Advances in Mathematics of Communications
Volume 14, No. 1, 2020, 127–136

doi:10.3934/amc.2020010

HIGHLY NONLINEAR (VECTORIAL) BOOLEAN FUNCTIONS THAT ARE SYMMETRIC UNDER SOME PERMUTATIONS

Selçuk Kavut*

Department of Computer Engineering, Faculty of Engineering
Balıkesir University, 10145 Balıkesir, Turkey

Seher Tutdere

Department of Mathematics, Faculty of Arts and Science
Balıkesir University, 10145 Balıkesir, Turkey

(Communicated by Subhamoy Maitra)

Abstract. We first give a brief survey of the results on highly nonlinear single-output Boolean functions and bijective S-boxes that are symmetric under some permutations. After that, we perform a heuristic search for the symmetric (and involution) S-boxes which are bijective in dimension 8 and identify corresponding permutations yielding rich classes in terms of cryptographically desirable properties.

1. Introduction

A vectorial Boolean function, also called a multi-output Boolean function or a substitution box (S-box), with the number of input variables n and output variables m is defined as a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. When $m = 1$, the corresponding function is called a single-output Boolean function, or simply a Boolean function. Hence, an S-box is composed of m Boolean functions, called coordinate functions, each with n variables. (Vectorial) Boolean functions are crucial cryptographic primitives used as building blocks in symmetric cryptosystems. For an S-box, high nonlinearity and low differential uniformity are required to prevent linear [16] and differential [2] cryptanalyses (in block ciphers), whereas for a Boolean function high nonlinearity is a prerequisite for thwarting best affine approximation attacks [4] (in stream ciphers). We mainly consider two challenging problems in symmetric cryptography:

- Construction of Boolean functions with an odd number n of variables, $n \geq 9$, achieving maximum possible nonlinearity,
- Construction of bijective S-boxes in even dimensions n=6 and 8, having high nonlinearity and low differential uniformity.

In fact, most of the best known results regarding to these problems are either symmetric under some permutations or affine equivalent to them. In this paper, we first present a survey of the mentioned results in the related literature. Secondly, we classify all 8! permutations up to the linear equivalence of S-boxes (in dimension 8) that are symmetric under those permutations, which results in 22 different classes,

2010 *Mathematics Subject Classification:* 11T71, 94A60.

Key words and phrases: Boolean functions, covering radius, differential uniformity, heuristic search, nonlinearity.

This work is supported financially by Balıkesir University under grant BAP 2015/23.

* Corresponding author: Selçuk Kavut.

and then identify rich classes in terms of desirable cryptographic properties by performing the steepest-descent-like iterative search algorithm [1] in each class. We also apply our search for the symmetric S-boxes that are involutions, which provides better results in some cases.

2. Background

2.1. Boolean functions. The truth table of an n-variable Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is given by the binary output vector of length 2^n, i.e., $f = [f(0, 0, \ldots, 0), f(1, 0, \ldots, 0), \ldots, f(1, 1, \ldots, 1)]$. The Hamming weight $wt(f)$ of f is defined as the number of ones in its truth table and the Hamming distance $d(f, g)$ between two n-variable Boolean functions f and g is the number of positions in which their truth tables differ, i.e., $d(f, g) = wt(f \oplus g)$. The function f is said to be balanced if the respective truth table has the same number of ones and zeros, i.e., $wt(f) = 2^{n-1}$, which is a required property to avoid the statistical imbalance in the output of f.

A Boolean function $f(x)$ can be represented by a multivariate polynomial over $\mathbb{F}_2$, called the algebraic normal form (ANF),

$$\bigoplus_{u \in \mathbb{F}_2^n} a_u \left(\prod_{i=0}^{n-1} x_i^{u_i} \right),$$

where $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$ and $a_u \in \mathbb{F}_2$. The highest Hamming weight of u with $a_u \neq 0$ is called the algebraic degree, or simply the degree, of f and denoted by $deg(f)$. To have good confusion properties, it is cryptographically desired to achieve a high algebraic degree. A Boolean function with degree at most one is called an affine function. Linear functions are those affine functions with constant term equal to zero.

