions with high nonlinearity. In: B. Preneel (ed.) Fast Software Encryption, *Lecture Notes in Computer Science*, vol. 1008, pp. 61–74. Springer (1994)

[9] Filiol, E., Fontaine, C.: Highly nonlinear balanced Boolean functions with a good correlation-immunity. In: K. Nyberg (ed.) EUROCRYPT, *Lecture Notes in Computer Science*, vol. 1403, pp. 475–488. Springer (1998)

[10] Fontaine, C.: The nonlinearity of a class of Boolean functions with short representation. In: J. Přibyl (ed.) PRAGOCRYPT'96, pp. 129–144. CTU Publishing House (1996)

[11] Fontaine, C.: On some cosets of the first-order Reed-Muller code with high minimum weight. IEEE Transactions on Information Theory **45**(4), 1237–1243 (1999)

[12] Hell, M., Maximov, A., Maitra, S.: On efficient implementation of search strategy for rotation symmetric Boolean functions. In: Proceedings of Ninth International Workshop on Algebraic and Combinatoral Coding Theory, ACCT 2004, pp. 19–25 (2004)

[13] Kavut, S., Maitra, S., Sarkar, S., Yücel, M.D.: Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity $> 240$. In: R. Barua, T. Lange (eds.) INDOCRYPT, *Lecture Notes in Computer Science*, vol. 4329, pp. 266–279. Springer (2006)

[14] Kavut, S., Maitra, S., Yücel, M.D.: Autocorrelation spectra of balanced Boolean functions on odd number input variables with maximum absolute value $< 2^{\frac{n+1}{2}}$. In: Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06, pp. 73–86. Publications of Universities of Rouen and Havre (2006)

[15] Kavut, S., Maitra, S., Yücel, M.D.: Search for Boolean functions with excellent profiles in the rotation symmetric class. IEEE Transactions on Information Theory **53**(5), 1743–1751 (2007)

[16] Maitra, S., Sarkar, P.: Cryptographically significant Boolean functions with five valued walsh spectra. Theoretical Computer Sciience **276**(1-2), 133–146 (2002)

[17] Maitra, S., Sarkar, P.: Modifications of patterson-wiedemann functions for cryptographic applications. IEEE Transactions on Information Theory **48**(1), 278–284 (2002)

[18] Maximov, A.: Classes of plateaued rotation symmetric Boolean functions under transformation of walsh spectra. In: International Workshop on Coding and Cryptography, WCC 2005, pp. 325–334 (2005)

[19] Maximov, A., Hell, M., Maitra, S.: Plateaued rotation symmetric Boolean functions on odd number of variables. In: First International Workshop on Boolean Functions: Cryptography and Applications, BFCA 05, pp. 83–104. Publications of Universities of Rouen and Havre (2005)

[20] Meier, W., Pasalic, E., Carlet, C.: Algebraic attacks and decomposition of Boolean functions. In: C. Cachin, J. Camenisch (eds.) EUROCRYPT, *Lecture Notes in Computer Science*, vol. 3027, pp. 474–491. Springer (2004)

[21] Mykkeltveit, J.J.: The covering radius of the $(128, 8)$ Reed-Muller code is 56. IEEE Transactions on Information Theory **26**(3), 359–362 (1980)

[22] Pasalic, E., Johansson, T.: Further results on the relation between nonlinearity and resiliency for Boolean functions. In: M. Walker (ed.) IMA International Conference, *Lecture Notes in Computer Science*, vol. 1746, pp. 35–44. Springer (1999)

[23] Patterson, N.J., Wiedemann, D.H.: The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. IEEE Transactions on Information Theory **29**(3), 354–356 (1983). See also the correction in [24]

[24] Patterson, N.J., Wiedemann, D.H.: Correction to 'the covering radius of the ($2^{15}$, 16) Reed-Muller code is at least 16276' (may 83 354-356). IEEE Transactions on Information Theory **36**(2), 443 (1990)

[25] Pieprzyk, J., Qu, C.X.: Rotation-symmetric functions and fast hashing. Jornal of Universal Computer Science **5**(1), 20–31 (1999)

[26] Preneel, B., Leekwijck, W.V., Linden, L.V., Govaerts, R., Vandewalle, J.: Propagation characteristics of Boolean functions. In: Advances in Cryptology-EUROCRYPT, *Lecture Notes in Computer Science*, vol. 473, pp. 161–173 (1990)

