IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2017, No. 1, pp. 398–404. DOI:10.13154/tosc.v2017.i1.398-404

A Note on 5-bit Quadratic Permutations' Classification

Dušan Božilov[1,2], Begül Bilgin[2] and Hacı Ali Şahin[3]

[1] NXP Semiconductors, Leuven, Belgium
[2] imec - Computer Security and Industrial Cryptography (COSIC) research group, Department of Electrical Engineering (ESAT), KU Leuven, Leuven, Belgium
name.lastname@esat.kuleuven.be
[3] Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

Abstract. Classification of vectorial Boolean functions up to affine equivalence is used widely to analyze various cryptographic and implementation properties of symmetric-key algorithms. We show that there exist 75 affine equivalence classes of 5-bit quadratic permutations. Furthermore, we explore important cryptographic properties of these classes, such as linear and differential properties and degrees of their inverses, together with multiplicative complexity and existence of uniform threshold realizations.

Keywords: permutation, S-box, classification, affine equivalence, vectorial Boolean function

1 Introduction

S-boxes are the main nonlinear building blocks of many symmetric-key primitives. They must be chosen with extreme care to make the algorithm cryptographically sound while being efficient for implementation. One consideration during S-box choice is its linear and differential properties which give an idea about its resistance against linear and differential cryptanalysis [6, 18]. Another consideration is its algebraic degree which reflects resilience against higher-order differential and algebraic attacks [15]. Moreover, algebraic degree is a good indicator of the implementation cost. Low-degree permutations tend to occupy smaller area on hardware, and can be used to generate a permutation with higher algebraic degree [10]. Hence, we focus on S-boxes with the lowest algebraic degree that are bijective, namely quadratic permutations. Relevance of the 5-bit quadratic S-boxes can also be seen by their presence in several cryptographic primitives, e.g. the Keccak [3], Ketje [4], Keyak [5], Ascon [16], Fides [8] and PRIMATEs [1] algorithms.

We opt for affine equivalence classification since algebraic degree, linearity and differential uniformity are invariant within the equivalence class. However, classifying all n-bit permutations is an exponentially hard problem in n, allowing only 3- and 4-bit permutations to be classified so far [14]. Here, we provide the affine equivalence classification of all quadratic 5-bit permutations.

2 Preliminaries

We use small letters to represent elements of the finite field $\mathbb{F}_2^n$ and capital letters to represent (vectorial) Boolean functions. Subscripts are used to specify each bit of an element or each coordinate function of a vectorial Boolean function, i.e. $x = (x_1, \cdots, x_n)$, where $x_i \in \mathbb{F}_2$ and $S(x) = (S_1(x), \cdots, S_m(x))$ where S is defined from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ and S_i's are defined from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. We omit subscripts if $n = 1$ or $m = 1$. We denote absolute value, inner product, composition and addition in $\mathbb{F}_2^n$ and subtraction in $\mathbb{Z}$ with $|.|$, $\langle ., . \rangle$, $\circ$, $\oplus$ and $-$ respectively.

Received: 2016-06-01, Revised: 2016-11-23, Accepted: 2017-01-24, Published: 2017-03-08

2.1 Algebraic Properties

Every Boolean function F can be represented uniquely by its *Algebraic Normal Form* (ANF):

$$F(x) = \bigoplus_{j=(j_1,\ldots,j_n)\in\mathbb{F}_2^n} a_j x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}. \tag{1}$$

Definition 1. The $n \times 2^n$ binary matrix representing the ANF of a vectorial Boolean function $y = S(x)$ where the i^{th} row corresponds to the coordinate function y_i and the j^{th} column corresponds to the term a_j occurring in the ANF of S_i is denoted by S_{ANF}.

The *algebraic degree* of F is the largest Hamming weight of j in Eq. (1) where a_j is nonzero.

The algebraic degree of a vectorial Boolean function S is equal to the highest algebraic degree of its coordinate functions S_i.