The Walsh-Hadamard transform $W_f : \mathbb{F}_2^n \to [-2^n, 2^n]$ of an n-variable Boolean function f is an integer valued function defined as

$$W_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} (-1)^{w \cdot x},$$

where $w \cdot x = w_0 x_0 \oplus w_1 x_1 \oplus \ldots \oplus w_{n-1} x_{n-1}$ is the inner product of $w = (w_0, \ldots, w_{n-1})$ and $x = (x_0, \ldots, x_{n-1})$. The nonlinearity of an n-variable function f can be expressed in terms of its Walsh-Hadamard spectrum, defined as the minimum Hamming distance from the set of all n-variable affine functions, i.e.,

$$NL_f = 2^{n-1} - \frac{1}{2} \max_{w \in \mathbb{F}_2^n} |W_f(w)|.$$

2.2. S-boxes. An S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ can be expressed as $S(x) = (f_0(x), f_1(x), \ldots, f_{m-1}(x))$ $\forall x \in \mathbb{F}_2^n$, where the functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ for $i = 0, 1, \ldots, m-1$ are the coordinate functions. A linear combination $c \cdot S(x)$ of the coordinate functions is called a component function, where $c \neq (0, 0, \ldots, 0) \in \mathbb{F}_2^m$. We are now ready to extend the definitions of nonlinearity and algebraic degree to S-boxes using the component functions. The nonlinearity of S is the worst (i.e., lowest) nonlinearity among the $2^m - 1$ component functions, whereas the algebraic degree of S is the highest one over all component functions.

The function S is called differentially δ-uniform if there are at most δ solutions to the equation $S(x) \oplus S(x \oplus \gamma) = \beta$, where $\gamma \neq (0, 0, \ldots, 0) \in \mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^m$. Accordingly, δ is called the differential uniformity of S. It is cryptographically desirable to have a small differential uniformity as it implies that the probability of occurence of a particular pair (γ, β) is low; otherwise, a high occurence probability can be utilized to realize a differential cryptanalysis. When $n = m$, the lowest achievable value of δ is 2, and such functions are called almost perfect nonlinear (APN). For even n, no APN functions had been known until, in 2009, a counterexample for $n = 6$ was identified [3].

2.3. Symmetric (vectorial) functions. Let us consider the action of a permutation group G on $\mathbb{F}_2^n$. The set $G(x) = \{\pi(x) \mid \pi \in G\}$, where the group action moves $x \in \mathbb{F}_2^n$, is called the orbit of x. The orbits partition the vector space $\mathbb{F}_2^n$ by defining the equivalence relation: $x \sim y$ if and only if there exists a permutation $\pi \in G$ such that $\pi(x) = y$ for all $x, y \in \mathbb{F}_2^n$. The number of orbits, denoted by g_n, can be determined by using Burnside's lemma.

Lemma 2.1 (Burnside's Lemma)**.** *If G is a finite group of permutations acting on a set X, then the number of orbits of G on X is given by $\frac{1}{|G|}\sum_{\pi\in G}|X^\pi|$, where $X^\pi = \{x \in X | \pi(x) = x\}$.*

The lexicographically least element belonging to the i^{th} orbit, where $0 \le i \le g_n - 1$, is said to be the orbit representative and represented by Λ_i. A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called symmetric under a permutation π if it is invariant under that permutation, i.e., $f(\pi(x)) = f(x)$ for all $x \in \mathbb{F}_2^n$. Clearly, the number of Boolean functions which are symmetric under a permutation π is 2^{g_n} and a Boolean function f among these can be represented by its outputs $(f(\Lambda_0), f(\Lambda_1), \ldots, f(\Lambda_{g_n-1}))$ corresponding to the orbit representatives, which is shorter than the ANF or truth table representations. It can be shown [22, Lemma 1] that $W_f(u) = W_f(v)$ for any u, v belonging to the same orbit, implying that the number of distinct values in the Walsh-Hadamard spectrum of f can be at most g_n. Using this fact, the Walsh-Hadamard transform of f can be computed [22] efficiently as follows:

$$W_f(\Lambda_j) = \sum_{i=1}^{g_n}(-1)^{f(\Lambda_i)}\mathcal{M}_{i,j},$$

where $\mathcal{M}_{i,j} = \sum_{x\in G(\Lambda_i)}(-1)^{x\cdot\Lambda_j}$ defines a matrix $\mathcal{M}$ of size $g_n \times g_n$.