[27] Rothaus, O.S.: On "bent" functions. Journal of Combinatorial Theory, Series A **20**(3), 300–305 (1976)

[28] 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)

[29] Sarkar, P., Maitra, S.: Nonlinearity bounds and constructions of resilient Boolean functions. In: M. Bellare (ed.) CRYPTO, *Lecture Notes in Computer Science*, vol. 1880, pp. 515–532. Springer (2000)

[30] Sarkar, P., Maitra, S.: Construction of nonlinear resilient Boolean functions using "small" affine functions. IEEE Transactions on Information Theory **50**(9), 2185–2193 (2004)

[31] Seberry, J., Zhang, X., Zheng, Y.: Nonlinearly balanced Boolean functions and their propagation characteristics (extended abstract). In: D.R. Stinson (ed.) CRYPTO, *Lecture Notes in Computer Science*, vol. 773, pp. 49–60. Springer (1993)

[32] Stănică, P., Maitra, S.: Rotation symmetric Boolean functions – count and cryptographic properties. In: R. C. Bose Centenary Symposium on Discrete Mathematics and Applications, *Electronic Notes in Discrete Mathematics*, vol. 15. Elsevier (2002)

[33] Stănică, P., Maitra, S., Clark, J.A.: Results on rotation symmetric bent and correlation immune Boolean functions. In: B.K. Roy, W. Meier (eds.) FSE, *Lecture Notes in Computer Science*, vol. 3017, pp. 161–177. Springer (2004)

[34] Xiao, G.Z., Massey, J.L.: A spectral characterization of correlation-immune combining functions. IEEE Transactions on Information Theory **34**(3), 569–571 (1988)

[35] Zhang, K., Zheng, Y.: Gac - the criterion for global avalance characteristics of cryptographic functions. Jornal of Universal Computer Science **1**(5), 320–337 (1995)

# Appendix A

In Table 3, 253 pairs in the upper part and 63 pairs in the lower part correspond to 15-variable functions with nonlinearity 16264 obtained respectively from the 8-degree and 9-degree PW functions. In each pair the first integer indicates the decimal value of the representative of the orbit of size 15 and the second one indicates the decimal value of the representative of the orbit of size 5. The decimal value corresponding to an $n$-bit binary vector $(x_n, x_{n-1}, \ldots, x_1) \in \{0,1\}^n$ is determined by taking $x_n$ as the most significant bit. Pairs marked (*) indicate the functions with the second maximum absolute Walsh spectrum value corresponding to $-232$. Pairs marked (+) indicate functions having 16 in their Walsh spectra.

