Classification of $$6\times 6$$ S-boxes Obtained by Concatenation of RSSBs

Conference Paper *in* Lecture Notes in Computer Science · March 2017

DOI: 10.1007/978-3-319-55714-4_8

CITATIONS
0

READS
39

2 authors:

Selçuk Kavut
Balikesir University
30 PUBLICATIONS **320** CITATIONS
SEE PROFILE

Sevdenur Baloglu
Middle East Technical University
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Classification of 6×6 S-boxes Obtained by Concatenation of RSSBs

Selçuk Kavut and Sevdenur Baloğlu

[1] Department of Computer Engineering, Balıkesir University, 10145 Balıkesir, Turkey. Email: skavut@balikesir.edu.tr
[2] Institute of Applied Mathematics, Middle East Technical University, 06800 Ankara, Turkey. Email: sevdenur.baloglu@metu.edu.tr

Abstract. We give an efficient exhaustive search algorithm to enumerate 6×6 bijective S-boxes with the best known nonlinearity 24 in a class of S-boxes that are symmetric under the permutation $\tau(x) = (x_0, x_2, x_3, x_4, x_5, x_1)$, where $x = (x_0, x_1, \ldots, x_5) \in \mathbb{F}_2^6$. Since any S-box $S : \mathbb{F}_2^6 \to \mathbb{F}_2^6$ in this class has the property that $S(\tau(x)) = \tau(S(x))$ for all x, it can be considered as a construction obtained by the concatenation of 5×5 rotation-symmetric S-boxes (RSSBs). The size of the search space, i.e., the number of S-boxes belonging to the class, is $2^{61.28}$. By performing our algorithm, we find that there exist $2^{37.56}$ S-boxes with nonlinearity 24 and among them the number of differentially 4-uniform ones is $2^{33.99}$, which indicates that the concatenation method provides a rich class in terms of high nonlinearity and low differential uniformity. Moreover, we classify those S-boxes achieving the best possible trade-off between nonlinearity and differential uniformity within the class with respect to absolute indicator, algebraic degree, and transparency order.

1 Introduction

The design of vectorial Boolean functions, or so-called S-boxes, is one of the most important subjects in secret-key cryptography since the S-boxes are the only nonlinear parts of iterated block ciphers, providing confusion for the cryptosystem. It is usually crucial for an S-box to be bijective, e.g. in a Substitution-Permutation Network (SPN), which in practice is required to exist in even dimension for implementation efficiency. Constructing such S-boxes with desirable cryptographic properties such as high nonlinearity, low differential uniformity, and high algebraic degree is essential in order to resist against linear [20], differential [1], and higher order differential [17] cryptanalyses, respectively. For instance, the SPN-based block cipher Advanced Encryption Standard (AES) uses the S-box affine equivalent to the inverse function [24] over $\mathbb{F}_{2^8}$, which achieves the best known trade-off (in dimension 8) among these cryptographic properties, i.e., the nonlinearity 112, differential uniformity 4, and maximum possible algebraic degree 7. Yet, in even dimension n, there are very few differentially 4-uniform constructions that are bijective with the nonlinearity $2^{n-1}-2^{\frac{n}{2}}$ (conjectured [7] to be the maximum) in the relevant literature (e.g., Gold [10], Kasami [11], the

binomial function [3], and the constructions in [2, 18, 19, 31]). In fact, most of these constructions exhibit some potential weaknesses; for instance, the binomial function and the power mappings except the inverse and Kasami functions have low algebraic degrees, which should be greater than 3 to provide robustness against higher order differential cryptanalysis. In addition, there exists only one sporadic example of an Almost Perfect Nonlinear (APN; that is, differentially 2-uniform) permutation in dimension n=6, identified [4] in 2009. It is well-known that there is no APN bijections over $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^4}$, and the construction of more APN bijections over $\mathbb{F}_{2^n}$ for even $n \geq 6$ is an important open problem.

Recall that in [9], a cryptographic criterion, so-called the non-possession of linear redundancy, was proposed as an indicator of randomness for S-boxes. Let m_{lr} denote the number of distinct (extended) affine equivalence classes to which the component Boolean functions of an S-box belong. For any S-box described as a power map over $\mathbb{F}_{2^n}$, it is well-known that $m_{lr} = 1$ (notice that $m_{lr} = 1$ for the AES S-box), and hence such S-boxes are considered [9] as a potential source of a new cryptanalysis. For our case, if we take the symmetric S-boxes into account in terms of linear redundancy, m_{lr} can be at most one less than the number of distinct orbits (which can be deduced from Corollary 5 in [13]). However, we here focuse only on the most important cryptographic properties mentioned previously and do not analyze our results in terms of linear redundancy.

While the aforementioned cryptanalytic attacks are realized independently from the hardware or software implementation of a cryptographic system, the side channel analysis (SCA) can be mounted using the information leaked through its implementation such as the timing of operations [15], power consumption [16], and electromagnetic radiation [28]. Therefore, the resistance of cryptographic primitives against SCA attacks is of great importance as well. In this class of attacks, one of the most powerful is the differential power analysis (DPA) attacks, which have received significant attention from cryptographers for nearly two decades. In 2005, the DPA resistivity of an S-box was quantified [27] introducing the notion of transparency order (TO). A decade later, the definition of TO was modified [6] by taking the cross-correlation terms between the coordinate functions into account. We here use the former definition [27] in our classification, for which its validity has been verified by several implementation results on cryptographic devices such as SASEBO-GII board [21–23] and ATmega163 smartcard [25, 26].

In this paper, we aim to classify 6×6 bijective S-boxes with nonlinearity ≥ 24 and differential uniformity ≤ 4 belonging to a rich class in terms of these cryptographic properties, for which the search space is of size $2^{61.28}$, with respect to absolute indicator, algebraic degree, and transparency order. This class corresponds to the S-boxes that are symmetric under the permutation $\tau(x)$=(x_0, x_2, x_3, x_4, x_5, x_1), where x=(x_0, $x_1, \ldots, x_5$) $\in \mathbb{F}_2^6$ (an n×n S-box is called symmetric under a permutation π if it satisfies $S(\pi(x)) = \pi(S(x))\ \forall x \in \mathbb{F}_2^n$). In [13], all 6! permutations are classified up to the linear equivalence of 6×6 S-boxes that are symmetric under them, and 11 different classes are obtained. Among these classes, the one for which the S-boxes are symmetric under the representative

permutation $\sigma(x)$=$(x_0,\ x_4, x_1, x_2, x_5, x_3)$ seems to be rich in terms of desirable cryptographic properties, since highly nonlinear S-boxes with low differential uniformity could be obtained [13] in this class by heuristic search. In fact one can find that (using Proposition 13 in [13]) the latter class is linearly equivalent to the former one. We here prefer using the former permutation, since in this case the S-boxes can be interpreted as those obtained by the concatenation of two 5×5 RSSBs and of two 5-variable rotation-symmetric Boolean functions (RSBFs). Notice that since an RSSB can be represented by a single rotation-symmetric Boolean function (RSBF), all the output bits of an S-box that is symmetric under τ can be described by only four 5-variable RSBFs, which can be utilized to provide implementaton advantages in both hardware or software.