One can extend [9] the definition of symmetric Boolean functions to the case when the functions are vectorial. A vectorial function $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called symmetric under a permutation π if $S(\pi(x)) = \pi(S(x))$ for all $x \in \mathbb{F}_2^n$, that is, its output is permuted by the permutation π when the same permutation is applied to the corresponding input. The number of bijective S-boxes that are symmetric under an arbitrary permutation can be found using the following proposition [9].

Proposition 1. *Let S be a bijective S-box in dimension n, which is symmetric under a permutation π. The number of such S-boxes is given by*

$$\prod_{i=1}^{d} t_i! s_i^{t_i},$$

where t_i is the number of orbits having the same orbit size s_i and d is the number of distinct orbit sizes.

It can be shown [9] that the component functions $u \cdot S(x)$ and $v \cdot S(x)$ are linear equivalent when u and v belong to the same orbit, and hence there can be at most $g_n - 1$ component functions which are not affine equivalent. This provides an efficient way to compute the nonlinearity of S, as we need to compute the nonlinearities of

Table 1. A summary of the highest nonlinearities for odd $n \geq 9$.

Number of variables (n)	9	11	13	15
Bounds				
Bent concatenation bound $(2^{n-1} - 2^{\frac{n-1}{2}})$	240	992	4032	16256
Upper bound $(2 \lfloor 2^{n-2} - 2^{\frac{n}{2}-2} \rfloor)$	244	1000	4050	16292
Unbalanced nonlinearities				
[18]	–	–	–	16276
[13]	242	996	4040	–
Balanced nonlinearities				
[15]	–	–	4036	–
[20]	–	–	–	16272

only the $g_n - 1$ component functions to determine it. On the other hand, it should be noted that S can be represented by the coordinate function(s) for which the coefficient vector(s) is/are the orbit representative(s) with weight one.

3. Highly nonlinear Boolean functions

For an even number n of variables, the upper bound $2^{n-1} - 2^{\frac{n}{2}-1}$ on nonlinearity, which can be obtained by using the Parseval's theorem, is attained by the so-called bent functions. One can see that the concatenation of two $(n-1)$-variable bent functions with proper weights constructs a balanced n-variable Boolean function having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$, which is called the bent concatenation bound. This bound had been conjectured to be the achievable upper bound on nonlinearity for odd number of variables, until disproved in 1983 [18]. The problem of determining the maximum possible nonlinearity for an odd number n of variables is also related to the covering radius of the first order Reed-Muller codes of length 2^n. Recall that the covering radius of a code is defined as the smallest integer R such that the whole space is covered by the spheres of radius R centered at codewords. In our situation, there are 2^n codewords, each being an affine function, and the space size, i.e., the number of Boolean functions, is 2^{2^n}. It was shown [8] that R can be at most $2 \lfloor 2^{n-2} - 2^{\frac{n}{2}-2} \rfloor$ for the first order Reed-Muller codes of length 2^n, which can be considered as an upper bound on nonlinearity of n-variable Boolean functions.

For odd number of variables, we summarize in Table 1 the best known nonlinearities of (balanced and unbalanced) Boolean functions together with the upper and bent concatenation bounds. For odd $n \leq 7$, it was known that the achievable nonlinearity can be at most equal to the bent concatenation bound $2^{n-1} - 2^{\frac{n-1}{2}}$. In 1983, for the first time the existence of Boolean functions with an odd number of variables having nonlinearity greater than the bent concatenation bound was shown in [18] by identifying two functions with 15 variables attaining nonlinearity $2^{15-1} - 2^{\frac{15-1}{2}} + 20 = 16276$ within the idempotent class (a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called idempotent if $f(\alpha^2) = f(\alpha)$ for all $\alpha \in \mathbb{F}_{2^n}$). It can be shown that using direct sum of an m-variable bent function and one of these two functions, it is possible to construct Boolean functions with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \cdot 2^{\frac{n-15}{2}}$, $n = m + 15$, for odd $n \geq 15$.