| | | | | | |
|---|---|---|---|---|---|
| $(1819, 19)^{*+}$ | $(2249, 2485)^{*+}$ | $(2789, 173)^{*+}$ | $(3059, 2893)^{*+}$ | $(5755, 1269)^{*+}$ | $(5997, 2923)^{+}$ |
| $(1819, 53)^{+}$ | $(2249, 2893)^{*+}$ | $(2789, 329)^{+}$ | $(3059, 3359)^{+}$ | $(5755, 1297)^{+}$ | $(5997, 3385)^{*+}$ |
| $(1819, 173)^{*+}$ | $(2249, 3385)^{*+}$ | $(2789, 575)^{*+}$ | $(3059, 3385)^{*+}$ | $(5755, 1417)^{*+}$ | $(5997, 3411)^{*+}$ |
| $(1819, 225)^{+}$ | $(2249, 3411)^{*+}$ | $(2789, 1099)^{*+}$ | $(3059, 3411)^{*+}$ | $(5755, 1507)^{*+}$ | $(5997, 3689)^{*+}$ |
| $(1819, 329)^{+}$ | $(2249, 3531)$ | $(2789, 1297)^{+}$ | $(3059, 3689)^{*+}$ | $(5755, 1639)^{*+}$ | $(5997, 3799)^{*+}$ |
| $(1819, 987)^{+}$ | $(2249, 3689)^{*+}$ | $(2789, 1417)^{*+}$ | $(3059, 3799)^{*+}$ | $(5755, 1715)^{*+}$ | $(5997, 4795)^{+}$ |
| $(1819, 1099)^{*+}$ | $(2249, 3739)^{+}$ | $(2789, 1507)^{*+}$ | $(3059, 4071)^{+}$ | $(5755, 1957)^{*+}$ | $(5997, 4855)^{*+}$ |
| $(1819, 1183)^{*+}$ | $(2249, 3799)^{*+}$ | $(2789, 1639)^{*+}$ | $(3059, 4855)^{*+}$ | $(5755, 1999)^{*+}$ | $(5997, 5037)^{+}$ |
| $(1819, 1269)^{*+}$ | $(2249, 4855)^{*+}$ | $(2789, 1715)^{*+}$ | $(3059, 5725)^{+}$ | $(5755, 2211)^{*+}$ | $(5997, 5631)^{*+}$ |
| $(1819, 1417)^{*+}$ | $(2249, 5631)^{+}$ | $(2789, 1753)^{*+}$ | $(3059, 7151)^{*+}$ | $(5755, 2485)^{*+}$ | $(5997, 7613)^{+}$ |
| $(1819, 1507)^{*+}$ | $(2249, 6837)^{+}$ | $(2789, 1853)^{+}$ | $(3059, 8119)^{*+}$ | $(5755, 2685)^{+}$ | $(5997, 8119)^{*+}$ |
| $(1819, 1639)^{*+}$ | $(2249, 7151)^{*+}$ | $(2789, 1999)^{+}$ | $(3059, 12255)^{+}$ | $(5755, 2893)^{+}$ | $(8157, 173)^{*+}$ |
| $(1819, 1715)^{*+}$ | $(2249, 7613)^{+}$ | $(2789, 2211)^{+}$ | $(3773, 19)^{*+}$ | $(5755, 3385)^{*+}$ | $(8157, 503)^{+}$ |
| $(1819, 1753)^{*+}$ | $(2249, 8119)^{*+}$ | $(2789, 2485)^{*+}$ | $(3773, 329)^{+}$ | $(5755, 3411)^{*+}$ | $(8157, 575)^{*+}$ |
| $(1819, 1957)^{*+}$ | $(2527, 19)^{*+}$ | $(2789, 2685)^{+}$ | $(3773, 575)^{*+}$ | $(5755, 3689)^{*+}$ | $(8157, 1099)^{+}$ |
| $(1819, 1999)^{*+}$ | $(2527, 173)^{*+}$ | $(2789, 2893)^{*+}$ | $(3773, 1099)^{*+}$ | $(5755, 3739)^{+}$ | $(8157, 1183)^{*+}$ |
| $(1819, 2211)^{*+}$ | $(2527, 575)^{+}$ | $(2789, 3385)^{*+}$ | $(3773, 1133)^{+}$ | $(5755, 3799)^{*+}$ | $(8157, 1269)^{*}$ |
| $(1819, 2287)^{+}$ | $(2527, 1099)^{*+}$ | $(2789, 3411)^{*+}$ | $(3773, 1183)^{*+}$ | $(5755, 4071)$ | $(8157, 1417)^{*+}$ |
| $(1819, 2893)^{*+}$ | $(2527, 1133)^{+}$ | $(2789, 3689)^{*+}$ | $(3773, 1269)^{*+}$ | $(5755, 4855)^{*+}$ | $(8157, 1507)^{*+}$ |
| $(1819, 2923)^{+}$ | $(2527, 1183)^{*+}$ | $(2789, 3799)^{*+}$ | $(3773, 1417)^{*+}$ | $(5755, 5327)^{+}$ | $(8157, 1639)^{*+}$ |
| $(1819, 3359)^{+}$ | $(2527, 1269)^{*+}$ | $(2789, 3891)^{+}$ | $(3773, 1507)^{+}$ | $(5755, 5631)^{*+}$ | $(8157, 1715)^{*+}$ |
