A FAMILY OF 6-TO-4-BIT S-BOXES WITH LARGE LINEAR BRANCH NUMBER

DANIEL LOEBENBERGER AND MICHAEL NÜSKEN

2 April 2013

Abstract. We propose a family of 6-to-4-bit S-boxes with linear branch number 3. Since they also fulfill various further desirable properties such S-boxes can serve as a building block for various block ciphers.

Keywords. DES, S-box, branch number

1. Introduction

During all the time of analysis and improvement proposals to DES it seemed like there might be no 6-to-4-bit S-box with linear branch number 3. While almost all S-boxes used so far have differential branch number 2 and only fail at differentials with zero output differences to achieve even differential branch number 3, they only have linear branch number 2. Since Matsui (1994) discovered linear cryptanalysis, several teams have tried to describe a set of properties that makes DES invulnerable to differential and linear cryptanalysis. Kim, Lee, Park & Lee (1994, 1995) use some conditions asking several specific 1-to-1-bit biases to be zero. In contrast, linear branch number 3 (or higher) means that all 1-to-1-bit biases are zero. Neither the DES S-boxes nor later replacements like the s²DES S-boxes found in Kim et al. (1994, 1995) have linear branch number 3. DESL, the lightweight variant of DES proposed by Leander, Paar, Poschmann & Schramm (2007), employs a single S-box in place of the eight different ones in DES. Also the DESL S-box has linear branch number 2 only.

Here, we propose the S-box $U$:

<table>
<thead>
<tr>
<th>$efgh$</th>
<th>0 1 2 3 4 5 6 7 8 9 A B C D E F</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U(0efgh0)$</td>
<td>0 9 7 2 B E C 5 3 F D 8 4 1 A 6</td>
</tr>
<tr>
<td>$U(0efgh1)$</td>
<td>B 6 8 F 2 1 5 C D A E 3 7 4 0 9</td>
</tr>
<tr>
<td>$U(1efgh0)$</td>
<td>E 4 8 D 2 7 1 B 5 A 6 3 9 C F 0</td>
</tr>
<tr>
<td>$U(1efgh1)$</td>
<td>1 D 4 2 F 8 A 7 6 0 9 5 C B 3 E</td>
</tr>
</tbody>
</table>

Note that we represent four bit strings $efgh$ as hexadecimal digits as usual.

It does have linear branch number 3 and enjoys the properties summarized in Figure 1.1, that ensure good resistance against differential and linear cryptanalysis. Actually, we started scanning for an S-box with the legendary conditions given by Coppersmith (1994) and augmented them with conditions from Leander et al. (2007).
S-7 \( \text{diff}_S(\Delta x \to \Delta y) \leq \frac{16}{64} \) for \( \Delta x \neq 0 \).
S-3 \( \text{diff}_S(0\cdots0 \to 0000) = 0 \).
Q1' \( \text{diff}_S(0\cdots0 \to 0000) = 0 \).
S-4 \( \text{diff}_S(\overline{wt_1} \to \overline{wt_1}) = 0 \).
S-5 \( \text{diff}_S(001100 \to \overline{wt_1}) = 0 \).
Q2 \( |\text{bias}_S(a,b)| \leq \frac{16}{64} \) for \( a \neq 0 \).
Q3 \( |\text{bias}_S(\overline{wt_1}, \overline{wt_1})| = 0 \).
Q4 \( |\text{bias}_S(\overline{wt_k}, \overline{wt_1})| \leq \frac{16}{64} \) when \( 0 < k + \ell \leq 4 \).

Figure 1.1: Summary of conditions for 6-to-4-bit S-boxes.
The properties S-? are from Coppersmith (1994), the properties Q?+ are stronger forms of the conditions in Leander et al. (2007). The property Q1' is equivalent to Leander et al.'s Condition 1 under S-3.