As it is pointed out in [6, 7], by a proper choice of basis, the idempotents can be considered as Boolean functions which are invariant under the cyclic rotation of input variables, and such Boolean functions are called rotation-symmetric. Boolean functions with number of variables $n < 15$ having nonlinearity exceeding the bent concatenation bound were unknown until 2006, when 9-variable Boolean functions with nonlinearity $2^{9-1} - 2^{\frac{9-1}{2}} + 1 = 241$ were identified [12] by using a heuristic search (the steepest-descent-like iterative search algorithm) in the class of rotation-symmetric Boolean functions (RSBFs) for which the space size is 2^{60}. Later it was found [11] that in this class there are 1512 RSBFs with nonlinearity 241, among which there are only 2 which are different up to affine equivalence, and there is no RSBF with nonlinearity exceeding 241. Shortly after that, the nonlinearity result was improved [13] to 242 by generalizing the class of RSBFs as k-rotation-symmetric Boolean functions (k-RSBFs). An n-variable Boolean function is called k-rotation symmetric if

$$f(x_0, x_1, \ldots, x_{n-1}) = f(x_{(0+k) \mod n}, x_{(1+k) \mod n}, \ldots, x_{(n-1+k) \mod n})$$

for all $(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$, where k is a fixed divisor of n. It can be shown that the class of k-RSBFs can be regarded as a generalized class of idempotents for which the functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ satisfy the condition $f(\alpha^{2^k}) = f(\alpha)$ for all $\alpha \in \mathbb{F}_{2^n}$. Note that when $k = 1$, the class of k-RSBFs is the same as the class of RSBFs.

In fact, since nonlinearity is invariant under liner transformations, all 9! permutations are classified in [13] up to the linear equivalence of Boolean functions that are symmetric under them, by using the following proposition.

Proposition 2. *Let f and g be symmetric Boolean functions under permutations π_f and π_g, respectively. If $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a bijective linear mapping such that $f = g \circ A$, then $\pi_f = A^{-1} \circ \pi_g \circ A$.*

Then it is found [13] that there are 30 classes which are different up to the equivalence relation defined by $\pi_f \sim \pi_g$ if and only if there exists A such that $\pi_f = A^{-1} \circ \pi_g \circ A$. Boolean functions with nonlinearity 242 could be attained in [13] within 4 of these classes (one of which is 3-RSBFs) by performing the steepest-descent-like iterative search algorithm. Using one of these functions, one can get Boolean functions with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 2 \cdot 2^{\frac{n-9}{2}}$ for odd $n \geq 9$ via the direct sum method, and hence the nonlinearity results 996 and 4040 are obtained [13] for $n = 11$ and 13, respectively, as shown in Table 1. However, these functions are unbalanced since the functions with nonlinearity 242 are unbalanced.

Balancedness is an important cryptographic property to avoid statistical imbalance in the output of a Boolean function. Balanced functions with nonlinearity greater than the bent concatenation bound have received a lot of attention in the literature. To construct such functions the aforementioned unbalanced functions in Table 1 can be exploited. In [13], using one of the functions with nonlinearity 242, a 13-variable Boolean function f with nonlinearity 4040 and Hamming weight 4088 was first constructed. Then a balanced 13-variable function with nonlinearity 4034 could be generated [14] by performing a random search which flips 8 zeros to ones in the truth table of f. This result was later improved in [15] to 4036 by using a heuristic search. The balanced function with nonlinearity 16272 was obtained in [20] by interpreting the unbalanced construction with nonlinearity 16276 as an RSBF. By performing an exhaustive search in a suitably chosen neighbourhood of this RSBF, it was found [20] that toggling the outputs at some orbits generates an RSBF with nonlinearity 16272 having zeros in its Walsh-Hadamard spectrum, which yields a balanced function via a linear transformation.

