# On Algebraic Relations of Serpent S-Boxes

Bhupendra Singh, Lexy Alexander, Sanjay Burman
Email:{scientistbsingh, lexyalexander, sanjayburman}@gmail.com
CAIR, DRDO, Bangalore - 560093, India.

**Abstract:** Serpent is a 128-bit block cipher designed by Ross Anderson, Eli Biham and Lars Knudsen as a candidate for the Advanced Encryption Standard (AES). It was a finalist in the AES competition. The winner, Rijndael, got 86 votes at the last AES conference while Serpent got 59 votes [1]. The designers of Serpent claim that Serpent is more secure than Rijndael.In this paper we have observed that the nonlinear order of all output bits of serpent S-boxes are not 3 as it is claimed by the designers.

## 1 Introduction

Serpent [2] is one of the five block ciphers chosen as AES finalists. It is a 32-round SP-network operating on four 32-bit words, thus having a block size of 128 bits. The cipher consists of:

- An initial permutation IP;
- 32 rounds, each consisting of a key mixing operation, a pass through S-boxes, and (in all but the last round) a linear transformation. In the last round, this linear transformation is replaced by an additional key mixing operation;
- A final permutation FP;

The 32 rounds use 8 different S-boxes each of which maps four inputs bits to four output bits. Each S-box is used in precisely four rounds, and in each of these rounds it is used 32 times in parallel.

## 2 The S-boxes

In the description of the design of S-boxes [Section 2.1,[2]], it is claimed that "The S-boxes of Serpent are 4-bit permutations with the following properties:
- each differential characteristic has a probability of at most 1/4, and a one-bit input difference will never lead to a one-bit output difference;
- each linear characteristic has a probability in the range $1/2 \pm 1/4$, and a linear relation between one single bit in the input and one single bit in the output has a probability in the range $1/2 \pm 1/8$;
**-the nonlinear order of the output bits as a function of the input bits is the maximum, namely 3.**"

But we have found there are some output bits whose nonlinear order as a function of the input bits is only 2. Contrary to the designers claim that the nonlinear order of the output bits of S-boxes are 3.

The S-boxes used in Serpent for encryption from $S_0$ to $S_7$ are given below:

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S0: | 3 | 8 | 15 | 1 | 10 | 6 | 5 | 11 | 14 | 13 | 4 | 2 | 7 | 0 | 9 | 12 |
| S1: | 15 | 12 | 2 | 7 | 9 | 0 | 5 | 10 | 1 | 11 | 14 | 8 | 6 | 13 | 3 | 4 |
| S2: | 8 | 6 | 7 | 9 | 3 | 12 | 10 | 15 | 13 | 1 | 14 | 4 | 0 | 11 | 5 | 2 |
| S3: | 0 | 15 | 11 | 8 | 12 | 9 | 6 | 3 | 13 | 1 | 2 | 4 | 10 | 7 | 5 | 14 |
| S4: | 1 | 15 | 8 | 3 | 12 | 0 | 11 | 6 | 2 | 5 | 4 | 10 | 9 | 14 | 7 | 13 |
| S5: | 15 | 5 | 2 | 11 | 4 | 10 | 9 | 12 | 0 | 3 | 14 | 8 | 13 | 6 | 7 | 1 |
| S6: | 7 | 2 | 12 | 5 | 8 | 4 | 6 | 11 | 14 | 9 | 1 | 15 | 13 | 3 | 10 | 0 |
| S7: | 1 | 13 | 15 | 0 | 14 | 8 | 2 | 11 | 7 | 4 | 12 | 10 | 9 | 3 | 5 | 6 |

The inverse S-boxes used in Serpent for decryption from InvS0 to InvS7 are given below:

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| InvS0: | 13 | 3 | 11 | 0 | 10 | 6 | 5 | 12 | 1 | 14 | 4 | 7 | 15 | 9 | 8 | 2 |
| InvS1: | 5 | 8 | 2 | 14 | 15 | 6 | 12 | 3 | 11 | 4 | 7 | 9 | 1 | 13 | 10 | 0 |
| InvS2: | 12 | 9 | 15 | 4 | 11 | 14 | 1 | 2 | 0 | 3 | 6 | 13 | 5 | 8 | 10 | 7 |
| InvS3: | 0 | 9 | 10 | 7 | 11 | 14 | 6 | 13 | 3 | 5 | 12 | 2 | 4 | 8 | 15 | 1 |
| InvS4: | 5 | 0 | 8 | 3 | 10 | 9 | 7 | 14 | 2 | 12 | 11 | 6 | 4 | 15 | 13 | 1 |
| InvS5: | 8 | 15 | 2 | 9 | 4 | 1 | 13 | 14 | 11 | 6 | 5 | 3 | 7 | 12 | 10 | 0 |
| InvS6: | 15 | 10 | 1 | 13 | 5 | 3 | 6 | 0 | 4 | 9 | 14 | 7 | 2 | 12 | 8 | 11 |
| InvS7: | 3 | 0 | 6 | 13 | 9 | 14 | 15 | 8 | 5 | 12 | 11 | 7 | 10 | 1 | 4 | 2 |