Property 1. A vectorial Boolean function is *balanced* if and only if, for every $x \in \mathbb{F}_2^n$, each possible output $y = S(x) \in \mathbb{F}_2^m$ is equiprobable. Clearly if $m = n$, a balanced S is an n-bit permutation.

Definition 2 ([20])**.** The Moebius transformation $\mathcal{M}$ uniquely links the matrix S_{TT} corresponding to the truth table (TT) of S, where the $(i,j)^{\text{th}}$ element corresponds to y_i for input $x = j$, and S_{ANF} with the equation $S_{\text{ANF}} \times \mathcal{M} = S_{\text{TT}}$.

Values in the j^{th} column of Moebius transformation matrix $\mathcal{M}$ correspond to the terms $(1\ x_1\ x_2\ x_1x_2\ x_3\ x_1x_3\ \ldots\ x_1\cdots x_n)^T$ in ANF for input $x = j$. Also note that $\mathcal{M}^2 = I$.

An example of link between S_{ANF} and S_{TT} is provided below for permutation $S = [1\,0\,3\,6\,5\,2\,7\,4]$.

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix},$$

Permutation S is said to have *odd parity* if the number of transpositions needed to obtain S from identity permutation is odd. Otherwise, S is said to have *even parity.*

2.2 Cryptographic Properties

Definition 3. The difference distribution table (DDT) of an n-bit permutation S is a $2^n \times 2^n$ table where the $(i,j)^{\text{th}}$ entry is

$$\Gamma_S(i,j) = \#\{x \in \mathbb{F}_2^n, S(x \oplus i) = S(x) \oplus j\}. \tag{2}$$

The highest value in DDT is called its *differential uniformity*, and is denoted by δ. Uniform and small DDT entries are desirable as they translate to possible resistance against attacks that use differential characteristics. S-boxes that achieve the theoretical minimal δ of 2 are referred to as almost perfect nonlinear (APN) permutations [19].

Definition 4. The linear approximation table (LAT) of an n-bit permutation S is a $2^n \times 2^n$ matrix where the $(i,j)^{\text{th}}$ entry is

$$\Lambda_S(i,j) = |\#\{x \in \mathbb{F}_2^n, \langle i,x\rangle = \langle j, S(x)\rangle\} - 2^{n-1}|. \tag{3}$$

The highest value in LAT is denoted by λ. The smaller the value of λ, the higher the resistance against linear cryptanalysis. If $\lambda = 2^{(n-1)/2}$, S is called an almost bent (AB) permutation [12].

2.3 Affine Equivalence Relation

Definition 5. Two permutations S and S' are affine equivalent if and only if there exist affine output and input permutations A and B respectively satisfying $S' = A \circ S \circ B$. Permutations that are affine equivalent form an equivalence class.

Given S, a unique representative defining the affine equivalence class that S belongs to can be efficiently computed with an average $O(2^{3n})$ worst-case complexity using the algorithm provided in [14] which we refer to as *GetRepr*(S). Here, we use the lexicographically smallest permutation within the class with respect to the table look-up description as the representative of that class.

Lemma 1 ([17])**.** *Let S be an n-bit permutation. Then S is affine equivalent to another permutation S' with $S'(x) = x$, for $x \in \{0, 1, 2, 4, 8, ..., 2^{n-1}\}$.*

2.4 Implementation Aspects

The first implementation criteria we consider, namely multiplicative complexity (MC) is defined to be the minimum number of AND gates required to implement a (set of) function(s) by using only 2-input AND and XOR gates, and NOT gate. It can be used as a rough estimate for implementation size, resistance to algebraic attacks [13] and implementation costs of Boolean masking based side-channel countermeasures.

A more specific implementation metric is efficiency of threshold implementation (TI), which is a side-channel analysis countermeasure. The efficiency of TI depends not only on the MC and the number of gates of a permutation, but also on the amount of fresh randomness that is required.

This amount is defined by the (non-)satisfaction of the uniformity condition of TI which is a hard problem.

For more in-depth analysis of TI and its properties such as uniformity, we refer to [7].