Note that the class of 6×6 bijective RSSBs with nonlinearity 24 and differential uniformity 4 (which is the best possible trade-off within the class) are classified in [13] in terms of algebraic degree and absolute indicator (later their TOs are computed in [8]). This class corresponds to another one among the aforementioned 11 classes. The search strategy in [13] uses the fact that some of the component functions of an n×n RSSB are k-rotation-symmetric Boolean functions (k-RSBFs) [12], and thus it is mainly based on first sieving some of these k-RSBFs and then regenerating the RSSBs containing those k-RSBFs. Here, since none of the component functions of an S-box (symmetric under the permutation τ) is a k-RSBFs, it is not possible to apply the search method of [13]. Hence, we give a different search strategy in which the 5×5 RSSBs mentioned above are eliminated efficiently.

The remainder of this paper is organized as follows. In the following section, we provide some preliminaries and technical background on the symmetric S-boxes constructed by the concatenation of RSSBs. In Section 3, we present our search strategy to enumerate 6×6 bijective S-boxes having nonlinearity 24 that are symmetric under the permutation τ. The classification results of those with differential uniformity 4 are presented in Section 4, and we draw our conclusions in Section 5.

2 Preliminaries

2.1 Cryptographic Properties

For completeness, we briefly review the basic definitions regarding to the cryptographic properties of the S-boxes. Let us consider an n×m S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and represent S as a composition of m Boolean functions $f_0, f_1, \ldots, f_{m-1}$ each of which is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, that is, $S(x) = (f_0(x), f_1(x), \ldots, f_{m-1}(x))$ for all $x \in \mathbb{F}_2^n$. The functions $(f_i)_{0\le i\le m-1}$ are called the coordinate functions, and their linear combinations $\bigoplus_{i=0}^{m-1} v_i f_i$ with non all-zero masking (or coefficient) vectors $v = (v_0, v_1, \ldots, v_{m-1}) \in \mathbb{F}_2^m$ are called the component functions.

Algebraic degree. There are two notions of the algebraic degree relevant to cryptography [5]: The maximum degree of the coordinate functions and the

minimum degree of the component functions, which we denote as $d_{\max}$ and $d_{\min}$ respectively. The degree of a component (or coordinate) function can be computed using the algebraic normal form (ANF) of a Boolean function $f(x)$ of n-variable $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$, which is a unique representation in the form of a multivariate polynomial over $\mathbb{F}_2$,

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

where the coefficients $a_u \in \mathbb{F}_2$. The algebraic degree, or simply the degree of f is defined as the maximum Hamming weight of u such that $a_u \neq 0$. A Boolean function is called affine if its algebraic degree is ≤ 1. An affine function with zero constant term is called a linear function.

Nonlinearity. Nonlinearity of S is defined as the minimum Hamming distance of all $2^m - 1$ component functions from all n-variable affine functions, which can be expressed in terms of its Walsh transformation defined as an even integer-valued function $W_S : \mathbb{F}_2^n \times \mathbb{F}_2^m \to [-2^n, 2^n]$:

$$W_S(\omega, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\omega \cdot x \oplus v \cdot S(x)},$$

where the inner product is over $\mathbb{F}_2$, $\omega \in \mathbb{F}_2^n$, and $v \in \mathbb{F}_2^{m*}$. It can be seen that if one of the component functions $v \cdot S(x)$ is affine, then the maximum value in the absolute Walsh spectrum is 2^n, giving rise to zero nonlinearity. Nonlinearity of S is then given by

$$NL_S = 2^{n-1} - \frac{1}{2} \max_{\substack{\omega \in \mathbb{F}_2^n, \\ v \in \mathbb{F}_2^{m*}}} |W_F(\omega, v)|.$$

Diferential Uniformity. The differential uniformity δ [24] of S is defined as the maximum number of solutions of the equation $S(x) \oplus S(x \oplus \gamma) = \beta$, where $\gamma \neq (0, 0, \ldots, 0)$, i.e.,

$$\delta = \max_{\substack{\gamma \in \mathbb{F}_2^{n*}, \\ \beta \in \mathbb{F}_2^m}} \left| \{ x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \gamma) = \beta \} \right|,$$

Accordingly, S is called differentially-δ uniform.

Absolute Indicator. The absolute indicator is an important cryptographic criterion related to the autocorrelation spectrum, which is used to have good diffusion properties. The autocorrelation function of S is defined as

$$r_S(a, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot (S(x) \oplus S(x \oplus a))},$$

where $a \in \mathbb{F}_2^n$. The maximum absolute value in the autocorrelation spectrum, except those values for all-zero input difference and masking vectors, is referred to as the absolute indicator, denoted as

$$\Delta_S = \max_{\substack{a \in \mathbb{F}_2^{n*}, \\ v \in \mathbb{F}_2^{m*}}} |r_S(a, v)|.$$

Transparency Order. For an $n \times m$ S-box S, it is given [6] by

$$\tau_S = m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \left| \sum_{\substack{v \in \mathbb{F}_2^m, \\ wt(v)=1}} r_S(a, v) \right|.$$

In the following, we first restate some basic definitions related to RSSBs and then explain our method to construct a bijective S-box that is symmetric under the permutation $\tau(x)=(x_0, x_2, x_3, x_4, x_5, x_1)$ as a concatenation of two 5×5 RSSBs. After that, the search space of size $2^{61.28}$ (mentioned in Introduction) is partitioned into four subspaces, each of which is traversed efficiently as explained in Section 3.

2.2 (Concatenation of) RSSBs

Rotation-symmetric S-boxes (RSSBs) were defined in [29]. Let

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

be the k-cyclic shift operator. An S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called rotation-symmetric if $\rho^k(S(x)) = S(\rho^k(x)) \; \forall \; x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$ and $1 \leq k \leq n$. If $m = 1$, then it is called rotation-symmetric Boolean function (RSBF). Let S be generated from $s : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ using a normal basis for $\mathbb{F}_{2^n}$. Then, as indicated in [29], the S-boxes satisfying $(s(\alpha))^2 = s(\alpha^2)$, $\forall \; \alpha \in \mathbb{F}_{2^n}$, can be regarded as rotation-symmetric. In the rest of this paper, we consider the S-boxes for which $m = n$.

The orbit of $x \in \mathbb{F}_2^n$ under the cyclic rotation is given by the set $G_n(x) = \{\rho^k(x) \mid 1 \leq k \leq n\}$. Let g_n be the number of distinct orbits. Using Burnside's Lemma, it can be shown [30] that $g_n = \frac{1}{n} \sum_{t|n} \phi(t) 2^{\frac{n}{t}} (\approx \frac{2^n}{n})$, where $\phi(t)$ is the Euler's *phi*-function. The lexicographically first element within the i^{th} orbit is called the orbit representative and denoted by Λ_i, where $1 \leq i \leq g_n$.

Since an $n \times n$ RSSB S is uniquely defined by its outputs for the orbit representatives Λ_i's, the concatenation $F : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^n$ of two $n \times n$ RSSBs S_1 and S_2, described by $F(x) = (x_0 \oplus 1) S_1(x_1, ..., x_n) + x_0 S_2(x_1, ..., x_n)$, is denoted as

$$(S_1(\Lambda_1), ..., S_1(\Lambda_{g_n})) || (S_2(\Lambda_1), ..., S_2(\Lambda_{g_n})),$$

or simply as $S_1 || S_2$, where $x = (x_0, x_1, ..., x_n) \in \mathbb{F}_2^{n+1}$. Let $f : \mathbb{F}_2^{n+1} \to \mathbb{F}_2$ be a Boolean function such that the S-box $\mathcal{S} : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}$, given by $\mathcal{S}(x) =$

$(f(x), F(x))$, is bijective and symmetric under the permutation $\tau(x) = (x_0, x_2, x_3, \ldots, x_n, x_1)$. Then, notice that as f is invariant under τ, $f(x)$ is either equal to 1 or 0 for all cyclic rotations of $(x_1, ..., x_n)$. In addition, since $\mathcal{S}$ is bijective, the outputs of F contain all the orbit representatives Λ_i's, $i = 1, 2, \ldots, g_n$, and these orbit representatives are pairwise the same with one another. Accordingly, for such a pair $f(x)$=1 for one orbit and $f(x)$=0 for the other one.