For instance, we used Condition 5 from Leander et al. (2007):

\[
Q5 \ |\text{bias}_S(a,b_1) \cdot \text{bias}_S(a,b_2)| \leq \frac{240}{64^2} \quad \text{for all } a \in \mathbb{F}_2^6, b_1, b_2 \in \mathbb{F}_2^4 \text{ with } \text{wt}(b_1 + b_2) = 1.\]

Our program, however, also reported S-boxes that violate this particular condition. Among those we found the S-box \( U \). It only has \( |\text{bias}_S(a,b_1) \cdot \text{bias}_S(a,b_2)| \leq \frac{384}{64^2} \) for all \( a \in \mathbb{F}_2^6, b_1, b_2 \in \mathbb{F}_2^4 \) with \( \text{wt}(b_1 + b_2) = 1.\)

It turns out that this new S-box has good differential and linear properties, including linear branch number 3 implied by Q3+. To our knowledge this is the first known 6-to-4-bit S-box with these properties.

Finally, note that all these properties are invariant under many transformations of S-boxes. Thus we are actually talking about a family of \( 2^66! \cdot 2^44! \) S-boxes when looking at the high level conditions listed in Section 2 or of a smaller family of \( 2^62^1 \cdot 2^44! \) S-boxes when considering all properties from Figure 1.1.

In the following, we consider properties of the proposed family of S-boxes in the spirit of Saarinen (2012). That work continues many other investigations including Biryukov, De Cannière, Braeken & Prouneel (2003); Courtois & Bard (2007); Daemen & Rijmen (2002); Kim et al. (1994, 1995); Leander et al. (2007). In this text, we do not treat properties like most of the DES design properties in Coppersmith (1994), the conditions in Leander et al. (2007), or the ones listed in Figure 1.1 any further.

2. S-box properties

To formulate all conditions we fix the following standard notions. Let \( k, \ell \in \mathbb{N}_{>0} \) and consider a candidate \( k \)-to-\( \ell \)-bit S-box

\[
S : \mathbb{F}_2^k \to \mathbb{F}_2^\ell.
\]

\(^1\)For the considerations in Leander et al. (2007) this weakened condition would have still been sufficient for their reasonings. The issue of so far mostly omitted cases involving neighboring active S-boxes is treated by us in a future paper.
2.1. Differential cryptanalysis. For differential cryptanalysis the following notion is central.

**Definition 2.1** (Differential probabilities). Given an input difference \( \Delta x \in \mathbb{F}_2^k \) and an output difference \( \Delta y \in \mathbb{F}_2^\ell \) we define

\[
\text{diff}_S(\Delta x \rightarrow \Delta y) = \text{prob}\left(S(X) \oplus S(X \oplus \Delta x) = \Delta y \Big| X \in \mathbb{F}_2^k\right) = \frac{1}{2^k} \# \{ x \in \mathbb{F}_2^k \mid S(x) \oplus S(x \oplus \Delta x) = \Delta y \}
\]

Here, \( X \) denotes a uniform random variable with values \( \mathbb{F}_2^k \).

This definition matches Definition 1 in Saarinen (2012).

2.2. Linear cryptanalysis. For linear cryptanalysis the bias of a linear expression in inputs and outputs is essential: We write \( \langle a | x \rangle = \bigoplus_i a_i x_i \) for applying a linear form \( a \in \mathbb{F}_2^{k'} \) to a vector \( x \in \mathbb{F}_2^k \). Actually this way, we identify the dual space \( \mathbb{F}_2^{k'} := \{ \mathbb{F}_2^k \to \mathbb{F}_2 \} \) with \( \mathbb{F}_2^k \), matching the bilinear form \( \langle \cdot | \cdot \rangle \). As it turns out to be important not to mix vectors and dual vectors, we keep the notation, at least as a reminder.

**Definition 2.2.** Given linear forms \( a \in \mathbb{F}_2^{k'} \) and \( b \in \mathbb{F}_2^{\ell'} \) we define the bias

\[
\text{bias}_S(a, b) = \text{prob}\left(\langle a | X \rangle = \langle b | S(X) \rangle\right) - \text{prob}\left(\langle a | X \rangle \neq \langle b | S(X) \rangle\right) = 2 \text{prob}\left(\langle a | X \rangle = \langle b | S(X) \rangle\right) - 1 = \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^k} (-1)^{\langle a | x \rangle} (-1)^{\langle b | S(x) \rangle} \in [-1, 1],
\]

which is the correlation between the chosen linear forms on input and output of \( S \).

The value used in Definition 2 in Saarinen (2012) equals \( \frac{1}{2} |\text{bias}_S(\beta_i, \beta_o)| \). We prefer our definition — also found in Daemen & Rijmen (2002), for example — since it makes Matsui’s piling-up lemma much nicer and also equals the correlation of the selected input and output bits.