3 Classification of Quadratic Permutations

Let us denote the set of S (resp. S_{ANF}) satisfying certain criteria as $\mathbf{S}$ (resp. $\mathbf{S}_{\text{ANF}}$) and the set of affine equivalent class representatives as $\mathbf{C}$. A naive algorithm to classify all S is as follows:

```
Data: $\mathbf{S}$ and $\mathbf{C} = \emptyset$
Result: $\mathbf{C}$
for all $S \in \mathbf{S}$ do
    $c = GetRepr(S)$
    if $c \notin \mathbf{C}$ then
        $\mathbf{C} = \mathbf{C} \cup c$
    end
end
```

In this section, we briefly describe the criteria on S_{ANF} that increase efficiency.

Step 1. Since we focus on 5-bit quadratic permutations, we fix the columns in S_{ANF} corresponding to affine constant and degree greater than two terms to 0. That is, we only vary the terms in columns corresponding x_1, x_2, x_1x_2, x_3, x_1x_3, x_2x_3, x_4, x_1x_4, x_2x_4, x_3x_4, x_5, x_1x_5, x_2x_5, x_3x_5, x_4x_5 in S_{ANF} giving $|\mathbf{S}_{\text{ANF}}| = 2^{5\times15}$. Hereon, we ignore the all-zero columns for ease of notation.

Step 2. By Lemma 1, we can fix the columns corresponding to x_1, x_2, x_3, x_4 and x_5 of S_{ANF} with $(1, 0, 0, 0, 0)^T$, $(0, 1, 0, 0, 0)^T$, $(0, 0, 1, 0, 0)^T$, $(0, 0, 0, 1, 0)^T$ and $(0, 0, 0, 0, 1)^T$ respectively as described in Eqn. (4). This reduces the number of possible S_{ANF} matrices to $2^{5\times10}$.

$$S_{\text{ANF}} = \begin{pmatrix} 1 & 0 & c_{1,1} & 0 & c_{1,2} & c_{1,3} & 0 & c_{1,4} & c_{1,5} & c_{1,6} & 0 & c_{1,7} & c_{1,8} & c_{1,9} & c_{1,10} \\ 0 & 1 & c_{2,1} & 0 & c_{2,2} & c_{2,3} & 0 & c_{2,4} & c_{2,5} & c_{2,6} & 0 & c_{2,7} & c_{2,8} & c_{2,9} & c_{2,10} \\ 0 & 0 & c_{3,1} & 1 & c_{3,2} & c_{3,3} & 0 & c_{3,4} & c_{3,5} & c_{3,6} & 0 & c_{3,7} & c_{3,8} & c_{3,9} & c_{3,10} \\ 0 & 0 & c_{4,1} & 0 & c_{4,2} & c_{4,3} & 1 & c_{4,4} & c_{4,5} & c_{4,6} & 0 & c_{4,7} & c_{4,8} & c_{4,9} & c_{4,10} \\ 0 & 0 & c_{5,1} & 0 & c_{5,2} & c_{5,3} & 0 & c_{5,4} & c_{5,5} & c_{5,6} & 1 & c_{5,7} & c_{5,8} & c_{5,9} & c_{5,10} \end{pmatrix} \tag{4}$$

Step 3. In order to describe the next optimization, we refer to the following Lemma from [2].

Lemma 2. *There exist only two quadratic 5-bit Boolean functions up to extended affine equivalence, namely* $x_1x_2 \oplus \bigoplus_i a_ix_i$ *and* $x_1x_2 \oplus x_3x_4 \oplus \bigoplus_i a_ix_i$.

Lemma 2 implies that for one of the rows of S_{ANF}, we can reduce the complexity even further. Namely, it can have at most two quadratic terms such that the indices of these quadratic terms are different leaving only 25 options. Note that due to the optimization performed in Step 2, the search space cannot be limited to the two quadratic and one linear representative alone or extended to more than one row. We apply this optimization on the first row without loss of generality.