| $(1819, 3411)^{*+}$ | $(2527, 1417)^{*+}$ | $(2789, 4795)^{+}$ | $(3773, 1639)^{+}$ | $(5755, 7151)^{+}$ | $(8157, 1853)^{+}$ |
| $(1819, 3689)^{*+}$ | $(2527, 1507)^{*+}$ | $(2789, 4855)^{*+}$ | $(3773, 1715)^{*+}$ | $(5755, 7639)$ | $(8157, 1957)^{*+}$ |
| $(1819, 3739)^{+}$ | $(2527, 1639)^{*+}$ | $(2789, 5037)^{+}$ | $(3773, 1753)^{*+}$ | $(5755, 8119)^{*+}$ | $(8157, 1999)^{*+}$ |
| $(1819, 3799)^{+}$ | $(2527, 1715)^{*+}$ | $(2789, 5327)^{+}$ | $(3773, 1957)^{*+}$ | $(5997, 19)^{+}$ | $(8157, 2211)^{*+}$ |
| $(1819, 4855)^{*+}$ | $(2527, 1753)^{*+}$ | $(2789, 7151)^{*+}$ | $(3773, 1999)^{*+}$ | $(5997, 53)^{+}$ | $(8157, 2287)^{+}$ |
| $(1819, 5631)^{*+}$ | $(2527, 1853)^{+}$ | $(2789, 8119)^{*+}$ | $(3773, 2211)^{*+}$ | $(5997, 173)^{*+}$ | $(8157, 2485)^{*+}$ |
| $(1819, 7151)^{*+}$ | $(2527, 1957)^{*+}$ | $(2789, 8187)^{+}$ | $(3773, 2485)^{*+}$ | $(5997, 575)^{*+}$ | $(8157, 3359)^{+}$ |
| $(1819, 8187)^{+}$ | $(2527, 1999)^{*+}$ | $(3059, 19)^{*+}$ | $(3773, 2893)^{*+}$ | $(5997, 987)^{+}$ | $(8157, 3385)^{*+}$ |
| $(2249, 19)^{*+}$ | $(2527, 2211)^{*+}$ | $(3059, 173)^{*+}$ | $(3773, 3385)^{*+}$ | $(5997, 1133)^{+}$ | $(8157, 3411)^{*+}$ |
| $(2249, 173)^{*+}$ | $(2527, 2893)^{*+}$ | $(3059, 575)^{*+}$ | $(3773, 3411)^{*+}$ | $(5997, 1183)^{*+}$ | $(8157, 3531)^{+}$ |
| $(2249, 225)^{+}$ | $(2527, 3385)^{+}$ | $(3059, 1099)^{*+}$ | $(3773, 3799)^{*+}$ | $(5997, 1209)^{+}$ | $(8157, 3689)^{*+}$ |
| $(2249, 503)^{+}$ | $(2527, 3411)^{*+}$ | $(3059, 1209)^{+}$ | $(3773, 4071)$ | $(5997, 1269)^{*+}$ | $(8157, 3799)^{*+}$ |
| $(2249, 575)^{*+}$ | $(2527, 3689)^{*+}$ | $(3059, 1269)^{+}$ | $(3773, 4855)^{*+}$ | $(5997, 1417)^{*+}$ | $(8157, 3891)^{+}$ |
| $(2249, 869)^{+}$ | $(2527, 3891)^{+}$ | $(3059, 1417)^{*+}$ | $(3773, 5631)^{*+}$ | $(5997, 1507)^{*+}$ | $(8157, 4855)^{*+}$ |
| $(2249, 1099)^{*+}$ | $(2527, 4855)^{*+}$ | $(3059, 1507)^{*+}$ | $(3773, 7151)^{*+}$ | $(5997, 1639)^{*+}$ | $(8157, 5631)^{*+}$ |
| $(2249, 1133)^{+}$ | $(2527, 5631)^{*+}$ | $(3059, 1639)^{*+}$ | $(3773, 7613)^{+}$ | $(5997, 1715)^{*+}$ | $(8157, 6837)^{+}$ |
| $(2249, 1183)^{+}$ | $(2527, 5725)^{+}$ | $(3059, 1715)^{*+}$ | $(3773, 8119)^{*+}$ | $(5997, 1753)^{+}$ | $(8157, 8119)^{*+}$ |
| $(2249, 1417)^{*+}$ | $(2527, 7151)^{*+}$ | $(3059, 1753)^{*+}$ | $(3773, 8187)^{+}$ | $(5997, 1957)^{*+}$ | |
| $(2249, 1507)^{*+}$ | $(2527, 7613)^{+}$ | $(3059, 1957)^{+}$ | $(5755, 173)^{*+}$ | $(5997, 1999)^{*+}$ | |
| $(2249, 1639)^{*+}$ | $(2527, 7639)$ | $(3059, 2287)^{+}$ | $(5755, 225)^{+}$ | $(5997, 2211)^{*+}$ | |
| $(2249, 1715)^{*+}$ | $(2527, 12255)^{+}$ | $(3059, 2451)^{+}$ | $(5755, 575)^{*+}$ | $(5997, 2451)^{+}$ | |
| $(2249, 1753)^{*+}$ | $(2789, 19)^{*+}$ | $(3059, 2485)^{*+}$ | $(5755, 1183)^{*+}$ | $(5997, 2485)^{*+}$ | |