Let us consider the case when the number n of variables is even. Note that bent functions are not balanced since $W_f(w) = \pm 2^{\frac{n}{2}}$ for all $w \in \mathbb{F}_2^n$ and a Boolean function is balanced if and only if $W_f(w) = 0$ for $w = (0, 0, \ldots, 0)$. For even $n < 8$, the maximum achievable nonlinearities for balanced Boolean functions are known, which are 0, 4, and 26 for $n = 2$, 4, and 6, respectively. For even $n \geq 8$, it was conjectured [5] in 1994 that $\mathrm{nlb}(n) \not> 2^{n-1} - 2^{\frac{n}{2}} + \mathrm{nlb}(n/2)$, which is still open. Specifically, the conjecture implies that there are no balanced Boolean functions with 8 and 10 variables having nonlinearities 118 and 494, respectively.

4. Symmetric bijective S-boxes

An S-box is called rotation-symmetric if any cyclic rotation of its input variables rotates the corresponding output variables by the same amount. In [19], it was shown that the S-boxes obtained from power maps (or their sums) are linear equivalent to rotation-symmetric S-boxes (RSSBs) (for instance the inverse function, used as the S-box of AES, can be considered as an RSSB). The definition of RSSBs is then generalized in [9] by defining k-rotation-symmetric S-boxes (k-RSSBs). Let ρ^i be the i-cyclic shift operator defined as

$$\rho^i(x_0, x_1, \ldots, x_{n-1}) = (x_{(0+i) \mod n}, x_{(1+i) \mod n}, \ldots, x_{(n-1+i) \mod n}),$$

where $1 \leq i \leq n$. An S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is said to be k-rotation-symmetric if $\rho^k(S(x_0, x_1, \ldots, x_{n-1})) = S(\rho^k(x_0, x_1, \ldots, x_{n-1}))$ for all $(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$, where k is a fixed divisor of n. Note that when $k = 1$, the corresponding class of k-RSSBs is the same as the class of RSSBs.

Let us consider a mapping s from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ such that $(s(\alpha))^2 = s(\alpha^2)$ for all $\alpha \in \mathbb{F}_{2^n}$. It was pointed out in [19] that the S-boxes (i.e., the mappings $\mathbb{F}_2^n \to \mathbb{F}_2^n$) obtained from s using a normal basis can be considered as RSSBs. One can then show that the S-boxes for which $(s(\alpha))^{2^k} = s(\alpha^{2^k})$ in the above argument correspond to k-RSSBs.

In [9], all possible permutations up to the linear equivalence of S-boxes that are symmetric under those permutations are classified using the following proposition which is an extended form of Proposition 2 for the S-boxes.

Proposition 3. *Let $S, T : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be symmetric S-boxes under permutations π_s and π_t, respectively. If $A, B : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are bijective linear mappings such that $S = A \circ T \circ B$, then $\pi_s = A \circ \pi_t \circ B$ and $A = B^{-1}$.*

The classification were accomplished in [9] for $n = 6$ by defining the equivalence relation: $\pi_s \sim \pi_t$ if and only if there exists A such that $\pi_s = A \circ \pi_t \circ A^{-1}$. The number of equivalence classes was found to be 11 (including the identity permutation which gives the whole space of S-boxes). After that, the steepest descent-like-iterative search algorithm was performed in each class identifying the rich ones in terms of high nonlinearity and low differential uniformity. More specifically, in 4 classes (out of 11) differentially 4-uniform S-boxes with (the best known) nonlinearity 24 could be generated; 3 of these classes correspond to k-RSSBs and the other one can be considered as the class of S-boxes that are obtained by the concatenation of two RSSBs in dimension 5. In [10], an exhaustive search was performed for the latter class of functions for which the space size is $2^{61.28}$. It was found [10] that there

Table 2. Best achieved cryptographic properties [nonlinearity, differential uniformity, algebraic degree].