Step 4. By Property 1, each row should represent a balanced Boolean function. A precomputation shows that for each of the last four rows, only 472 out of 2^{10} possibilities and for the first row 10 out of 26 (one linear and 25 quadratic) possibilities are balanced.

We conclude our optimization by iterating the balancedness condition to the whole S_{ANF} matrix one row at a time, i.e. by adding output component functions one by one. Specifically, we get 10, 2610, 220942, 3941730 and 10374528 balanced cases for 1 to 5 bits, respectively.

Calculating the affine representative has an average complexity 2^{15} [14] giving the complexity estimate of 2^{39} to find all 5-bit quadratic permutations.

We represented each row of S_{ANF} and S_{TT} and each column of $\mathcal{M}$ as an integer, and ran the optimized algorithm on a machine running Linux with Intel XEON E5 processor with 16 logical cores. Execution was parallelized using 16 threads where all 10374528 permutations were split in 16 parts and processed by each thread separately. The program finished within three hours.

We enumerate all 75 quadratic classes our program produced lexicographically. Inverses of the permutations belonging to 18 of these classes provided in Table 1 are quadratic and in the same affine equivalence class respectively. The remaining 57 classes given in Table 2 have inverses with algebraic degree three. Further details on cryptographic properties and implementation aspects are also provided in these tables.

Table 1: List of all quadratic 5-bit affine equivalence class representatives with quadratic inverses

Cl. #	Representative	δ	λ	MC	TI
1	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,25,24,27,26,29,28,31,30	32	16	1	yes
2	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,21,20,23,22,26,27,24,25,31,30,29,28	32	16	2	yes
3	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,21,20,23,22,28,29,30,31,25,24,27,26	32	16	2	yes
4	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,24,25,26,27,28,29,30,31,20,21,22,23	32	16	2	yes
5	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,19,18,22,23,21,20,28,29,31,30,26,27,25,24	32	16	3	yes
6	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,19,18,24,25,27,26,28,29,31,30,20,21,23,22	32	16	3	yes
7	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,20,21,24,25,28,29,22,23,18,19,30,31,26,27	32	16	3	yes
8	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,19,17,24,26,27,25,28,30,31,29,20,22,23,21	16	16	4	yes
9	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,19,17,24,26,27,25,29,31,30,28,21,23,22,20	16	16	4	yes
10	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,20,22,24,26,28,30,19,17,23,21,27,25,31,29	16	16	4	yes
11	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,20,22,24,26,28,30,31,29,27,25,23,21,19,17	16	16	4	yes
12	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,18,19,22,23,20,21,28,29,30,31,27,26,25,24	32	16	3	yes
13	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,18,19,24,25,26,27,28,29,30,31,21,20,23,22	32	16	3	yes
14	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,19,18,20,21,23,22,24,25,27,26,29,28,30,31	32	16	2	yes
15	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,19,18,20,21,23,22,26,27,25,24,31,30,28,29	32	16	3	yes
16	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,19,18,22,23,21,20,28,29,31,30,27,26,24,25	32	16	4	yes
17	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,19,18,24,25,27,26,28,29,31,30,21,20,22,23	32	16	4	yes
30	0,1,2,3,4,5,6,7,8,9,10,11,16,17,18,19,12,13,14,15,24,25,26,27,28,29,30,31,20,21,22,23	32	16	3	unk.

Table 2: List of all quadratic 5-bit affine equivalence class representatives with cubic inverses