| | | | | |
|---|---|---|---|---|
| $(181, 1057)^{*}$ | $(935, 7399)^{*+}$ | $(1643, 11627)^{*+}$ | $(3493, 1057)^{*+}$ | $(5099, 7399)^{*+}$ |
| $(181, 7399)^{*+}$ | $(935, 11627)^{*+}$ | $(1843, 1057)^{*+}$ | $(3493, 7399)^{*+}$ | $(5099, 11627)^{*+}$ |
| $(181, 11627)^{*+}$ | $(1165, 1057)^{*}$ | $(1843, 7399)^{*+}$ | $(3493, 11627)^{*+}$ | $(6967, 1057)^{*}$ |
| $(595, 1057)^{*}$ | $(1165, 7399)^{*+}$ | $(1843, 11627)^{*+}$ | $(4097, 1057)^{*+}$ | $(6967, 7399)^{*+}$ |
| $(595, 7399)^{*+}$ | $(1165, 11627)^{*+}$ | $(1993, 1057)^{*+}$ | $(4097, 7399)^{*}$ | $(6967, 11627)^{*+}$ |
| $(595, 11627)^{*}$ | $(1401, 1057)^{*}$ | $(1993, 7399)^{*+}$ | $(4097, 11627)^{*+}$ | $(8181, 1057)^{*}$ |
| $(767, 1057)^{*}$ | $(1401, 7399)^{*+}$ | $(1993, 11627)^{*+}$ | $(4837, 1057)^{*+}$ | $(8181, 7399)^{*+}$ |
| $(767, 7399)^{*+}$ | $(1401, 11627)^{*}$ | $(2861, 1057)^{*}$ | $(4837, 7399)^{*+}$ | $(8181, 11627)^{*+}$ |
| $(767, 11627)^{*+}$ | $(1493, 1057)^{*+}$ | $(2861, 7399)^{*+}$ | $(4837, 11627)^{*+}$ | $(10939, 1057)^{*}$ |
| $(861, 1057)^{*+}$ | $(1493, 7399)^{*+}$ | $(2861, 11627)^{*+}$ | $(5053, 1057)^{*}$ | $(10939, 7399)^{*+}$ |
| $(861, 7399)^{*}$ | $(1493, 11627)^{*+}$ | $(2939, 1057)^{*}$ | $(5053, 7399)^{*+}$ | $(10939, 11627)^{*}$ |
| $(861, 11627)^{*+}$ | $(1643, 1057)^{*+}$ | $(2939, 7399)^{*+}$ | $(5053, 11627)^{*+}$ | |
| $(935, 1057)^{*+}$ | $(1643, 7399)^{*}$ | $(2939, 11627)^{*+}$ | $(5099, 1057)^{*}$ | |