#	Representative permutation	Space size	Best result	Best result (for involution S-boxes)
1	$(7,6,2,1,8,5,4,3)$	$2^{147.93}$	$[84,44,7]$	$[84,44,7]$
2	$(2,3,1,7,4,5,6,8)$	$2^{191.48}$	$[84,52,7]$	$[84,52,7]$
3	$(6,7,5,8,4,3,1,2)^a$	$2^{208.29}$	$[\mathbf{106},\mathbf{6},\mathbf{7}]$	$[\mathbf{106},\mathbf{6},\mathbf{7}]$, ***[108,8,6]***
4	$(4,3,2,5,8,1,7,6)$	$2^{227.35}$	$[0,-,-]$	$[0,-,-]$
5	$(4,5,3,2,8,1,6,7)$	$2^{243.74}$	$[\mathbf{106},\mathbf{6},\mathbf{7}]$	$[\mathbf{106},\mathbf{6},\mathbf{7}]$
6	$(8,3,4,6,7,1,5,2)$	$2^{277.78}$	$[104,6,7]$	$[104,6,7]$, ***[106,8,7]***
7	$(8,6,3,5,2,1,7,4)$	$2^{283.02}$	$[104,10,7]$	*[104, 8, 7]*
8	$(4,6,7,5,1,2,3,8)$	$2^{357.97}$	$[84,44,7]$	$[84,44,7]$
9	$(2,6,3,4,5,8,1,7)$	$2^{358.65}$	$[100,10,7]$	$[100,10,7]$, *[104, 20, 7]*
10	$(7,3,6,1,8,2,4,5)$	$2^{359.22}$	$[0,-,-]$	$[0,-,-]$
11	$(7,6,1,2,3,8,5,4)^b$	$2^{412.21}$	$[104,6,7]$	$[104,6,7]$, ***[106,8,7]***
12	$(2,7,4,3,5,6,1,8)$	$2^{431.91}$	$[0,-,-]$	$[0,-,-]$
13	$(6,4,8,2,1,7,5,3)$	$2^{440.19}$	$[84,22,7]$	$[84,22,7]$
14	$(1,3,6,7,2,5,4,8)$	$2^{446.24}$	$[84,22,7]$	$[84,22,7]$
15	$(1,5,6,4,3,2,7,8)$	$2^{476.86}$	$[84,52,7]$	$[84,52,7]$
16	$(4,3,8,5,1,6,7,2)$	$2^{565.87}$	$[104,6,7]$	$[104,6,7]$
17	$(1,6,3,4,2,5,7,8)$	$2^{693.43}$	$[84,44,7]$	$[84,44,7]$
18	$(7,6,5,8,3,2,1,4)^c$	$2^{824.73}$	$[104,6,7]$	$[104,6,7]$
19	$(1,5,8,4,2,7,6,3)$	$2^{835.24}$	$[104,8,7]$	$[104,8,7]$
20	$(1,2,7,4,5,8,3,6)$	$2^{890.27}$	$[84,22,7]$	$[84,22,7]$
21	$(8,2,3,4,5,6,7,1)$	$2^{1076.16}$	$[0,-,-]$	$[0,-,-]$
22	$(1,2,3,4,5,6,7,8)^d$	2^{1684}	$[102,6,7]$	*[104, 6, 7]*

[a] : Linear equivalet to RSSBs

[b] : Linear equivalent to 2-RSSBs

[c] : Linear equivalent to 4-RSSBs

[d] : The search space of all bijective S-boxes

exist $2^{37.56}$ S-boxes with nonlinearity 24, among which the number of those with differential uniformity 4 is $2^{33.99}$. Another exhaustive search was carried out in [9] for the class of RSSBs (in dimension 6) whose space size is $2^{47.9}$. In this case, the number of RSSBs with nonlinearity 24 is found to be 2^{28} and the number of differentially 4-uniform RSSBs with nonlinearity 24 is computed as $2^{24.7}$. It seems both classes are rich in terms of high nonlinearity and low differential uniformity and the class of RSSBs is more dense than the other class with respect to those cryptographic properties.