More specifically, let $H_n(x)$ and $H_n(x')$ be two distinct sets with the same cardinality, where $H_n(x) = \{\tau^k(x) | 1 \leq k \leq n\}$. Then, for all Λ_i there exist $\nu, \mu \in G_n(\Lambda_i)$ such that $F(\tau^l(x))$=$\rho^l(\nu)$ and $F(\tau^l(x'))$=$\rho^l(\mu)$ for which $f(\tau^l(x))$=e and $f(\tau^l(x'))$=$e \oplus 1$ $\forall$ l=1, ..., n, where $e \in \mathbb{F}_2$. As a consequence, f is a balanced function such that it is a concatenation of two n-variable RSBFs f_1 and f_2, i.e., $f(x)$=$(x_0 \oplus 1) f_1(x_1, \ldots, x_n) + x_0 f_2(x_1, \ldots, x_n)$, and the number of f's to construct a bijective $\mathcal{S}$ given the concatenation F is equal to 2^{g_n}.

2.3 Partitioning Search Space

As already mentioned, the concatenation $F = S_1 || S_2$ contains each orbit representative Λ_i pairwisely in its outputs, from which one can see that both the S-boxes S_1 and S_2 follow a certain structure. For instance, if one of the RSSBs has a pair of the same orbit representatives in its outputs, then the other one cannot have these outputs. Following this argument, the output orbit representatives of S_1 can be completely determined given those of S_2, and vice versa. For our case n=5, the number of orbits g_5=8 such that six of them are of size 5 and the rest two are of size 1. Therefore, F contains four orbits of size 1, that is,

$$\begin{aligned}(F(0, \Lambda_1), F(0, \Lambda_8), F(1, \Lambda_1), F(1, \Lambda_8)) &= (S_1(\Lambda_1), S_1(\Lambda_8), S_2(\Lambda_1), S_2(\Lambda_8)) \\ &\in \mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8),\end{aligned}$$

where Λ_1 and Λ_8 are the all-zero and all-one vectors, respectively, and $\mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8)$ is the set of permutations of $\{\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8\}$. Similarly, the outputs $(f(0, \Lambda_1), f(0, \Lambda_8), f(1, \Lambda_1), f(1, \Lambda_8)) \in \mathcal{P}(0, 0, 1, 1)$.

Now, let us consider the output orbits of size 5. In this case, since the S-box $\mathcal{S} = (f, F)$ is bijective, any choice of the output orbit representatives for both S_1 and S_2 belong to one of the following four sets:

1. $\mathbb{S}_0$=$\{(\Lambda_2, \ldots, \Lambda_7)\}$,
2. $\mathbb{S}_1$=$\{(\Lambda_{i_1}, \ldots, \Lambda_{i_6}) \mid i_1 = i_2, i_1 \neq i_3 \neq i_4 \neq i_5 \neq i_6\}$,
3. $\mathbb{S}_2$=$\{(\Lambda_{i_1}, \ldots, \Lambda_{i_6}) \mid i_1 = i_2, i_3 = i_4, i_1 \neq i_3 \neq i_5 \neq i_6\}$,
4. $\mathbb{S}_3$=$\{(\Lambda_{i_1}, \ldots, \Lambda_{i_6}) \mid i_1 = i_2, i_3 = i_4, i_5 = i_6, i_1 \neq i_3 \neq i_5\}$,

where $i_1, \ldots, i_6 \in \{2, \ldots, 7\}$ and $(\Lambda_{i_1}, \ldots, \Lambda_{i_6})$'s are different up to permutation. As can be seen, the set $\mathbb{S}_0$ consists of only one choice $(\Lambda_2, \ldots, \Lambda_7)$ for the output orbit representatives, which implies that all the output orbits (of size 5) are different from each other for both S_1 and S_2. The other sets are interpreted similarly, e.g., if the representatives of the output orbits of S_1 belong to $\mathbb{S}_1$, then those of S_2 should also belong to $\mathbb{S}_1$, and each of S_1 and S_2 have one pair

of the same orbit representatives in their outputs. Notice that the numbers of the choices for the sets $\mathbb{S}_1$, $\mathbb{S}_2$, and $\mathbb{S}_3$ are $\binom{6}{1}\binom{5}{4}$=30, $\binom{6}{2}\binom{4}{2}$=90, and $\binom{6}{3}$=20, respectively.

Here, we give an example which shows that given the output orbit representatives of S_1, those of S_2 and all possible choices of the Boolean function f can be completely found.

Example 1. Let

$$(S_1(\Lambda_1), \ldots, S_1(\Lambda_8)) = (F(0, \Lambda_1), \ldots, F(0, \Lambda_8)) = \\ (\mathbf{1}, \pi_1(\rho^{k_1}(\Lambda_4), \rho^{k_2}(\Lambda_4), \rho^{k_3}(\Lambda_7), \rho^{k_4}(\Lambda_7), \rho^{k_5}(\Lambda_2), \rho^{k_6}(\Lambda_3)), \mathbf{0}),$$

where $(k_1, ..., k_6) \in \{1, ..., 5\}^6$, π_1 is any permutation of the six outputs, $\mathbf{0}$ and $\mathbf{1}$ are the all-zero and all-one vectors, respectively. It can be seen that the output orbit representatives (of size 5) of S_1 belong to the set $\mathbb{S}_2$. Hence, those of S_2 should also belong to the same set as given below:

$$(S_2(\Lambda_1), \ldots, S_2(\Lambda_8)) = (F(1, \Lambda_1), \ldots, F(1, \Lambda_8)) = \\ (u, \pi_2(\rho^{l_1}(\Lambda_5), \rho^{l_2}(\Lambda_5), \rho^{l_3}(\Lambda_6), \rho^{l_4}(\Lambda_6), \rho^{l_5}(\Lambda_2), \rho^{l_6}(\Lambda_3)), u \oplus \mathbf{1}),$$

where $u \in \{\mathbf{0}, \mathbf{1}\}$, $(l_1, ..., l_6) \in \{1, ..., 5\}^6$, and π_2 is also a permutation. Further, if $F(x) = F(x')$ for two distinct $x, x' \in \mathbb{F}_2^6$, then $f(\tau^l(x')) = f(\tau^l(x)) \oplus 1 \ \forall \ 1 \leq l \leq 5$. For instance, considering the orbits Λ_1 and Λ_8, if $(F(0, \Lambda_1), F(0, \Lambda_8), F(1, \Lambda_1), F(1, \Lambda_8)) = (\mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{1})$ (i.e. $u = \mathbf{0}$), then

$$(f(0, \Lambda_1), f(0, \Lambda_8), f(1, \Lambda_1), f(1, \Lambda_8)) \in \\ \{(0, 0, 1, 1), (0, 1, 0, 1), (1, 0, 1, 0), (1, 1, 0, 0)\}.$$

Otherwise, if $(F(0, \Lambda_1), F(0, \Lambda_8), F(1, \Lambda_1), F(1, \Lambda_8)) = (\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0})$ (i.e., $u = \mathbf{1}$), then

$$(f(0, \Lambda_1), f(0, \Lambda_8), f(1, \Lambda_1), f(1, \Lambda_8)) \in \\ \{(0, 0, 1, 1), (0, 1, 1, 0), (1, 0, 0, 1), (1, 1, 0, 0)\}.$$

Let us refer to the set of S-boxes $\mathcal{S} = (f, F)$ for which the output orbit representatives (other than Λ_1 and Λ_8) of both S_1 and S_2 belong to $\mathbb{S}_k$ as 'Set-k', $k = 0, 1, 2, 3$. Then, each Set-k is generated by the algorithm given below.