Table 3: 15-variable functions with nonlinearity 16264 obtained from 8 and 9-degree PW functions

# Appendix B

Truth table of the 15-variable 1-resilient function with nonlinearity 16264, degree 12, maximum autocorrelation value 232 and algebraic immunity 7 as given in Example 4 is as follows:

49D1CCFBCED8C4BD485BAE6B5D0E130BEAEAEDB7E9016569171EE5C63C43B9D60AC22A8B5BD2E025E5FFDB6C2AA57201413D498087AE07293F62DFA77BDDAB69
FE02CE542EE83C702D6E13B811BBF1463057171C79FE868BBE3549660711D14CB9DFA6AA727E860AA0752AD37CCF7E5F887232ED8417BA58C7E3DCB1B8BCD299
C2E4EB2E44CA090752EC400E75936CF9D625BA0AD413EBFE41B34873DD1BCD44A7F64EA5BA7D5A2789B11A774F141062D60B9710B139781D9AF5D99E47E4DB19
6A9D72DEFDDA06230DCCA45A1CB8FA9B2788CDD610ED0E6E29129B72B0EA2ADCB195AB7551799726D0F06E869A5850CE36756E9A82E6FE56E944BEC62B802B74
C36FA87BA2674837FB09B73DDF6C74DD3D65E3EDA4E65F95524F3E4B8AF3B2EDE54385FDB1EB5E98D8B87EFDD1C2C4EDC40F6109C79C6026471994B6D6BD5EDB
C87FD6CA40952939B7B2E2DB5BBD1B8E9414126E92582400E9963B152B8B554889F413607D75CFDFFD9CE2D53CF86B95C4E2E5B235F0E8F4266EBE1D156A399F
3307F97EA963B49B0FE40067450B10EBB44D97C2E0581500D04AD9C7EDE492BB4925FA9042802EB355251BF3B9DD1366BE6F9D925216924EF67E343EFC663206
70A3030536EC545D6C16308F70ACC8D7261A948EE1CD594F2C8188263C19F3DE2D18C1FA4D051C7DF91C63D512F31E33136994C02EE307A43B09D02EF3BCED6E
496434E025159CD0C78F8444A495FA702F3FD43C5992BF7058287C7D4CADB45E862630E173E1B3B3922B3F13DC6879B60F1EE672AF85A7267E87A90CBC098A84
113362C0110A307D88758E2FAE116379FB3D505B4EBA461CCCE37C5DAE54C8759AFBC676920BE19CFB89BB2443E54CA3E45F13CAD45501E2061F7AE5BD766A4F
3A21153F04E11F6F2D231C9CA95C741DA1BE00F8258CB711AFFAF8D1128473BD332B08F158AD69830BA7F402190CA7490C93BCEB352013F5844D03EEDF9D2450
BEB81490DFA69C5F9688D25A624812D2BAD31CF4F919DC742358789A19B5D8F211BB3F52BD866B8907008AFEFB8439F47FDD49087EA672E3F1D0D9E630B85F22
E9A0CA2E201D6A74C8FC949A8851F8EC15F1E3AF9340859ABB5AD8989B06EA30DA2D2AC7A0CA6E2850327D72E8C7770AD5EA7884E12A49BE0F5A83E62EABC8E5
1DC0429F00CB57798DCD3D33D091D43EFA3BFF17EF63F4F118836A45D7DCED2267EA93AA7069BAB2A4A2AE7089581974E6B387116B3184ED53D361D7FE4D252B
07E4449538648DC846CEA6EAD75C141FE690BEAE854445DD122F497CE98010ABDEED960DCE08B72210DAF7E0C1A5E3BEB656A36BD8E02AFF2C4AD01B4BF5A77E
1C015EC56C5601A54A101952ACD6BADEEEC9677D1CACB98DDC91BA9E67BE58692C5B0ACA693B95F2746460199D78AE8D04355A8C6ADE748D1DF941A05769A537
758D661E151A0F75F28BBD0F98FFB60170F641AA589B8CD43178883BD62804D49A46AD031B5A3E5AD4052909B93E3BD4E5294172754F5D4F6FA850E28C7F9197
D34D21E91DF685C9151538B9CC43DCF1052A8E9F43172747EA0E2A414C589CAAD2EAEF9823D79841802414AC61C8882C02C328BF990767467F62DA785E7FBE96
DDB07B23A80EF82D3EE263A98E97741F81E554D21070B48A20432B4A55639DD454FDF4D4F2C2349E584B3AC52EA9AA2C8FF654C91036CDA3B23398F065D18832
9FC8299FE8427AD805AFE93BF82007129B2E2A61E0598765C618F3C35DB035B9BC0016B9A08CFF4FE2BBC10EA3004C84977F86074ECE3ADADE109029E4D51A85