# 3 Algebraic Relations of Serpent S-Boxes

Let $x_3$, $x_2$, $x_1$, $x_0$ be the input bits to a S-box and let $s_{i,3}$, $s_{i,2}$, $s_{i,2}$, $s_{i,0}$ denote the output bits of the $i$th S-box Si. Then, we can represent each of the output bit as a function of the input bits as follows:

$$
\begin{aligned}
s_{0,3} &= x_0 + x_1 + x_2 + x_3 + x_3x_0 \\
s_{0,2} &= x_1 + x_1x_0 + x_2x_0 + x_2x_1x_0 + x_3 + x_3x_1 + x_3x_2x_1 \\
s_{0,1} &= 1 + x_0 + x_2x_0 + x_2x_1 + x_2x_1x_0 + x_3x_1 + x_3x_2x_0 + x_3x_2x_1 \\
s_{0,0} &= 1 + x_0 + x_1x_0 + x_2 + x_2x_0 + x_2x_1 + x_2x_1x_0 + x_3 + x_3x_2x_0 + x_3x_2x_1 \\
s_{1,3} &= 1 + x_1 + x_2x_0 + x_3 + x_3x_0 + x_3x_1x_0 + x_3x_2x_0 + x_3x_2x_1 \\
s_{1,2} &= 1 + x_1 + x_1x_0 + x_2 + x_3 \\
s_{1,1} &= 1 + x_0 + x_1x_0 + x_2 + x_2x_0 + x_3 + x_3x_1 + x_3x_1x_0 + x_3x_2x_0 + x_3x_2x_1 \\
s_{1,0} &= 1 + x_0 + x_1 + x_2x_1 + x_3x_0 + x_3x_2 + x_3x_2x_0 + x_3x_2x_1 \\
s_{2,3} &= 1 + x_0 + x_1 + x_2 + x_2x_1x_0 + x_3x_1 \\
s_{2,2} &= x_0 + x_1 + x_2x_1 + x_3 + x_3x_1 + x_3x_1x_0 + x_3x_2 + x_3x_2x_0 \\
s_{2,1} &= x_0 + x_1 + x_2 + x_2x_1 + x_2x_1x_0 + x_3x_0 + x_3x_1x_0 + x_3x_2 + x_3x_2x_0 \\
s_{2,0} &= x_1 + x_2 + x_2x_0 + x_3 \\
s_{3,3} &= x_0 + x_1 + x_1x_0 + x_2 + x_2x_0 + x_2x_1x_0 + x_3 + x_3x_2 + x_3x_2x_0 \\
s_{3,2} &= x_0 + x_1x_0 + x_2 + x_2x_1x_0 + x_3 + x_3x_1 + x_3x_1x_0 \\
s_{3,1} &= x_0 + x_1 + x_2x_0 + x_3x_0 + x_3x_1x_0 + x_3x_2 + x_3x_2x_0 \\
s_{3,0} &= x_0 + x_1 + x_2x_1 + x_3 + x_3x_0 + x_3x_2 + x_3x_2x_0 + x_3x_2x_1 \\
s_{4,3} &= x_0 + x_1 + x_2 + x_2x_1 + x_3x_0 + x_3x_1 + x_3x_1x_0 \\
s_{4,2} &= x_0 + x_1x_0 + x_2 + x_2x_1 + x_2x_1x_0 + x_3x_1 + x_3x_1x_0 + x_3x_2 + x_3x_2x_1 \\
s_{4,1} &= x_0 + x_2x_0 + x_2x_1 + x_3 + x_3x_1 + x_3x_2 + x_3x_2x_0 + x_3x_2x_1 \\
s_{4,0} &= 1 + x_1 + x_1x_0 + x_2 + x_3 + x_3x_0 + x_3x_1 \\
s_{5,3} &= 1 + x_0 + x_1 + x_2 + x_2x_1x_0 + x_3 + x_3x_0 + x_3x_2x_0 \\
s_{5,2} &= 1 + x_1 + x_2x_0 + x_3 + x_3x_1x_0 + x_3x_2 + x_3x_2x_0 + x_3x_2x_1 \\
s_{5,1} &= 1 + x_0 + x_1x_0 + x_2 + x_3 + x_3x_1 + x_3x_1x_0 + x_3x_2 \\
s_{5,0} &= 1 + x_1 + x_1x_0 + x_2 + x_3 + x_3x_0 + x_3x_1 \\
s_{6,3} &= x_1 + x_1x_0 + x_2 + x_2x_0 + x_2x_1x_0 + x_3 + x_3x_2 + x_3x_2x_1 \\
s_{6,2} &= 1 + x_0 + x_1x_0 + x_2 + x_2x_1 + x_2x_1x_0 + x_3x_1 + x_3x_1x_0 + x_3x_2 + x_3x_2x_1 \\
s_{6,1} &= 1 + x_1 + x_2 + x_3x_0 \\
s_{6,0} &= 1 + x_0 + x_1 + x_2 + x_2x_0 + x_2x_1 + x_2x_1x_0 + x_3 + x_3x_1x_0 + x_3x_2x_1 \\
s_{7,3} &= x_0 + x_1 + x_2 + x_2x_0 + x_2x_1x_0 + x_3x_0 \\
s_{7,2} &= x_0 + x_1 + x_2 + x_2x_1x_0 + x_3 + x_3x_0 + x_3x_1 + x_3x_1x_0 + x_3x_2x_1 \\
s_{7,1} &= x_1 + x_1x_0 + x_2 + x_2x_0 + x_2x_1 + x_3 + x_3x_0 + x_3x_1x_0 + x_3x_2x_0 \\
s_{7,0} &= 1 + x_1x_0 + x_2 + x_3x_0 + x_3x_1 + x_3x_2 + x_3x_2x_0 + x_3x_2x_1
\end{aligned}
$$