2.3. Algebraic attacks. For algebraic attacks polynomial relations of input and output bits are essential. The smaller the degree is, the stronger the attack can be. Actually, at most quadratic and possibly cubic equations seem to be relevant in practice. For example, when looking for cubic equations we try to fulfill

\[
\alpha_0 + \sum_i \alpha_i z_i + \sum_{i<j} \alpha_{ij} z_i z_j + \sum_{i<j<k} \alpha_{ijk} z_i z_j z_k = 0
\]
for all \( z = (x_0, \ldots, x_{k-1}, y_0, \ldots, y_{\ell-1}) \in \mathbb{F}_2^{k+\ell} \) with \( y = S(x) \) when \( S \) is a \( k \)-to-\( \ell \)-bit S-box. For \( k = 6 \), \( \ell = 4 \) and degree 3, this is a linear system with 64 equations for the 176 coefficients \([\alpha_s]\). Since we have \( u^2 = u \) for \( u \in \mathbb{F}_2 \), we usually consider only multilinear polynomials, i.e., polynomials of degree at most 1 with respect to each variable.

**Definition 2.3 (General algebraic relations).** An algebraic relation is a polynomial \( p \in \mathbb{F}_2[x, y] \) such that \( p(x, S(x)) = 0 \) for all \( x \in \mathbb{F}_2^k \). Given \( d \in \mathbb{N} \) we define the number

\[
\dimrel(S)_d := \dim \left\{ p \in \mathbb{F}_2[x, y] \left| \begin{array}{l}
p \text{ multilinear} \land \deg p \leq d \\
\forall x \in \mathbb{F}_2^k : p(x, S(x)) = 0
\end{array} \right. \right\}
\]

of independent (multilinear) relations for \( S \) in degree \( d \). The algebraic degree

\[
\algdeg(S) := \min \left\{ d \in \mathbb{N} \leq k \left| \dimrel(S)_d > 0 \right. \right\}
\]

of \( S \) is the smallest degree that allows a non-trivial algebraic relation.

In general, \( \dimrel(S)_d \geq \sum_{j \leq d} \binom{k+\ell}{j} - 2^k \) and \( \algdeg(S) \leq k \).

We wish to have the number of independent relations as small as possible to avoid algebraic attacks as far as possible. In particular, for DES conditions we would like to have \( \dimrel(S)_2 = 0 \) and \( \dimrel(S)_d = \sum_{j \leq d} \binom{10}{j} - 2^6 \) for \( i \geq 3 \).

Saarinen (2012), Definition 3, considers more special relations:

**Definition 2.4 (Output-linear algebraic relations).** An output-linear algebraic relation is a pair \((p, b)\) with a multilinear polynomial \( p \in \mathbb{F}_2[x] \) and a (non-trivial) linear form \( b \in \mathbb{F}_2^{k'} \) so that \( \langle b \mid S(x) \rangle = p(x) \) for all \( x \in \mathbb{F}_2^k \). The smallest possible degree for \( p \) is called the degree \( \deg \langle b \mid S(\cdot) \rangle \) of \( \langle b \mid S(\cdot) \rangle \). We define the output-linear degree

\[
\outlindeg(S) := \min \left\{ \deg \langle b \mid S(\cdot) \rangle \left| b \in \mathbb{F}_2^{k'} \setminus \{0\} \right. \right\}
\]

as the least degree needed for \( p \) when varying over all \( b \). More details are revealed by the number

\[
\dimoutlinrel(S)_d := \dim \left\{ (p, b) \in \mathbb{F}_2[x] \times \mathbb{F}_2^{k'} \left| \begin{array}{l}
p \text{ multilinear} \land \deg p \leq d \\
\forall x \in \mathbb{F}_2^k : \langle b \mid S(x) \rangle = p(x)
\end{array} \right. \right\}
\]

of independent output-linear relations for \( S \) in degree \( d \). Now, \( \outlindeg(S) = \min \left\{ d \in \mathbb{N} \leq k \left| \dimoutlinrel(S)_d > 0 \right. \right\} \).

