A Note on 5-bit Quadratic Permutations’ Classification

Dušan Božilov\textsuperscript{1,2}, Begül Bilgin\textsuperscript{2} and Hacı Ali Şahin\textsuperscript{3}

\textsuperscript{1} NXP Semiconductors, Leuven, Belgium
\textsuperscript{2} imec-COSIC, ESAT, KU Leuven, Leuven, Belgium \texttt{name.lastname@esat.kuleuven.be}
\textsuperscript{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 \(\ominus\) respectively.
2.1 Algebraic Properties

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

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

**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 $S_{\text{ANF}}$.

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 $y = S(x) \in \mathbb{F}_2^n$ 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 $S_{\text{TT}}$ corresponding to the truth table (TT) of $S$, where the $(i,j)$th element corresponds to $y_i$ for input $x = j$, and $S_{\text{ANF}}$ 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 $(1 \ x_1 \ x_2 \ x_1 x_2 \ x_3 \ x_1 x_3 \ \ldots \ x_1 \cdots x_n)^T$ in ANF for input $x = j$. Also note that $\mathcal{M}^2 = I$.

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

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

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 $(i,j)$th entry is

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

The highest value in DDT is called its differential uniformity, and is denoted by $\delta$. 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 $\delta$ 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 $(i,j)$th entry is

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

The highest value in LAT is denoted by $\lambda$. The smaller the value of $\lambda$, 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 $\text{GetRepr}(S)$. 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 $x \in \{0, 1, 2, 4, 8, \ldots, 2^{n-1}\}$.

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

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

In this section, we briefly describe the criteria on $S_{\text{Anf}}$ that increase efficiency.

Step 1. Since we focus on 5-bit quadratic permutations, we fix the columns in $S_{\text{Anf}}$ 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 $S_{\text{Anf}}$ giving $|S_{\text{Anf}}| = 2^{5 \times 15}$. 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 $S_{\text{Anf}}$ 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 $S_{\text{ANF}}$ matrices to $2^{5 \times 10}$.

\[
S_{\text{ANF}} = \begin{pmatrix}
1 & 0 & c_{1,1} & 0 & c_{1,2} & c_{1,3} & c_{1,4} & c_{1,5} & c_{1,6} & 0 & c_{1,7} & c_{1,8} & c_{1,9} & c_{1,10} \\
0 & 1 & c_{2,1} & 0 & c_{2,2} & c_{2,3} & c_{2,4} & c_{2,5} & c_{2,6} & 0 & c_{2,7} & c_{2,8} & c_{2,9} & c_{2,10} \\
0 & 0 & c_{3,1} & 1 & c_{3,2} & c_{3,3} & c_{3,4} & c_{3,5} & c_{3,6} & 0 & c_{3,7} & c_{3,8} & c_{3,9} & c_{3,10} \\
0 & 0 & c_{4,1} & 0 & c_{4,2} & c_{4,3} & c_{4,4} & c_{4,5} & c_{4,6} & 0 & c_{4,7} & c_{4,8} & c_{4,9} & c_{4,10} \\
0 & 0 & c_{5,1} & 0 & c_{5,2} & c_{5,3} & 0 & c_{5,4} & c_{5,5} & c_{5,6} & 1 & c_{5,7} & c_{5,8} & c_{5,9} & c_{5,10}
\end{pmatrix}
\] (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 $x_1x_2 \oplus \bigoplus_i a_i x_i$ and $x_1x_2 \oplus x_3x_4 \oplus \bigoplus_i a_i x_i$.

Lemma 2 implies that for one of the rows of $S_{\text{ANF}}$, 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 $S_{\text{ANF}}$ 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 $2^{10}$ to find all 5-bit quadratic permutations.

We represented each row of $S_{\text{ANF}}$ and $S_{TT}$ and each column of $M$ 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>
<thead>
<tr>
<th>CL. #</th>
<th>Representative</th>
<th>$\delta$</th>
<th>$\lambda$</th>
<th>MC</th>
<th>TI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32</td>
<td>32</td>
<td>16</td>
<td>1</td>
<td>yes</td>
</tr>
<tr>
<td>2</td>
<td>0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32</td>
<td>32</td>
<td>16</td>
<td>2</td>
<td>yes</td>
</tr>
<tr>
<td>3</td>
<td>0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32</td>
<td>32</td>
<td>16</td>
<td>3</td>
<td>yes</td>
</tr>
<tr>
<td>4</td>
<td>0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32</td>
<td>32</td>
<td>16</td>
<td>4</td>
<td>yes</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Table 1: List of all quadratic 5-bit affine equivalence class representatives with quadratic inverses
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 \(Q_1, Q_{294}, Q_{12}, Q_{299}, Q_{293}\) 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**


A Note on 5-bit Quadratic Permutations’ Classification