E698D48BC54F9FF23976989BDB26F47AC4AF0DC1D015FC2CF69A90ABD3B7BB928748D7910599C2AABD1B899318463B24F565A1A7CF7BDCE82C900BD2C544AD41
1BE9082B35BD5897059C1AF9150F2D6B4740770070346F38919FEE353212F7AB3E2B5FDFD0FB25B2FFD4FA0B7A565CFB5C00108D745A8D5162D1DAEDF1A37FA8
428862454CB17D652957560F7D9213F326B5D9929F71D93BDDFB7D21DA580045E417D249D6215B1C2F1F391DBCDF124E79CD6F3CB9925F7E74092E45F0233E93
9D04AF08A0CB9816564758C16EBFF7BC5BABC26C7816C8775ECEC598E7166C2111C8C6FD3240B765F16CA1AD2923F4798BEB5CB37DA3852BB3FCE30C80C9C471
13F5ACA22EB9AF335A1285E500634B99DC1B8A188B64AB19E30019B452F41A8C3E8DAD8B2A83BB15E9F3DC540F25CA79919BDE418B5058F6772599B4352F0511
D8F81662B4E4794F7D373354E256FDAB4729E724C1AD997D3A7377B5C023008ACDA3EAA90263EE7DF64982BF48804768224C703AA1CA2A15B6DD070F25103ED4
19C3101B9E0FA71EEB74FD07E91C701C58CE6B7985DA1D9F35C33F25F9BDC4D3E66C377C5D157D17E2B8E89F8347F32CC78E3EA864923B936FD7F42CDA2021F0
3495CBBF17F22790BE9B4F90C885F1F6A4FC85133C2E6BE1DA787165F93BF22FE9372F4E415ECD9ED151C2146BF93206796AD6C789529838698F6AB5CB3E22A0
7DB32F13F9F3457482CB0E61CD4EB3E8EEF7916265C254B611A2E93D808E1D0BD04153A83A96A9455E5517C3390712EE96E7EE7915A4B033CE282711324350F0
4E3EBE0A10ED7262D7A15A4CDBCB39941E05E60CF286C93ADDF3FDA7C0490AA52F4B99283B2744CB5A52D26702CFA267F0C3319B33CD621D81A7E15EBEF57300
5830A26FA319C1304BC235C691F017588214C89CC874875BADD4A34CD8CE68E3A2E5006F54BBE0740AD5651360B9C6166EBD9C903CE0485C907D167660E065F5
3A334D7CCE4347E526EC52D0643C539EB829ADB819F78776B7EBA81CB1131F2873E7B08690803DD84655F0A73D999083E1F5BBBD50D2B3997295D9231D2BFEF0
5D414AAEB601FD67E9EAC51520B13F769C48E36DE5AA1CFBF33FCFC37E2E836A62C9E238442269188E4E00962813A7F29131C8056BB9332A81957B61B77BA1B8
0F52320DA73814C2784B071B865530BDC30821B9BF7E3B559C85EAC647F111AD305BDC2D65E4C9286DA48801A41BDFC3025AD58853B389A1546086B1469D664E
45AA2022C6249D5A5EC98DD8E83F93C19C4FE75ACB53394E750CB371C91DA8D7BC64A82B68F1896229BC8F86CCDCA9953B58F772C321E89B6D61FA0902600D86
CF49DDE9748511F2995B73F0CCE8B3C3183D90BA68E4915A7A43C8A4B5CEA12ECE50651C3FEA8E9C71C60B403F6F43FB55B82BE2B4786D26C708AA22C1BF779C
33B3D8EC8F75228AF2177EE908EDFCCD97AAE1C21B10179DD5CE8E23C4D294199A96E24317ADEB5279D8424EA3213512AD9BB141233EAC69CEE229B9BA042323
B1690CF65E10D6742F1608943C3A146D674BAE9A09288B32C80C82FE9E576B8AB4C5EBED8590BB89BAE45A7D3ED467429315BCEC87670822EA4055078A8514DD
A2B5235F7865635D16C33DC170DD9F090B9FB865ABBD7143FFF1004704D7380895F40E30AFF1F63A50BAC045117C249B4667571C9B6F43A713BDEEB1209F1600
CBE86E39926A972CEC6BB6058EE0C6C688D3C4BD488049783250E32F4263E26DD4B1A0EFBA04A57EDE9175F746F764046C29BB8D9C6793E60F01C9D999DCF77A
832520BBCA91B7A961022A193C30E01940CB391577B5BB4A3779B4E8BC1DF8D2FE5EEF66F279E770352EFF5959EF4013D914AF3656F0F79CC9D08822E7DF42EE
9DBF2EFCCE11315F5A2F64613C0ACCECD000971DC2D7580603C0277FC3A8EA08BBE0E829AF9C22F35F79137BABFE82172C2F2C1D512AC3D8DBCFA3FEEA4CB241