In general, \( \dimoutlinrel(S)_d \geq \sum_{j \leq d} \binom{5}{j} - 2^k \) and \( \outlindeg(S) \leq k \). Since each output-linear algebraic relation is an algebraic relation \( \langle b \mid y \rangle = p(x) = 0 \) of same degree, we have that \( \dimoutlinrel(S)_d > 0 \) implies \( \dimrel(S)_d > 0 \). However, the converse is wrong. In other words, \( \algdeg(S) \leq \outlindeg(S) \) but equality may not hold. The DES S-box \( S_1 \) actually has \( \algdeg(S_1) = 2 \) and \( \outlindeg(S_1) = 3 \).
2.4. Avalanche effect. Finally, we define the differential and linear branch numbers.

**Definition 2.5 (Branch numbers).** The differential branch number is defined as

$$\text{diffbranch}(S) = \min \{ \text{wt}(\Delta x) + \text{wt}(\Delta y) \mid \text{diff}_S(\Delta x \to \Delta y) \neq 0 \},$$

where $\Delta x \in \mathbb{F}_2^k$, $\Delta y \in \mathbb{F}_2^\ell$, $(\Delta x, \Delta y) \neq (0,0)$. The linear branch number is defined as

$$\text{linbranch}(S) = \min \{ \text{wt}(a) + \text{wt}(b) \mid \text{bias}_S(a, b) \neq 0 \},$$

where $a \in \mathbb{F}_2^{k\lor}$, $b \in \mathbb{F}_2^{\ell\lor}$, $(a, b) \neq (0,0)$.

The larger the branch numbers are, the stronger the avalanche effect should be. Saarinen (2012), Definition 4, only considers differential branch numbers.

3. Equivalence classes

Given one S-box $S$ we can derive others by affine transformation:

$$T: \mathbb{F}_2^k \rightarrow \mathbb{F}_2^\ell, \quad x \mapsto JS(Ix + s) + t,$$

where $I: \mathbb{F}_2^k \rightarrow \mathbb{F}_2^k$, $J: \mathbb{F}_2^\ell \rightarrow \mathbb{F}_2^\ell$ are invertible linear maps and $s \in \mathbb{F}_2^k$, $t \in \mathbb{F}_2^\ell$.

**Definition 3.1 (Equivalence).** We call $S$ and $T$ linear-affine equivalent if there is an affine transformation.

We call $S$ and $T$ permutation-affine equivalent if there is an affine transformation where the matrices are even permutation matrices.

Note that permutation matrices are exactly those invertible linear maps that respect the weight. One can check that two permutation equivalent S-boxes $S$ and $T$ have strongly related differential probabilities and biases. Namely, considered as matrices $\text{diff}_S(\cdot \to \cdot)$ and $\text{diff}_T(\cdot \to \cdot)$ are obtained from each other by permuting rows and columns according to the permutations $I$ and $J^{-1}$; for $\text{bias}_S(\cdot, \cdot)$ and $\text{bias}_T(\cdot, \cdot)$ additionally some signs change depending on the shifts $s$ and $t$. The algebraic quantities, namely $\text{dimrel}(S)$, $\text{algdeg}(S)$, $\text{dimoutlinrel}(S)$ and $\text{outlindeg}(S)$, are even invariant under linear-affine transformation. This still holds for the finer multiset $\{ \text{deg}(b \mid S(\cdot)) \mid b \in \mathbb{F}_2^4 \setminus \{0\} \}$. The branch numbers do not change under permutation equivalence. Summarizing: all quantities introduced in Section 2 are essentially invariant under permutation-affine transformations.
4. Properties of the proposed S-box

The differential probabilities are found in Figure 4.2. The different colors mark values affected by different properties from Figure 1.1. Figure 4.2 shows that \( \text{diffbranch}(U) = 2 \). Actually, the orange area, reflecting \( S_4 \), and its surrounding shows that it only fails marginally to reach 3: There are only five differentials \( \Delta x \to 0000 \) with \( \text{wt}(\Delta x) = 2 \) that have non-zero probability, there is no nontrivial differential \( \Delta x \to \Delta y \) with \( \Delta y \neq 0 \) and \( \text{wt}(\Delta x) + \text{wt}(\Delta y) = 2 \). Most of this behavior is part of the design properties for the DES S-boxes.