Cls. #	Representative	δ	λ	MC	TI
18	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,20,21,18,19,22,23,24,25,28,29,27,26,31,30	32	16	2	yes
19	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,20,21,18,19,22,23,26,27,30,31,25,24,29,28	32	16	3	yes
20	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,20,21,22,23,18,19,24,25,28,29,31,30,27,26	32	16	3	yes
21	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,20,21,24,25,28,29,18,19,22,23,27,26,31,30	32	16	3	yes
22	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,20,21,24,25,28,29,22,23,18,19,31,30,27,26	32	16	4	yes
23	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,17,20,21,24,25,28,29,30,31,26,27,23,22,19,18	32	16	3	yes
24	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,18,17,19,24,26,25,27,28,30,29,31,21,23,20,22	32	16	4	yes
25	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,18,19,17,20,22,23,21,24,26,27,25,29,31,30,28	16	16	3	yes
26	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,18,19,17,20,22,23,21,28,30,31,29,25,27,26,24	16	16	4	yes
27	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,18,19,17,24,26,27,25,28,30,31,29,21,23,22,20	16	16	5	yes
28	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,20,17,21,18,22,19,23,24,28,25,29,27,31,26,30	16	16	3	unk.
29	0,1,2,3,4,5,6,7,8,9,10,11,13,12,15,14,16,20,17,21,24,28,25,29,18,22,19,23,27,31,26,30	16	16	4	unk.
31	0,1,2,3,4,5,6,7,8,9,10,11,16,17,18,19,12,13,15,14,22,23,21,20,28,29,31,30,26,27,25,24	32	16	4	yes
32	0,1,2,3,4,5,6,7,8,9,10,11,16,17,18,19,12,13,15,14,24,25,27,26,28,29,31,30,20,21,23,22	32	16	4	unk.
33	0,1,2,3,4,5,6,7,8,9,10,11,16,17,18,19,12,14,15,13,20,22,23,21,24,26,27,25,28,30,31,29	16	16	3	yes
34	0,1,2,3,4,5,6,7,8,9,10,11,16,17,18,19,12,14,15,13,20,22,23,21,28,30,31,29,24,26,27,25	16	16	4	yes
35	0,1,2,3,4,5,6,7,8,9,10,11,16,17,18,19,12,14,15,13,24,26,27,25,28,30,31,29,20,22,23,21	16	8	5	unk.
36	0,1,2,3,4,5,6,7,8,9,10,11,16,17,18,19,12,14,15,13,24,26,27,25,29,31,30,28,21,23,22,20	16	8	5	unk.
37	0,1,2,3,4,5,6,7,8,9,11,10,14,15,13,12,16,18,20,22,17,19,21,23,24,26,29,31,27,25,30,28	16	16	4	unk.
38	0,1,2,3,4,5,6,7,8,9,11,10,14,15,13,12,16,18,20,22,19,17,23,21,24,26,29,31,25,27,28,30	16	16	4	unk.
39	0,1,2,3,4,5,6,7,8,9,11,10,14,15,13,12,16,18,22,20,19,17,21,23,24,26,31,29,25,27,30,28	16	16	4	unk.
40	0,1,2,3,4,5,6,7,8,9,11,10,14,15,13,12,16,18,24,26,17,19,25,27,20,22,29,31,23,21,30,28	16	16	5	unk.
41	0,1,2,3,4,5,6,7,8,9,11,10,14,15,13,12,16,20,18,22,19,23,17,21,24,28,27,31,25,29,26,30	16	16	3	unk.
42	0,1,2,3,4,5,6,7,8,9,11,10,14,15,13,12,16,20,22,18,23,19,17,21,24,28,31,27,29,25,26,30	16	16	4	unk.
43	0,1,2,3,4,5,6,7,8,9,11,10,14,15,13,12,16,24,18,26,19,27,17,25,20,28,23,31,21,29,22,30	16	16	4	unk.
44	0,1,2,3,4,5,6,7,8,9,12,13,14,15,10,11,16,24,18,26,28,20,30,22,17,25,21,29,31,23,27,19	16	16	4	unk.
45	0,1,2,3,4,5,6,7,8,10,12,14,11,9,15,13,16,20,19,23,22,18,21,17,24,31,29,26,25,30,28,27	8	16	5	unk.
46	0,1,2,3,4,5,7,6,8,9,12,13,14,15,11,10,16,18,24,26,20,22,29,31,21,23,27,25,19,17,28,30	16	16	5	unk.