Algorithm 1: Forming Set-k from the orbit representatives in $\mathbb{S}_k$.

Input: $\mathbb{S}_k$
Output: Set-k

Set-k is empty;
for *each* $(S_1(\Lambda_1), S_1(\Lambda_8), S_2(\Lambda_1), S_2(\Lambda_8)) \in \mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8)$ **do**
  for *each* $(S_1(\Lambda_2), ..., S_1(\Lambda_7)) \in \mathbb{S}_k$ **do**
    for *each* $(S_1(\Lambda_2), ..., S_1(\Lambda_7)) \in \mathcal{P}(S_1(\Lambda_2), ..., S_1(\Lambda_7))$ **do**
      Determine the output orbits of S_2 from S_1;
      for *each* $(S_2(\Lambda_2), ..., S_2(\Lambda_7)) \in \mathcal{P}(S_2(\Lambda_2), ..., S_2(\Lambda_7))$ **do**
        for *each* $(k_1, ..., k_6) \in \{1, ..., 5\}^6$ **do**
          $S_1 = (S_1(\Lambda_1), \rho^{k_1}(S_1(\Lambda_2)), ..., \rho^{k_6}(S_1(\Lambda_7)), S_1(\Lambda_8))$;
          for *each* $(l_1, ..., l_6) \in \{1, ..., 5\}^6$ **do**
            $S_2 = (S_2(\Lambda_1), \rho^{l_1}(S_2(\Lambda_2)), ..., \rho^{l_6}(S_2(\Lambda_7)), S_2(\Lambda_8))$;
            $F = S_1 || S_2$;
            $\mathcal{F} = \{f : \mathbb{F}_2^6 \to \mathbb{F}_2 | f(\tau^l(x)) = f(\tau^l(x')) \oplus 1,$
            for all two distinct $x, x' \in \mathbb{F}_2^5$ s.t. $F(x) = F(x')\}$;
            for *each* $f \in \mathcal{F}$ **do**
              Add $\mathcal{S} = (f, F)$ to the Set-k;
            end
          end
        end
      end
    end
  end
end

In the algorithm, we see that $|\mathcal{P}(\Lambda_1, \Lambda_1, \Lambda_8, \Lambda_8)|$=6, $|\mathcal{F}|$=2^8, and the number of all rotations is equal to 5^{12} (as can be seen from the fifth and sixth loops of the algorithm) for each Set-k. Hence, the number of S-boxes, e.g., in Set-1 is computed as $6 \times 30 \times 360^2 \times 5^{12} \times 2^8 \approx 2^{60.34}$, since $|\mathbb{S}_1|$=30 and $|\mathcal{P}(S_1(\Lambda_2), ..., S_1(\Lambda_7))|$ $=|\mathcal{P}(S_2(\Lambda_2), ..., S_2(\Lambda_7))|$=360 for all $(S_1(\Lambda_2), ..., S_1(\Lambda_7)), (S_2(\Lambda_2), ..., S_2(\Lambda_7)) \in \mathbb{S}_1$. Similarly, the numbers of S-boxes in Set-0, Set-2, and Set-3 are found to be $2^{57.43}$, $2^{59.92}$, and $2^{55.75}$, respectively.

3 Search Strategy

In this section, we present our search strategy, which can be considered as a three step process, to enumerate the S-boxes with nonlinearity 24 in each of the subsets Set-k, $k = 0, 1, 2, 3$, formed by Algorithm 1.

3.1 Sieving Affine Equivalent Concatenations

Recall that the number of pairwise the same orbit representatives in the outputs of S_1 should be the same as the number of those in the outputs of S_2. Let

$S_j^{(k)}$ denote the RSSB S_j ($j = 1, 2$) for which this number is represented by $k \in \{0, 1, 2, 3\}$. Then, taking all possible permutations of ($S_1^{(k)}(\Lambda_1)$, $S_1^{(k)}(\Lambda_8)$, $S_2^{(k)}(\Lambda_1)$, $S_2^{(k)}(\Lambda_8)$) into account, the number of choices in $\mathbb{S}_k$ is multiplied by 6. More specifically, it can be computed as $\binom{6}{k}\times\binom{6-k}{6-2k}\times 6$ for each $\mathbb{S}_k$. Here, we sieve some of these choices leading to affine equivalent S-boxes, due to the fact that the nonlinearity is invariant under affine transformations.

Let us define the circulant matrix $C^i(a)$, used in the following proposition, which is formed by taking $a=(a_0, a_1 \ldots, a_{n-1}) \in \mathbb{F}_2^n$ as the first row and rotating each row i-bit to the left relative to the preceding row, where $1 \leq i \leq n$:

$$C^i(a)= \begin{bmatrix} a \\ \rho^i(a) \\ \vdots \\ \rho^{(n-1)i \pmod n}(a) \end{bmatrix}.$$

The proposition given below defines some affine transformations (which can be obtained using those among the RSSBs given by Proposition 8 in [13]) among the concatenations.

Proposition 1. *Let $F = (S_1||S_2)$ be a concatenation of two $n\times n$ RSSBs S_1 and S_2. Then each of the following functions, denoted by F', is also a concatenation of two $n\times n$ RSSBs and affine equivalent to F:*

1. *(complement) $F'(x) = F(x)\oplus\mathbf{1}$,*
2. *(reverse) $F'(x) = F(x\oplus\mathbf{1})$,*
3. *(transposition) $F' = (S_2||S_1)$,*
4. *(circulant matrix multiplication) $F'(x) = F(xD^q(a))C^p(b)$,*

where p, q are co-prime to n such that $pq \equiv 1 \pmod n$, $D^q(a)= \left[\begin{array}{c|c} 1 & 0\cdots 0 \\ \hline 0 & \\ \vdots & C^q(a) \\ 0 & \end{array}\right]$, $a, b \in \mathbb{F}_2^n$, $x \in \mathbb{F}_2^{n+1}$, and $C^q(a)$, $C^p(b)$ are nonsingular circulant matrices over $\mathbb{F}_2$.

Using these transformations (or their compositions) we sieve the aforementioned choices for the output orbit representatives, which generate affine equivalent S-boxes as shown by the next proposition.