The biases are found in Figure 4.3. Note that for all \( a \in F_2^6 \) and \( b \in F_2^4 \) with \( a, b \) not both zero, we have \( |\text{bias}_U(a, b)| \leq \frac{24}{64} \), improving the previous best bound \( \frac{28}{64} \) again. The yellow area is all zero due to \( Q_3^+ \) and that implies that \( U \) has \( \text{linbranch}(U) = 3 \).

All earlier 6-to-4-bit S-boxes examined only have linear branch number 2.

Next, we consider the number of independent algebraic relations:

\[
\text{dimrel}(U) = [0, 0, 0, 112, 322, \ldots].
\]

These are the minimal possible numbers: \( \text{dimrel}(U)_d = \sum_{j \leq d} \binom{10}{j} - 2^6 \) for \( d \geq 3 \). Consequently, we have the optimal value

\[
\text{algdeg}(U) = 3.
\]

When restricting to special relations we find

\[
\text{outlindeg}(U) = 4.
\]

Optimal would be 5, but this is only achieved by some DES S-boxes which are worse

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|}
\hline
\text{Property} & \text{Optimal} & U & \text{DES1} & \text{DES2} & \text{DES3} & \text{DES4} & \text{DES5} & \text{DES6} & \text{DES7} & \text{DES8} \\
\hline
\text{diffbranch} & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
\hline
\text{linbranch} & 3 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
\hline
\text{algdeg} & 3 & 3 & 2 & 2 & 3 & 3 & 2 & 3 & 3 & 3 \\
\hline
\text{dimrel}_2 & 0 & 0 & 1 & 1 & 0 & 0 & 5 & 1 & 0 & 0 \\
\hline
\text{outlindeg} & 5 & 4 & 4 & 4 & 4 & 3 & 4 & 5 & 5 & 4 \\
\hline
\text{dimoutlinrel}_3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\hline
\text{dimoutlinrel}_4 & 0 & 4 & 2 & 1 & 2 & 3 & 1 & 1 & 0 & 1 \\
\hline
\text{dimoutlinrel}_5 & 3 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\
\hline
\end{array}
\]

Figure 4.1: Comparison of 6-to-4-bit S-boxes

in other aspects. Actually, there are four independent (ie. \( 2^4 - 1 \) in total) degree 4 relations. Equivalently, for \( b \in F_2^4 \setminus \{0\} \) each \( \langle b | U(\cdot) \rangle \) has degree 4. However, degree 4 is already a very high single round degree for algebraic attacks, anyways.
\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure.png}
\caption{$\Delta \cdot \text{diff} (\xi \rightarrow \eta)$}
\end{figure
<table>
<thead>
<tr>
<th>a \ b</th>
<th>0000</th>
<th>0001</th>
<th>0010</th>
<th>0011</th>
<th>0100</th>
<th>0101</th>
<th>0110</th>
<th>0111</th>
<th>1000</th>
<th>1001</th>
<th>1010</th>
<th>1011</th>
<th>1100</th>
<th>1101</th>
<th>1110</th>
<th>1111</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0001</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0010</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0011</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0100</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0101</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0110</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>0111</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1001</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1010</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1011</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1100</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>1101</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1110</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1111</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Figure 4.3: $2^6 \cdot \text{bias}_U(a, b)$
5. Bijective 4-to-4-bit sub-boxes

We briefly analyze the bijective 4-to-4-bit sub-boxes of the S-box $U$.

Like any DES-suitable S-box, the S-box $U$ is composed of four bijective 4-to-4-bit S-boxes, namely, $U(a****f)$ for $a, f \in \mathbb{F}_2$. Their canonical representatives in Saarinen’s language are:

<table>
<thead>
<tr>
<th>$af$</th>
<th>$U(a****f)$</th>
<th>permutation-affine canonical form</th>
<th>linear-affine canonical form</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0972BEC53FD841A6</td>
<td>035F78E1BD24C69A</td>
<td>012345768A9BCEFD</td>
</tr>
<tr>
<td>01</td>
<td>B68F215CDAE37409</td>
<td>035674ED9F28CAB1</td>
<td>012345896ACEFB7</td>
</tr>
<tr>
<td>10</td>
<td>E48D271B5A639CF0</td>
<td>03596AFCB42ED187</td>
<td>012345768A9BCEFD</td>
</tr>
<tr>
<td>11</td>
<td>1D42F8A76095CB3E</td>
<td>035874EF6AD2BC1</td>
<td>012345768ACEFB7</td>
</tr>
</tbody>
</table>

It turns out that the first and the third are linear-affine equivalent.