47	0,1,2,3,4,5,7,6,8,9,12,13,14,15,11,10,16,18,24,26,22,20,31,29,21,23,27,25,17,19,30,28	16	16	5	unk.
48	0,1,2,3,4,5,7,6,8,9,12,13,14,15,11,10,16,18,24,26,22,20,31,29,23,21,25,27,19,17,28,30	16	16	5	unk.
49	0,1,2,3,4,5,7,6,8,9,12,13,14,15,11,10,16,18,26,24,22,20,29,31,21,23,25,27,17,19,28,30	16	16	5	unk.
50	0,1,2,3,4,5,7,6,8,9,12,13,14,15,11,10,16,24,18,26,20,28,23,31,21,29,17,25,19,27,22,30	16	16	4	unk.
51	0,1,2,3,4,5,7,6,8,9,12,13,14,15,11,10,16,24,26,18,28,20,23,31,21,29,25,17,27,19,22,30	16	16	4	unk.
52	0,1,2,3,4,5,7,6,8,9,12,13,14,15,11,10,16,24,26,18,28,20,23,31,29,21,17,25,19,27,30,22	16	16	5	unk.
53	0,1,2,3,4,5,7,6,8,10,12,14,16,18,21,23,9,13,11,15,24,28,27,31,25,30,29,26,20,19,17,22	8	8	5	unk.
54	0,1,2,3,4,5,7,6,8,16,10,18,12,20,15,23,9,24,11,26,13,28,14,31,25,17,27,19,29,21,30,22	16	16	4	unk.
55	0,1,2,3,4,5,7,6,8,16,10,18,12,20,15,23,9,24,11,26,14,31,13,28,25,17,27,19,30,22,29,21	16	16	5	unk.
56	0,1,2,3,4,5,7,6,8,16,10,18,12,20,15,23,9,24,13,28,14,31,11,26,17,25,21,29,22,30,19,27	16	8	5	unk.
57	0,1,2,3,4,5,7,6,8,16,10,18,12,20,15,23,9,24,13,28,14,31,11,26,25,17,29,21,30,22,27,19	8	8	6	unk.
58	0,1,2,3,4,5,7,6,8,16,10,18,12,20,15,23,9,26,13,30,11,24,14,29,17,27,21,31,19,25,22,28	16	8	5	unk.
59	0,1,2,3,4,5,7,6,8,16,10,18,12,20,15,23,9,26,13,30,14,29,11,24,17,27,21,31,22,28,19,25	8	8	5	unk.
60	0,1,2,3,4,5,8,9,6,7,12,13,14,15,10,11,16,19,17,18,20,23,27,24,21,22,28,31,29,30,26,25	16	16	5	unk.
61	0,1,2,3,4,5,8,9,6,10,11,7,16,28,19,31,12,14,15,13,20,22,25,27,18,29,30,17,24,23,26,21	8	8	6	unk.
62	0,1,2,3,4,5,8,9,6,10,11,7,16,28,19,31,12,14,15,13,20,22,25,27,29,18,17,30,23,24,21,26	8	8	6	unk.
63	0,1,2,3,4,5,8,9,6,10,11,7,16,28,19,31,12,14,15,13,21,23,24,26,18,29,30,17,25,22,27,20	8	8	6	unk.
64	0,1,2,3,4,5,8,9,6,10,11,7,16,28,19,31,12,14,15,13,21,23,24,26,29,18,17,30,22,25,20,27	8	8	6	unk.
65	0,1,2,3,4,5,8,9,6,10,16,28,7,11,31,19,12,14,20,22,13,15,27,25,17,30,29,18,21,26,23,24	8	8	6	unk.
66	0,1,2,3,4,5,8,9,6,10,16,28,7,11,31,19,12,14,20,22,15,13,25,27,17,30,29,18,23,24,21,26	8	8	6	unk.
67	0,1,2,3,4,5,8,9,6,10,16,28,7,11,31,19,12,14,21,23,15,13,24,26,20,27,25,22,18,29,17,30	8	8	6	unk.
68	0,1,2,3,4,5,8,9,6,16,10,28,13,27,15,25,7,20,12,31,11,24,14,29,18,22,23,19,17,21,26,30	8	8	5	unk.
69	0,1,2,3,4,5,8,9,6,16,10,28,13,27,15,25,7,31,12,20,14,22,11,19,23,24,18,29,17,30,26,21	8	8	6	unk.
70	0,1,2,3,4,5,8,9,6,16,10,28,15,25,13,27,7,20,14,29,12,31,11,24,21,17,18,22,19,23,26,30	8	8	5	unk.
71	0,1,2,3,4,6,8,10,5,12,16,25,7,13,28,22,9,15,17,23,11,14,29,24,26,20,21,27,30,19,31,18	4	8	6	unk.
72	0,1,2,3,4,6,8,10,5,12,16,25,7,13,28,22,9,15,24,30,11,14,20,17,27,21,29,19,31,18,23,26	4	8	5	unk.
73	0,1,2,3,4,6,8,10,5,12,16,25,13,7,22,28,9,14,19,20,15,11,27,31,24,23,21,26,18,30,17,29	4	8	6	unk.
74	0,1,2,4,3,8,16,28,5,10,25,17,18,23,31,29,6,20,13,24,19,11,9,22,27,7,14,21,26,12,30,15	2	4	8	unk.
75	0,1,2,4,3,8,16,28,5,10,26,18,17,20,31,29,6,21,24,12,22,15,25,7,14,19,13,23,9,30,27,11	2	4	7	unk.