Proposition 2. *Let $\mathcal{S}(x) = (f(x), F(x))$ be an $(n+1)\times(n+1)$ symmetric S-box under the permutation $\tau(x) = (x_0, x_2, x_3, \ldots, x_n, x_1)$, where $x = (x_0, x_1, \ldots, x_n) \in \mathbb{F}_2^{n+1}$, f is an $(n+1)$-variable Boolean function, and F is a concatenation of two $n\times n$ RSSBs. Assume that F', also a concatenation of two $n\times n$ RSSBs, is obtained by the affine transformations given by Prop. 1. Then, there exists an $(n+1)$-variable Boolean function f' such that $\mathcal{S}' = (f', F')$ is symmetric under τ and affine equivalent to $\mathcal{S}$.*

Proof. It is easy to prove for the first three affine transformations in Prop. 1. Let us consider the last one, i.e., circulant matrix multiplication. Then, we have

$$\begin{aligned}\mathcal{S}'(x) &= (f'(x), F'(x)) \\ &= (f(xD^q(a)), F(xD^q(a))C^p(b)) \\ &= (f(xD^q(a)), F(xD^q(a)))D^p(b) \\ &= \mathcal{S}(xD^q(a))D^p(a),\end{aligned}$$

where $f'(x) = f(xD^q(a)) \ \forall \ x \in \mathbb{F}_2^{n+1}$, which shows that $\mathcal{S}$ and $\mathcal{S}'$ are affine equivalent. Next, we get the following:

$$\begin{aligned}&\mathcal{S}'(\tau(x)) = \mathcal{S}(\tau(x)D^q(a))D^p(b) \\ &= (f(\tau(x)D^q(a)), F(\tau(x)D^q(a))C^p(b)) \\ &= (f(x_0, \rho(x_1, \ldots, x_n)C^q(a)), F(x_0, \rho(x_1, \ldots, x_n)C^q(a))C^p(b)) \\ &= (f(x_0, \rho^{n-q}((x_1, \ldots, x_n)C^q(a))), F(x_0, \rho^{n-q}((x_1, \ldots, x_n)C^q(a)))C^p(b)) \\ &= (f(\tau^{n-q}(x_0, (x_1, \ldots, x_n)C^q(a))), \rho^{n-q}(F(x_0, (x_1, \ldots, x_n)C^q(a)))C^p(b)) \\ &= (f(x_0, (x_1, \ldots, x_n)C^q(a)), \rho^{(n-q)(n-p)}(F(x_0, (x_1, \ldots, x_n)C^q(a))C^p(b))) \\ &= (f(x_0, (x_1, \ldots, x_n)C^q(a)), \rho(F(x_0, (x_1, \ldots, x_n)C^q(a))C^p(b))) \\ &= (f(xD^q(a)), \rho(F(xD^q(a))C^p(b))) \\ &= \tau(\mathcal{S}(xD^q(a))D^p(b)) \\ &= \tau(\mathcal{S}'(x)),\end{aligned}$$

which follows from the fact that $\rho(x_1, \ldots, x_n)C^q(a) = \rho^{n-q}((x_1, \ldots, x_n)C^q(a))$, where ρ is the cyclic shift operator. Hence, $\mathcal{S}'$ is also symmetric under τ. □

As mentioned previously, for $k = 0, 1, 2, 3$ the number of choices (obtained by considering the 6 combinations of the orbits of size 1) for $\mathbb{S}_k$ can be found as 6, 180, 540, 120, respectively. After sieving those yielding affine equivalent concatenations these numbers are reduced to 2, 8, 21, and 9, respectively. In Table 1, we give these representative choices for each $\mathbb{S}_k$ along with the number of those generating affine equivalent S-boxes.

In addition, it is clear that any S-box obtained by rotating all of the outputs of an RSSB by the same number of positions is also an RSSB and this operation is an affine transformation (for which a more general form is given by the last item of Proposition 1). Hence, we set $F(0, 0, 0, 0, 0, 1) = \Lambda_i$, for any $i \in \{2, 3, \ldots, 7\}$, where Λ_i is an orbit representative with orbit size 5, in order to remove affine equivalent concatenations. This provides a reduction of the search space by a factor of $\frac{1}{5}$.

At the end of this step, the number of S-boxes in Set-k reduces from $2^{57.43}$, $2^{60.34}$, $2^{59.92}$, and $2^{55.75}$ to $2^{53.52}$, $2^{53.52}$, $2^{52.92}$, and $2^{49.69}$, respectively. Hence, the total search space reduces from $2^{61.28}$ to $2^{54.97}$.

Table 1. The representative choices and the number (N_i) of those for which the concatenations $(S_1||S_2)$ are affine equivalent for $\mathbb{S}_k$, $k = 0, 1, 2, 3$.

	i	S_1	S_2	N_i
$\mathbb{S}_0$	**1**	$(\boldsymbol{\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_1})$	$(\boldsymbol{\Lambda_8, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_8})$	**2**
	2	$(\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_8)$	$(\Lambda_8, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_1)$	4
$\mathbb{S}_1$	**1**	$(\boldsymbol{\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_1})$	$(\boldsymbol{\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8})$	**6**
	2	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_7, \Lambda_1)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_8)$	24
	3	$(\boldsymbol{\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_1})$	$(\boldsymbol{\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_8})$	**12**
	4	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	6
	5	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_1)$	12
	6	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	24
	7	$(\boldsymbol{\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_7, \Lambda_8})$	$(\boldsymbol{\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1})$	**48**
	8	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_1)$	48
$\mathbb{S}_2$	1	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_1)$	$(\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)$	12
	2	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_6, \Lambda_1)$	$(\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)$	12
	3	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_7, \Lambda_1)$	$(\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_8)$	24
	4	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_5, \Lambda_7, \Lambda_1)$	$(\Lambda_8, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_8)$	24
	5	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_1)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)$	12
	6	$(\boldsymbol{\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_7, \Lambda_1})$	$(\boldsymbol{\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_8})$	**12**
	7	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_1)$	$(\Lambda_8, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)$	6
	8	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_7, \Lambda_7, \Lambda_1)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_8)$	12
	9	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_8)$	$(\Lambda_1, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	12
	10	$(\boldsymbol{\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_7, \Lambda_8})$	$(\boldsymbol{\Lambda_1, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1})$	**24**
	11	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	12
	12	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_7, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1)$	12
	13	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	6
	14	$(\boldsymbol{\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_5, \Lambda_8})$	$(\boldsymbol{\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1})$	**48**
	15	$(\boldsymbol{\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_6, \Lambda_8})$	$(\boldsymbol{\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1})$	**24**
	16	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_7, \Lambda_8)$	$(\Lambda_8, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1)$	96
	17	$(\boldsymbol{\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_5, \Lambda_7, \Lambda_8})$	$(\boldsymbol{\Lambda_8, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1})$	**48**
	18	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	48
	19	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_7, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_1)$	48
	20	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_4, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	24
	21	$(\boldsymbol{\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_5, \Lambda_7, \Lambda_7, \Lambda_8})$	$(\boldsymbol{\Lambda_8, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_1})$	**24**
$\mathbb{S}_3$	1	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_1)$	$(\Lambda_8, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8)$	6
	2	$(\boldsymbol{\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_1})$	$(\boldsymbol{\Lambda_8, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_8})$	**12**
	3	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_1)$	$(\Lambda_8, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_7, \Lambda_7, \Lambda_8)$	2
	4	$(\boldsymbol{\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_8})$	$(\boldsymbol{\Lambda_1, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1})$	**6**
	5	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_8)$	$(\Lambda_1, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	12
	6	$(\Lambda_8, \Lambda_2, \Lambda_2, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_8)$	$(\Lambda_1, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_7, \Lambda_7, \Lambda_1)$	2
	7	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_8)$	$(\Lambda_8, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	24
	8	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_3, \Lambda_3, \Lambda_5, \Lambda_5, \Lambda_8)$	$(\Lambda_8, \Lambda_4, \Lambda_4, \Lambda_6, \Lambda_6, \Lambda_7, \Lambda_7, \Lambda_1)$	48
	9	$(\Lambda_1, \Lambda_2, \Lambda_2, \Lambda_5, \Lambda_5, \Lambda_6, \Lambda_6, \Lambda_8)$	$(\Lambda_8, \Lambda_3, \Lambda_3, \Lambda_4, \Lambda_4, \Lambda_7, \Lambda_7, \Lambda_1)$	8