4E1349A2B22D5E16417A1D2D990BD6D9486A06DFE993DE38BF59EEC027410BFDE4C1C70CFB85A61B1A3C0DD231C4438FA150562455D524BA99E834790A416DAE
C874312EE6C43B8C4B2ECCE1C9B719229113CEFF985D8EB1C7334FF59A4BC440E6C6B068792B7D0DA0E5B1A5DCC1EBC21B33769D95000B3B19567874A80174F4
23FCEAA021EE20321E6DCA14B050F60D5AC1AB83BAC848ADDCCB3AC10527D5446F4A047A7968E0B502AB015B683CB6B0AE54183FC86C606AC85B454880D2F03E
77B83A95FE769474D524770B3FAEC27369EEEF827AF4EE69ABE13C6169FEA05E51BF86571E7E0E6C6C5E6A7715ECBFCCD0DA3E632EAC2254D8ECD29D700C3658
1D9621A22D8FBF7F57C03C8F73EAB53EF403D66AF8E1F9219FFCA1DFE32C306524874AF07D8AAEB944A6A7D073A994CED2DBBB49E0A6115F2D55145352A4DAC7
16D448F2C06DE7E9B7CD71099426A665BD50648EABFEA1B6B120751F0A1D93D457A02716EC1046BEBAA8B31F174DC5799D6C1556ED81CAF8AFC22F5F68E9F3C5
3847D55081715C362336FC528DC6AB57E1E265A718DDD8E11D13B9A1405CCDE491CF4D6376DF21D88C8F9AABD38C53964AF56E2A8E3DBEEFE6AB13C1BC204816
E4FEE4D4866A24407A14FDBDC35B23130A8423AC397E385D77CB9FF7CE6FD40881B8AF8C9BDDEE965918D036EB470E57D920741D5363F0EFB61A1005E248220F
5B4108C0AFCB292F9E7A1DB633CC4D3392CDDB9BD714F9EA780116E2F5BF730E5EFAEA77B116525075CA5CCF1FF9A96DF7DD3D73BFDB731A6234A7818F6A95A6
1F837C077919617C7C58B360228189156CC09E38317AB0C9D634065B8E22707C83FCBB3DD9FC9D12D4F3441E03F0F7D53F79D115BA8306AF91E185911FE7C865
AFCAE540F04A3562483C412B138DA667F71E295FCA54866739DBB87F8FD7453E24BE3ACE0D05D731AEDED86C14CA5BD8CB0A0583EC56E94AA88FA23130F58804
E70846197ED757A38A3074CC8DEBC082DC7D9F46B2A437DF9FD672335369A2EA1BF21A4B964BE4F578D02DBDDC07953EDFEE1CD212B485B9B2AF88456CFD908F
1960BADAA9E73966C19615A4909752B5EB0288603E6F450AB0D138D2A19535ACC10A51015A9E76E15F6CCE6C7E065F5F942706A618607D10DDC8EA23FDC7C60F
1A777105D338CE47F7F0BFB6D13BCD0FEAA3F1AA19044CBC7C0299880991CF4012F446411AE0B03303245D329DBDA957AF6CDD13C7FB52C002DB2613872AA2AE
6F1B8F7B2559B8A7E872161BF8F8941DF825D52BE2E9EF6FEF68BA89D386E628DA64D91431D9779D936D7D42207ECE5415E56224601B1AD505120BA94FC0645E
843E4BCD0C58D948C4A9C9B56A41CEBF2BA07677A4AE993823427CFF72D83086D225A987441DE4132D8706FC02A03FA94E3D4B5EF86C0E9BD9B9F436AF1A32CF
F328A0E13916219D5F00D1A42E5378108F059CFDE34F3AFEFCFCB888F7B339C09D3B6CA9378067B51FDBAF48C60CC3AF6619AE9EBCA39FEBA0D75BFB1C67D7E7
06E154264D0F7FC168E875DEF67B0FE6520929628A2FA39F5E75868CB3C7C04025F351FF834717C6AC84AE427E5E4E7C12246CD72DE8AE3CB31C267E952455F4
F92C630E720569BD9B208FD6EBA7EDD3031E0C53F0E5375E565DC40373E11DD9ABD043B2AAD9942CB1C0557A2132070683E908AA85C51AC7F98045D1FBCD8148
35E5D9ADDD460F26E7FE74A812E5AE03868F01E67F87ECD807F844A24742160F316C21830D5BD247781E82F65D563BFA2A79400014157952A9CF5AEDD344E9B9
386558FDABEF24EC7E78A97A9AC5C3C6BD4E5D4BED7779A57E0667537EB8F0833F9EFA3E5ADFFA056CB65C2C759CCE88B3A389AB9B79D2A887803F2ABC200F04
B22E5E5383A500BD196BE9C029EF1EB604D0DC6A0C7D2BCA1AB879C52D2C287452C263C4C401CB034F2A1DC398B921B56E27272189B8EA3F7B041CD90863C697