4 Interpretation of Results

Parity. Only four classes have odd parity, namely 53, 71, 72 and 74. This can be used when decomposing a higher-degree permutation S into t quadratic permutations S^i where $S = S^1 \circ \cdots \circ S^t$.

Relation with Important Permutations. As shown in Tables 1 and 2, we confirm results given by Brinkmann and Leander [11] about existence of two quadratic, namely classes 74 and 75, and two cubic (as their inverse) almost bent (AB) permutations. An element from class 74 has already been used as the S-box of Fides and PRIMATEs authenticated encryption algorithms. The nonlinear transformations of Keccak, Ketje, Keyak and Ascon algorithms are members of class 68. Note that there exist 12 other cryptographically equally good classes ($\delta = 8$, $\lambda = 8$); some of which have elements with similar multiplicative complexity. There exist 3 other non-AB classes with better differential properties compared to class 68 ($\delta = 4$, $\lambda = 8$). Finally, we note that 5-bit classes 2, 4, 5, 8, 14 and 31 are extensions of the 4-bit quadratic classes Q_4, Q_{294}, Q_{12}, Q_{299}, Q_{293} and Q_{300} defined in [9] respectively. That is, given a 4-bit permutation $S(x_1, x_2, x_3, x_4) = (y_1, y_2, y_3, y_4)$, its 5-bit extension is generated by $S(x_1, x_2, x_3, x_4, x_5) = (y_1, y_2, y_3, y_4, x_5)$.

Implementation. By using the toolbox from [21], we analyzed MC for all the class representatives. The values given in Table 1 and Table 2 represent the minimum MC for which the tool produced a definitive result within an hour, not always guaranteeing minimal solution. For example, it has been shown in [21] that the PRIMATEs S-box from class 74 has MC 7. Therefore, we conclude that all 5-bit quadratic permutations can be implemented using at most 7 2-input AND gates.

Threshold implementations. We could find a 3-share uniform TI of at least one permutation for 30 of these classes (classes 1-27, 31, 33 and 34) using the sharing with correction terms described in Equation (3.17) of [7]. Moreover, each 5-bit quadratic permutation class has at least one S-box that has a uniform 4-share TI using the sharing in Appendix B.2.5 of [7].

Acknowledgments

The authors would like to thank the anonymous reviewers for providing constructive and valuable comments. Moreover, we thank V. Rijmen, V. Nikov and S. Nikova for useful discussions. This work was partially supported by NIST with the research grant 60NANB15D346, by the Flemish Government through FWO project Cryptography secured against side-channel attacks by tailored implementations enabled by future technologies (G0842.13) and by the Research Council KU Leuven (OT/13/071). Dušan Božilov is funded from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 643161. Begül Bilgin is a Postdoctoral Fellow of the Fund for Scientific Research - Flanders (FWO).