Here we classify all 8! permutations using Proposition 3 for the S-boxes in dimension 8, and found that there are 22 classes as shown in Table 2. For each class, we have performed the steepest-descent-like iterative search algorithm; the same algorithm is also applied for the corresponding subclasses each consisting of the involution S-boxes. The best obtained results are given in the last two columns of Table 2. As can be seen from Table 2, the nonlinearities of symmetric S-boxes belonging to 4 (out of 22) classes are found to be 0. This happens because we find that a certain component function is always linear for each of these classes. We recall that a similar situation occurs also in [9] for the symmeric S-boxes in dimension 6. More specifically, in our case, for the classes given by the 4th, 10th, 12th, and 21st permutations, we find that the coefficient vectors of the linear component functions are $(0, 1, 0, 1, 1, 1, 1, 1)$, $(0, 0, 0, 0, 1, 0, 0, 0)$, $(0, 0, 1, 0, 1, 1, 1, 1)$, and (1, 0, 0, 0, 0, 0, 0, 0), respectively.

From Table 2, we see that in most cases the cryptographic properties obtained from symmetric S-boxes are the same as those obtained from their subclasses of involution S-boxes. There are only 5 subclasses in Table 2 for which we get some better results indicated by italic font. The results with nonlinearities ≥ 106 are denoted by bold font (obtained for the classes corresponding to the 3rd, 5th, 6th, and 11th permutations). Note that the S-boxes which are symmetric under the 3rd and 11th permutations are linear equivalent to RSSBs and 2-RSSBs, respectively. We point out that although the inverse function is within the class of RSSBs, we couldn't get that function by our search, and its profile $[112, 4, 7]$ is superior than our results in Table 2. One can also find that the S-boxes which are symmetric under the 5th permutation are linear equivalent to the class of S-boxes which are obtained by concatenating two RSSBs in dimension 7. A more systematic search was performed in [10] for this class by exploiting some combinatorial properties related to the concatenation method.

The S-box with profile $[108, 8, 6]$, given below, achieves the highest nonlinearity in Table 2 and it is obtained within the subclass of involution S-boxes which are symmetric under the 3rd permutation.

(0, 66, 132, 23, 9, 212, 46, 209, 18, 4, 169, 148, 92, 105, 163, 101, 36, 204, 8, 190, 83, 91, 41, 3, 184, 27, 210, 25, 71, 112, 202, 103, 72, 128, 153, 99, 16, 194, 125, 188, 166, 22, 182, 120, 82, 161, 6, 201, 113, 235, 54, 68, 165, 65, 50, 243, 142, 229, 224, 248, 149, 123, 206, 115, 144, 53, 1, 90, 51, 214, 198, 28, 32, 176, 133, 104, 250, 80, 121, 222, 77, 181, 44, 20, 109, 170, 240, 251, 164, 195, 67, 21, 12, 239, 147, 137, 226, 146, 215, 35, 108, 15, 136, 31, 75, 13, 130, 162, 100, 84, 231, 167, 29, 48, 203, 63, 193, 191, 241, 119, 43, 78, 246, 61, 157, 38, 230, 234, 33, 139, 106, 232, 2, 74, 180, 178, 102, 95, 173, 129, 141, 140, 56, 179, 64, 177, 97, 94, 11, 60, 208, 228, 245, 34, 160, 249, 242, 124, 189, 185, 154, 45, 107, 14, 88, 52, 40, 111, 218, 10, 85, 253, 225, 138, 247, 196, 73, 145, 135, 143, 134, 81, 42, 211, 24, 159, 223, 187, 39, 158, 19, 117, 197, 116, 37, 89, 175, 192, 70, 217, 216, 47, 30, 114, 17, 252, 62, 220, 150, 7, 26, 183, 5, 254, 69, 98, 200, 199, 168, 233, 207, 221, 79, 186, 58, 172, 96, 236, 151, 57, 126, 110, 131, 219, 127, 49, 227, 244, 238, 93, 86, 118, 156, 55, 237, 152, 122, 174, 59, 155, 76, 87, 205, 171, 213, 255).

It took a month to obtain our results in Table 2 by using all 6 cores of a workstation with Intel Xeon CPU E5-1650v3 (15M Cache, 3.50 GHz) and 16 GB RAM under Windows 7 Professional 64-bit operating system.

5. Conclusion

It seems designing *rich* subspaces of cryptographic primitives and use of efficient (exhaustive or heuristic) search techniques are important tools to attack some of the most challenging problems in symmetric cryptography. We think that such tools, when combined with theory, provide many important results, some of which are mentioned here. On the other hand, symmetric (vectorial) Boolean functions are interesting to look into, as they can be used for efficient implementation of a cryptosystem and there are a plenty of functions with outstanding cryptographic properties, which can be considered as symmetric under some permutations.