3.2 Sieving RSSBs S_1 and S_2

In this step, we generate all the RSSBs S_1's and S_2's used to form the concatenation $F = (S_1||S_2)$. One can see that to construct an S-box $\mathcal{S} = (f, F)$ with nonlinearity ≥ 24, the nonlinearities of S_1 and S_2 have to be ≥ 8. We find that for some choices given in Table 1 there are no RSSBs (S_1 and S_2) with nonlinearity ≥ 8. More specifically, 6 out of the 21 choices (for $\mathbb{S}_2$) and 3 out of the 9 choices (for $\mathbb{S}_3$) in Table 1 generate neither S_1 nor S_2 with nonlinearity ≥ 8, and hence they are removed from the search space. These eliminated choices are N_5, N_7, N_{11}, N_{13}, N_{18}, N_{20} for $\mathbb{S}_2$ and N_3, N_6, N_9 for $\mathbb{S}_3$. Thus, after this preprocessing, the search space slightly reduces from $2^{54.97}$ to $2^{54.86}$.

Next, we apply a more efficient sieving method to reduce the number of choices for the output orbit representatives of S_1 and S_2. Let the sets Ω_1 and Ω_2 contain all the S_1's and S_2's generated from one of the remaining choices after the above elimination, respectively. Let the subset $\Omega_1^{[t,(\omega,v)]}$ of Ω_1 denote the S_1's for which the absolute Walsh spectrum value of a component function $v{\cdot}S_1$ at a position $\omega \in \mathbb{F}_2^5$ is equal to t (i.e., $|W_{S_1}(\omega, v)| = t$), where $v \neq \mathbf{0} \in \mathbb{F}_2^5$ and $t \in \{0, 2, ..., 16\}$. Similarly, given the triplet $[t, (\omega, v)]$, we constitute the subsets $\Omega_2^{[0,(\omega,v)]}$, $\Omega_2^{[2,(\omega,v)]}$, ..., $\Omega_2^{[16-t,(\omega,v)]}$ of Ω_2. As can be seen, the S_1's in $\Omega_1^{[t,(\omega,v)]}$ can be concatenated only with the S_2's in $\cup_{i\in\{0,2,...,16-t\}}\Omega_2^{[i,(\omega,v)]}$, since otherwise the nonlinearity of the concatenation F cannot reach to or exceed 24, leading to the fact that the nonlinearity of $\mathcal{S}$ is less than 24. Hence, if there is no S_2 in $\cup_{i\in\{0,2,...,16-t\}}\Omega_2^{[i,(\omega,v)]}$, then we update Ω_1 by $\Omega_1 \backslash \Omega_1^{[t,(\omega,v)]}$. Note that the set Ω_2 can also be updated similarly considering the concatenations formed by the S_2's in $\Omega_2^{[t,(\omega,v)]}$ and S_1's in $\cup_{i\in\{0,2,...,16-t\}}\Omega_1^{[i,(\omega,v)]}$. In addition, since for an RSSB S the component functions $(v{\cdot}S)$ for which the corresponding masking vectors (v) belong to the same orbit are affine equivalent (Prop. 4 in [13]), it suffices to apply this procedure only for the masking vectors that are orbit representatives.

Hence, we have performed the above method for all the triplets $[t, (\omega, v)]$, where the v's are orbit representatives, and found that the updated sets Ω_1 and Ω_2 are empty for some of the remaining choices in Table 1. More specifically, we find that these choices are N_1 for $\mathbb{S}_0$, N_2, N_4, N_5, N_6, N_8 for $\mathbb{S}_1$, N_1, N_2, N_3, N_4, N_8, N_9, N_{12}, N_{16}, N_{19} for $\mathbb{S}_2$, and N_1, N_5, N_7, N_8 for $\mathbb{S}_3$. Thus, the search space reduces from $2^{54.86}$ to $2^{53.63}$. In Table 1, the choices left after the first two steps of our search strategy are shown by bold font.

3.3 Sieving Concatenations with nonlinearity < 24

Let the updated sets of Ω_1 and Ω_2 after the previous step be $\overline{\Omega_1}$ and $\overline{\Omega_2}$, respectively. In this last step, we add the coordinate functions f's to the concatenations $F = (S_1||S_2)$ obtained from the S_1's in $\overline{\Omega_1}$ and S_2's in $\overline{\Omega_2}$. Here, as we enumerate the S-boxes in the form of $\mathcal{S} = (f, F)$ with nonlinearity ≥ 24, we select only those f's that achieve nonlinearity ≥ 24 among all possible f's (recall that given F, there can be only $2^{g_5} = 2^8$ f's making $\mathcal{S}$ bijective and symmetric under τ).

In addition, since the nonlinearities of $\mathcal{S} = (f, F)$ and $\mathcal{S}' = (f^c, F)$ are the same, where f^c is the complement of f, we fix $f(\mathbf{0}) = 0$, which reduces the search space by half.

To make this step more efficient, we apply a method similar to the one used in the previous step. Consider the subsets $\overline{\Omega_1}^{[t,(\omega,v)]}$ and $\cup_{i\in\{0,2,\ldots,16-t\}}\overline{\Omega_2}^{[i,(\omega,v)]}$ of $\overline{\Omega_1}$ and $\overline{\Omega_2}$, respectively. We choose each of the S_1's in the former subset and each of the S_2's in the latter one. If for some S_1 and S_2, the nonlinearity of $F \geq 24$, then we add each possible coordinate function f to form the S-box $\mathcal{S}$. If the nonlinearity of $\mathcal{S} \geq 24$, then we save $\mathcal{S}$ in a file. After that, as in the preceding step, since the S_1's in $\overline{\Omega_1}^{[t,(\omega,v)]}$ cannot be concatenated with any S_2's in $\overline{\Omega_2}$ except those in $\cup_{i\in\{0,2,\ldots,16-t\}}\overline{\Omega_2}^{[i,(\omega,v)]}$, we update $\overline{\Omega_1}$ by $\overline{\Omega_1}\backslash\overline{\Omega_1}^{[t,(\omega,v)]}$. Note that when we eliminate the S_1's in $\overline{\Omega_1}^{[t,(\omega,v)]}$, we also eliminate these S_1's belonging to the other subsets of Ω_1. Finally, by performing this procedure for all the triplets $[t, (\omega, v)]$, we reduce the search space to $2^{48.47}$.

4 Results

We find that in the class of 6×6 bijective S-boxes that are symmetric under the permutation τ, there are $2^{37.56}$ S-boxes with nonlinearity 24 and there is no S-box exceeding this nonlinearity. Further, among these S-boxes, the best differential uniformity is 4 and the number of differentially 4-uniform S-boxes is $2^{33.99}$. In [13], the S-boxes with the same cryptographic properties are enumerated in the class of bijective RSSBs for which the search space is of size $2^{47.90}$. In this class, it has been found that there are $2^{28.25}$ S-boxes with nonlinearity 24 and among them the number of those that are differentially 4-uniform is $2^{24.74}$. Compared to these results, our search identifies a much larger set of S-boxes achieving the same cryptographic properties than those found in [13].