References

[1] Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Florian Mendel, Bart Mennink, Nicky Mouha, Qingju Wang, and Kan Yasuda. CAESAR submission: PRIMATEs v1.02, March 2014. http://primates.ae/wp-content/uploads/primatesv1.02.pdf.

[2] Elwyn Berlekamp and Lloyd Welch. Weight distributions of the cosets of the (32,6) Reed-Muller code. *IEEE Transactions on Information Theory*, 18(1):203–207, Jan 1972.

[3] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The Keccak reference, January 2011. http://keccak.noekeon.org/.

[4] Guido Bertoni, Joan Daemon, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. CAESAR submission: Ketje v1, March 2014. https://competitions.cr.yp.to/round1/ketjev1.pdf.

[5] Guido Bertoni, Joan Daemon, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. CAESAR submission: Keyak v2, August 2015. https://competitions.cr.yp.to/round2/keyakv2.pdf.

[6] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In *International Cryptology Conference on Advances in Cryptology*, CRYPTO 1990, pages 2–21, London, UK, UK, 1991. Springer-Verlag.

[7] Begül Bilgin. *Threshold Implementations : As Countermeasure Against Higher-Order Differential Power Analysis*. PhD thesis, May 2015.

[8] Begül Bilgin, Andrey Bogdanov, Miroslav Knezevic, Florian Mendel, and Qingju Wang. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware. In *Cryptographic Hardware and Embedded Systems, CHES 2013*, volume 8086 of *LNCS*, pages 142–158, Heidelberg, Germany, 2013. Springer.

[9] Begül Bilgin, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen, Natalia Tokareva, and Valeriya Vitkup. Threshold implementations of small s-boxes. *Cryptography and Communications*, 7(1):3–33, 2015.

[10] Erik Boss, Vincent Grosso, Tim Güneysu, Gregor Leander, Amir Moradi, and Tobias Schneider. Strong 8-bit sboxes with efficient masking in hardware. In *Cryptographic Hardware and Embedded Systems – CHES 2016*, pages 171–193, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[11] Marcus Brinkmann and Gregor Leander. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography*, 49(1):273–288, 2008.

[12] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In *Advances in Cryptology — EUROCRYPT 1994*, pages 356–365, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[13] Nicolas Courtois, Daniel Hulme, and Theodosis Mourouzis. Multiplicative complexity and solving generalized brent equations with SAT solvers. In *The Third International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking*, pages 22–27, 2012.

[14] Christophe De Cannière. *Analysis and Design of Symmetric Encryption Algorithms.* PhD thesis, 2007.

[15] Christoph Dobraunig, Maria Eichlseder, and Florian Mendel. Higher-order cryptanalysis of LowMC. In *Information Security and Cryptology - ICISC 2015*, LNCS, pages 87–101. Springer, 2015.

[16] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. CAESAR submission: ASCON v1.1, August 2015. https://competitions.cr.yp.to/round2/asconv11.pdf.

[17] Gregor Leander and Axel Poschmann. On the classification of 4 bit s-boxes. In *Arithmetic of Finite Fields: First International Workshop, WAIFI 2007*, pages 159–176, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[18] Mitsuru Matsui and Atsuhiro Yamagishi. A new method for known plaintext attack of FEAL cipher. In *Advances in Cryptology — EUROCRYPT 1992*, pages 81–91, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

[19] Kaisa Nyberg and Lars Ramkilde Knudsen. Provable security against a differential attack. *Journal of Cryptology*, 8(1):27–37, 1995.

[20] Josef Pieprzyk and Xian-Mo Zhang. Computing Möbius transforms of boolean functions and characterizing coincident boolean functions. In *The conference BFCA 2007, Publications des Universités de Rouen et du Havre*, 2007.

[21] Ko Stoffelen. Optimizing s-box implementations for several criteria using SAT solvers. In *Fast Software Encryption: FSE 2016*, pages 140–160, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.