References

[1] M. Bartholomew-Biggs, Chapter 5: The steepest descent method, in *Nonlinear Optimization with Financial Applications.* Springer US, (2005), 51–64.

[2] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *Journal of Cryptology*, **4** (1991), 3–72.

[3] K. A. Browning, J. F. Dillon, M. T. McQuistan and A. J. Wolfe, An APN permutation in dimension six, *The 9th Conference on Finite Fields and Applications - Fq9*, *Contemporary Mathematics*, **518** (2010), 33–42.

[4] C. Ding, G. Xiao and W. Shan, *The Stability Theory of Stream Ciphers*, Lecture Notes in Computer Science, 561. Springer-Verlag, Berlin Heidelberg, 1991.

[5] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, *Fast Software Encryption – FSE 1994*, *Lecture Notes in Computer Science*, **1008** (1994), 61–74.

[6] E. Filiol and C. Fontaine, Highly nonlinear balanced Boolean functions with a good correlation-immunity, *Advances in Cryptology Eurocrypt'98*, *Lecture Notes in Computer Science*, **1403** (1998), 475–488.

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

[8] X.-D. Hou, On the norm and covering radius of first-order Reed-Muller codes, *IEEE Transactions on Information Theory*, **43** (1997), 1025–1027.

[9] S. Kavut, Results on rotation-symmetric S-boxes, *Information Sciences*, **201** (2012), 93–113.

[10] S. Kavut and Sevdenur Baloğlu, Results on symmetric S-boxes constructed by concatenation of RSSBs, *Cryptography and Communications*, **11** (2019), 641–660, `http://dx.doi.org/10.1007/s12095-018-0318-1`.

[11] S. Kavut, S. Maitra, S. Sarkar and M. D. Yücel, Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity > 240, *Progress in Cryptology-Indocrypt 2006*, *Lecture Notes in Computer Science*, **4329** (2006), 266–279.

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

[13] S. Kavut and M. D. Yücel, 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class, *Information and Computation*, **208** (2010), 341–350.

[14] S. Maitra, Balanced Boolean function on 13-variables having nonlinearity strictly greater than the bent concatenation bound, *Boolean Functions in Cryptology and Information Security*, 173–182, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 18, IOS, Amsterdam, 2008. Available from: `https://eprint.iacr.org/2007/309.pdf`.

[15] S. Maitra, S. Kavut and M. D. Yücel, Balanced Boolean function on 13-variables having nonlinearity greater than the bent concatenation bound, *Proceedings of Boolean Functions: Cryptography and Applications*, (2008), 109–118.

[16] M. Matsui, Linear cryptanalysis method for DES cipher, *Cryptographic Techniques-EUROCRYPT'93*, *Lecture Notes in Computer Science*, **765** (1993), 386–397.

[17] K. Nyberg, Differentially uniform mappings for cryptography, *Advances in Cryptology-EUROCRYPT'93*, *Lecture Notes in Computer Science*, **765** (1994), 55–64.

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

[19] V. Rijmen, P. S. L. M. Barreto and D. L. Gazzoni Filho, Rotation symmetry in algebraically generated cryptographic substitution tables, *Information Processing Letters*, **106** (2008), 246–250.

[20] S. Sarkar and S. Maitra, Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros, *Designs, Codes and Cryptography*, **49** (2008), 95–103.

[21] P. Stănică and S. Maitra, Rotation symmetric Boolean functions - count and cryptographic properties, *Discrete Applied Mathematics*, **156** (2008), 1567–1580.

[22] P. Stănică, S. Maitra and J. Clark, Results on rotation symmetric bent and correlation immune Boolean functions, *Fast Software Encryption Workshop – FSE 2004*, *Lecture Notes in Computer Science*, **3017** (2004), 161–177.

Received for publication November 2018.

E-mail address: skavut@balikesir.edu.tr
E-mail address: stutdere@gmail.com