Since the TO of an S-box is not in general invariant under the affine transformations, in our classification we generate (after completing the search) the S-boxes using those under which the TO is not invariant and compute the corresponding TOs. More specifically, let us consider an $n\times n$ S-box $T(x) = S(xA\oplus d)B\oplus e$, where A, B are nonsingular binary matrices and $d, e \in \mathbb{F}_2^n$. In [8], it was shown that the TO of $T(x)$ is the same as that of $S(xA\oplus d)\oplus e$, and later in [14] it has been shown that the TO of $T(x)$ is also invariant under the column permutation of B. Hence, we note that only the affine equivalent S-boxes obtained by the circulant matrix multiplication in Proposition 1 can have different the TOs.

In Table 2, we present the classification of the $2^{33.99}$ differentially 4-uniform S-boxes in terms of their absolute indicator (AI), algebraic degrees ($d_{\min}$ and $d_{\max}$, i.e., the minimum and maximum algebraic degrees among the component functions of a given S-box, resp.), and transparency order (TO). For each Set-k, $k = 0, 1, 2, 3$, the classification results are also given in Tables 3-6, from which it is seen that the numbers of differentially 4-uniform S-boxes with nonlinearity 24 are $2^{29.91}$, $2^{32.87}$, $2^{32.82}$, and $2^{29.09}$, respectively. It is seen from Table 2 that

the minimum transparency order the S-boxes have in this classification is 5.270. This value is attained from Set-2 and Set-3 as can be seen from Tables 5 and 6 (shown by bold font).

As mentioned in the previous section, we do not take the concatenations obtained by rotating all of the outputs by a fixed number of positions into account reducing the search space by a factor of $\frac{1}{5}$. Recall that, in addition, we fix $f(\mathbf{0}) = 0$, which further reduces the search space by a factor of $\frac{1}{2}$. Hence, the numbers of the S-boxes in Tables 2-6 are the multiples of 10.

Table 2. The classification of the 6×6 bijective S-boxes, constructed by the concatenation of RSSBs, with nonlinearity 24 and differential uniformity 4.

AI	$d_{\min}$	$d_{\max}$	TO	Number of S-boxes
24	3	4	$\geq 5.619, \leq 5.786$	10368×10
24	4	4	$\geq 5.413, \leq 5.889$	42695424×10
32	3	4	$\geq 5.548, \leq 5.849$	165888×10
32	4	4	$\geq 5.349, \leq 5.905$	629213184×10
32	4	5	$\geq 5.607, \leq 5.813$	10368×10
40	4	4	$\geq 5.421, \leq 5.905$	97096320×10
48	4	4	$\geq 5.480, \leq 5.889$	3400704×10
64	2	2	$\geq 5.714, \leq 5.714$	5184×10
64	2	3	$\geq 5.381, \leq 5.873$	730944×10
64	2	4	$\geq \mathbf{5.270}, \leq 5.905$	176613696×10
64	3	3	$\geq 5.500, \leq 5.905$	383616×10
64	3	4	$\geq 5.341, \leq 5.905$	753769152×10
64	3	5	$\geq 5.655, \leq 5.817$	10368×10
64	4	4	$\geq 5.607, \leq 5.770$	10368×10

The search algorithm is performed on a workstation with 2 CPUs of Intel Xeon Processor E5-2620v3 (15M Cache, 2.40 GHz, 6 cores) and 16 GB RAM under Windows 8.1 Professional 64-bit operating system. It takes around 10 days (236 hours) exploiting all the cores.

5 Conclusions

We have presented an efficient exhaustive search algorithm to enumerate the 6×6 bijective S-boxes with the best known nonlinearity 24 within the class of symmetric S-boxes under the permutation $\tau(x) = (x_0, x_2, x_3, x_4, x_5, x_1)$, where $x = (x_0, x_1 \ldots, x_5) \in \mathbb{F}_2^6$. Carrying out the search algorithm, which reduces the space from $2^{61.28}$ to $2^{48.47}$, we have classified differentially 4-uniform S-boxes among them in terms of absolute indicator, algebraic degree, and transparency order. Our results provide a large pool of choices for small-size S-boxes with desirable cryptographic properties such as low differential uniformity and high nonlinearity, especially suitable for lightweight cryptography.

Table 3. The classification of the S-boxes in Set-0 with nonlinearity 24 and differential uniformity 4.

AI	$d_{\min}$	$d_{\max}$	TO	Number of S-boxes
24	3	4	$\geq 5.619, \leq 5.730$	288×40
24	4	4	$\geq 5.440, \leq 5.889$	438336×40
32	3	4	$\geq 5.655, \leq 5.734$	288×40
32	4	4	$\geq 5.421, \leq 5.905$	9214560×40
32	4	5	$\geq 5.675, \leq 5.738$	288×40
40	4	4	$\geq 5.448, \leq 5.905$	1978848×40
48	4	4	$\geq 5.500, \leq 5.845$	126144×40
64	2	2	$\geq 5.714, \leq 5.714$	288×40
64	2	3	$\geq 5.381, \leq 5.873$	26496×40
64	2	4	$\geq 5.302, \leq 5.885$	2320704×40
64	3	3	$\geq 5.540, \leq 5.905$	25632×40
64	3	4	$\geq 5.341, \leq 5.905$	11161440×40
64	4	4	$\geq 5.607, \leq 5.770$	288×40

Table 4. The classification of the S-boxes in Set-1 with nonlinearity 24 and differential uniformity 4.

AI	$d_{\min}$	$d_{\max}$	TO	Number of S-boxes
24	3	4	$\geq 5.619, \leq 5.778$	3456×10
24	4	4	$\geq 5.417, \leq 5.889$	20560896×10
32	3	4	$\geq 5.556, \leq 5.849$	91008×10
32	4	4	$\geq 5.349, \leq 5.905$	290878848×10
32	4	5	$\geq 5.667, \leq 5.813$	3456×10
40	4	4	$\geq 5.429, \leq 5.905$	43205760×10
48	4	4	$\geq 5.480, \leq 5.889$	1359360×10
64	2	2	$\geq 5.714, \leq 5.714$	1152×10
64	2	3	$\geq 5.381, \leq 5.873$	271872×10
64	2	4	$\geq 5.341, \leq 5.905$	80786304×10
64	3	3	$\geq 5.500, \leq 5.905$	118656×10
64	3	4	$\geq 5.361, \leq 5.905$	350350848×10
64	3	5	$\geq 5.655, \leq 5.817$	4608×10
64	4	4	$\geq 5.607, \leq 5.770$	3456×10

Table 5. The classification of the S-boxes in Set-2 with nonlinearity 24 and differential uniformity 4.

AI	$d_{\min}$	$d_{\max}$	TO	Number of S-boxes
24	3	4	$\geq 5.619, \leq 5.786$	5760×10
24	4	4	$\geq 5.413, \leq 5.889$	19401984×10
32	3	4	$\geq 5.548, \leq 5.849$	71424×10
32	4	4	$\geq 5.349, \leq 5.905$	280242432×10
32	4	5	$\geq 5.607, \leq 5.813$	5760×10
40	4	4	$\geq 5.421, \leq 5.905$	41551488×10
48	4	4	$\geq 5.480, \leq 5.889$	1299456×10
64	2	2	$\geq 5.714, \leq 5.714$	2304×10
64	2	3	$\geq 5.381, \leq 5.873$	313344×10
64	2	4	$\geq \mathbf{5.270}, \leq 5.905$	81669888×10
64	3	3	$\geq 5.500, \leq 5.905$	110592×10
64	3	4	$\geq 5.361, \leq 5.905$	333317376×10
64	3	5	$\geq 5.655, \leq 5.817$	5760×10
64	4	4	$\geq 5.607, \leq 5.770$	5760×10

Table 6. The classification of the S-boxes in Set-3 with nonlinearity 24 and differential uniformity 4.