Due to property $Q1'$ there is a second way to compose the S-box $U$ from four 4-to-4-bit S-boxes, namely, by taking $U(****ef)$ for $e, f \in \mathbb{F}_2$. These are:

<table>
<thead>
<tr>
<th>$ef$</th>
<th>$U(****ef)$</th>
<th>permutation-affine canonical form</th>
<th>linear-affine canonical form</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>07BC3D4AE821569F</td>
<td>0358A46FE9B7D21C</td>
<td>012345896ABCE7DF</td>
</tr>
<tr>
<td>01</td>
<td>B825DE7014FA69C3</td>
<td>0356789FDBACE142</td>
<td>012345786ABCE9FD</td>
</tr>
<tr>
<td>10</td>
<td>92E5F8164D7B23C0</td>
<td>0358A46FE9B7D21C</td>
<td>012345896ABCE7DF</td>
</tr>
<tr>
<td>11</td>
<td>6F1CA349D28705BE</td>
<td>0356789FADC6B1E24</td>
<td>012345786ABCE9FD</td>
</tr>
</tbody>
</table>

Here, the first and third are even permutation-affine equivalent and the second and fourth are linear-affine equivalent.

These eight 4-to-4-bit S-boxes are the only bijective 4-to-4-bit sub-boxes of $U$. Even, when allowing linear-affine sub-boxes there is no further bijective 4-to-4-bit sub-box of $U$. None of the them is linear-affine equivalent to a golden S-box in terms of Saarinen (2012).

6. How to find good boxes

In order to find good S-boxes, we have written a C program that searches in a depth first manner the tree of all partially defined 6-to-4-bit S-boxes, where the leaves are all totally defined boxes. Thus the tree has depth $k$ and each node has $2^4$ child nodes, representing one new value for a so far undefined position. Since the complete tree has $(2^4)^{2^6} = 2^{256}$ leaves it is obviously infeasible to traverse the whole tree. Also, many S-boxes within this tree are trivially unsuitable or do not fulfill the necessary properties like the ones stated in Coppersmith (1994) or Leander et al. (2007).

Our search algorithm computes the table of differential probabilities and the bias tables incrementally along the path from the root to a leaf. During this progress the values for the differential probabilities increase monotonically by $0/2^b$, $1/2^b$ or
In each step and table position. Once a differential probability has bypassed a bound from a condition, no completion can fulfill that condition any more and thus that entire branch can be purged from the tree. In contrast, the values for the biases change by $\pm 1/2^6$ in each step. Thus a similar technique for the bias values is more tricky. Finally, conditions like $Q_5$, involving products of bias values, can only be checked at the leaves. These techniques allow us to reduce the size of the tree to estimated $2^{48}$ S-boxes, which now seems feasible. After 14.66 CPU-years on 12 to 16 Intel Xeon 3.00GHz processors, it has scanned an estimated fraction of 2–7% of the purged search tree. (The large interval is due to the inherent difficulty of telling the size of the subtrees below a given node. We thus use two different heuristics to estimate the processed fraction of the tree.) We estimate that the algorithm would finish with the whole tree in roughly 12 to 39 years on our tiny cluster. However, we do not expect to find even better S-boxes nor S-boxes inequivalent to \( U \).

7. Conclusion

We propose a family of 6-to-4-bit S-boxes with linear branch number 3. Besides that extraordinary feature, its biases are bounded by $2^{64}$, which is very small, and it also fulfills most other design criteria of Coppersmith (1994) and Leander et al. (2007). It may thus serve as a building block for DES-like ciphers.

We briefly discussed the structure of bijective 4-to-4-bit sub-boxes and observed that these sub-boxes are not golden but in a surprising way closely related to each other.

Acknowledgements

This work was funded by the B-IT foundation and the state of North Rhine-Westphalia.

References


DANIEL LOEBENBERGER
b-it
Universität Bonn
Dahlmannstr. 2
D53113 Bonn
daniel@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de/~loebenberger/

MICHAEL NÜSKEN
b-it
Universität Bonn
Dahlmannstr. 2
D53113 Bonn
nuesken@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de/~nuesken/