AI	$d_{\min}$	$d_{\max}$	TO	Number of S-boxes
24	4	4	$\geq 5.468, \leq 5.873$	979200×10
32	3	4	$\geq 5.599, \leq 5.746$	2304×10
32	4	4	$\geq 5.417, \leq 5.873$	21233664×10
40	4	4	$\geq 5.460, \leq 5.865$	4423680×10
48	4	4	$\geq 5.516, \leq 5.837$	237312×10
64	2	2	$\geq 5.714, \leq 5.714$	576×10
64	2	3	$\geq 5.500, \leq 5.794$	39744×10
64	2	4	$\geq \mathbf{5.270}, \leq 5.873$	4874688×10
64	3	3	$\geq 5.540, \leq 5.778$	51840×10
64	3	4	$\geq 5.341, \leq 5.873$	25455168×10

Acknowledgement. This work is a part of a project supported financially by The Scientific and Technological Research Council of Turkey (TÜBİTAK) under grant 114E486.

References

1. Biham, E., Shamir, A. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4(1), 3-72 (1991)
2. Bracken, C., Leander, G. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Finite Fields and Their Applications, 16(4), 231-242 (2010)
3. Bracken, C., Tan, C. H., Tan, Y. Binomial differentially 4 uniform permutations with high nonlinearity. Finite Fields and Their Applications, 18(3), 537-546 (2012)
4. Browning, K. A., Dillon, J. F., McQuistan, M. T., Wolfe, A. J. An APN permutation in dimension six. In: The 9th Conference on Finite Fields and Applications - Fq9, Contemporary Mathematics, 518, 33-42, AMS USA (2010)
5. Carlet, C. Vectorial Boolean functions for cryptography. Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Yves Crama and Peter L. Hammer (eds.), pp. 398-469, Cambridge University Press (2010)
6. Chakraborty, K., Sarkar, S., Maitra, S., Mazumdar, B., Mukhopadhyay, D., Prouff, E. Redefining the Transparency Order. In: Workshop on Coding and Cryptography (WCC), Paris, France (2015) (available online from `http://eprint.iacr.org/2014/367.pdf`)
7. Dobbertin, H. Almost perfect nonlinear power functions on GF(2^n): The Welch case. IEEE Transactions on Information Theory, 45(4), 1271-1275 (1999)
8. Evci, M. A., Kavut, S. DPA Resilience of rotation-symmetric S-boxes. In: IWSEC 2014, LNCS, vol. 8639, pp. 146-157, Springer International Publishing Switzerland (2014)
9. Fuller, J., Millan, W. Linear redundancy in s-boxes. In: FSE 2003, LNCS, vol. 2887, pp. 74-86, Springer Berlin Heidelberg (2003)
10. Gold, R. Maximal recursive sequences with 3-valued recursive crosscorrelation functions, IEEE Trans. Inform. Theory, 14, 154-156 (1968)
11. Kasami, T. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. Inform. Control, 18, 369-394 (1971)
12. Kavut, S., Yücel, M. D. 9-variable Boolean Functions with Nonlinearity 242 in the Generalized Rotation Symmetric Class. Information and Computation, 208(4), pp. 341-350, Elsevier (2010)
13. Kavut, S. Results on rotation-symmetric S-boxes. Information Sciences, 201, 93-113 (2012)
14. Kavut, S. DPA Resistivity of Small Size S-boxes. In: ISDFS 2015, Proceedings of the 3rd International Symposium on Digital Forensics and Security, pp. 64-69 (2015)
15. Kocher, P. C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: CRYPTO'96, LNCS, vol. 1109, pp. 104-113, Springer Berlin Heidelberg (1996)
16. Kocher, P. C., Jaffe, J., Jun, B. Differential Power Analysis. In: CRYPTO'99, LNCS, vol. 1666, pp. 388-397, Springer Berlin Heidelberg (1999)

17. Lai, X. Higher order derivatives and differential cryptanalysis. In: "Symposium on Communication, Coding and Cryptography", in honor of J. L. Massey on the occasion of his 60'th birthday, The Springer International Series in Engineering and Computer Science, vol. 276, pp. 27-233, Springer US (1994)
18. Li, Y., Wang, M., Yu, Y. Constructing Differentially 4-uniform Permutations over $GF(2^{2k})$ from the Inverse Function Revisited (2013) (available online from `http://eprint.iacr.org/2013/731`)
19. Li, Y., Wang, M. Constructing differentially 4-uniform permutations over $GF(2^{2m})$ from quadratic APN permutations over $GF(2^{2m+1})$. Des. Codes Cryptogr., 72(2), 249-264 (2014)
20. Matsui, M. Linear cryptanalysis method for DES cipher. In: EUROCRYPT'93, LNCS, vol. 765, pp. 386-397, Springer Berlin Heidelberg (1994)
21. Mazumdar, B., Mukhopadhyay, D., Sengupta, I. Constrained Search for a Class of Good Bijective S-boxes with Improved DPA Resistivity. IEEE Transactions on Information Forensics and Security, 8(12), 2154-2163 (2013)
22. Mazumdar, B., Mukhopadhyay, D., Sengupta, I. Design and Implementation of Rotation Symmetric S-boxes with High Nonlinearity and High DPA Resiliency. In: IEEE International Symposium on Hardware-Oriented Security and Trust – HOST, pp. 87-92 (2013)
23. Mazumdar, B., Mukhopadhyay, D. Construction of RSSBs with High Nonlinearity and Improved DPA Resistivity from Balanced RSBFs. IEEE Transactions on Computers, doi: 10.1109/TC.2016.2569410, (2016)
24. Nyberg, K. Differentially Uniform Mappings for Cryptography. In: EUROCRYPT'93, LNCS, vol. 765, pp. 55-64, Springer Berlin Heidelberg (1994)
25. Picek, S., Ege, B., Batina, L., Jakobovic, D., Chmielewski, Ł., Golub, M. On Using Genetic Algorithms for Intrinsic Side-channel Resistance: The Case of AES S-box. In: The First Workshop on Cryptography and Security in Computing Systems, CS2'14, pp. 13-18, ACM New York (2014)
26. Picek, S., Ege, B., Papagiannopoulos, K., Batina, L., Jakobović, D. Optimality and beyond: The case of 4×4 S-boxes. In: IEEE International Symposium on Hardware-Oriented Security and Trust – HOST, pp. 80-83 (2014)
27. Prouff, E. DPA Attack and S-boxes. In: FSE 2005, LNCS, vol. 3557, pp. 424-441, Springer Berlin Heidelberg (2005)
28. Quisquater, J.-J., Samyde, D. Electro Magnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In: Smart Card Programming and Security (E-Smart 2001), LNCS, vol. 2140, pp. 200-210, Springer Berlin Heidelberg (2001)
29. Rijmen, V., Barreto, P. S. L. M., Filho, D. L. G. Rotation Symmetry in Algebraically Generated Cryptographic Substitution Tables. Inf. Process. Lett., 106(6), 246-250 (2008)
30. Stănică, P., Maitra, S. Rotation Symmetric Boolean Functions − Count and Cryptographic Properties. Discrete Applied Mathematics, 156(10), 1567-1580 (2008)
31. Yu, Y., Wang, M., and Li, Y. Constructing differential 4-uniform permutations from know ones (2011) (available online from `http://eprint.iacr.org/2011/047`)