It can be seen from above para that some of the output bits are functions of the input bits with nonlinear order 2, namely $s_{0,3}$, $s_{1,2}$, $s_{2,0}$, $s_{4,0}$, $s_{5,0}$, $s_{6,1}$. Also $s_{4,0}$ and $s_{5,0}$ are identical.

Also, we can see that in the case of inverse S-boxes the nonlinear order of the output bits of the Serpent S-box is either 2 or 3. Let $x_3$, $x_2$, $x_1$, $x_0$ be the input bits to an Inverse S-box and let $invs_{i,3}$, $invs_{i,2}$, $invs_{i,2}$, $invs_{i,0}$ denote the output bits of the $i$th inverse S-box InvSi.

$$invs_{0,3} = 1 + x_0 + x_2x_1 + x_3 + x_3x_1x_0 + x_3x_2 + x_3x_2x_0 + x_3x_2x_1$$
$$invs_{0,2} = 1 + x_0 + x_1 + x_1x_0 + x_2 + x_3$$
$$invs_{0,1} = x_0 + x_1 + x_2 + x_2x_0 + x_3x_1 + x_3x_2x_0 + x_3x_2x_1$$
$$invs_{0,0} = 1 + x_1x_0 + x_2 + x_2x_1 + x_3x_0 + x_3x_1 + x_3x_1x_0 + x_3x_2 + x_3x_2x_0 + x_3x_2x_1$$
$$invs_{1,3} = x_0 + x_2 + x_3 + x_3x_1$$
$$invs_{1,2} = 1 + x_0 + x_1 + x_2x_0 + x_2x_1 + x_2x_1x_0 + x_3 + x_3x_2x_0$$
$$invs_{1,1} = x_1 + x_2 + x_2x_1x_0 + x_3 + x_3x_0 + x_3x_1 + x_3x_2x_0 + x_3x_2x_1$$
$$invs_{1,0} = 1 + x_0 + x_1 + x_1x_0 + x_2x_1x_0 + x_3x_1 + x_3x_2x_0 + x_3x_2x_1$$
$$invs_{2,3} = 1 + x_1x_0 + x_2x_1 + x_2x_1x_0 + x_3 + x_3x_2x_0$$
$$invs_{2,2} = 1 + x_0 + x_1x_0 + x_2 + x_3 + x_3x_0 + x_3x_1 + x_3x_1x_0 + x_3x_2x_0$$
$$invs_{2,1} = x_1 + x_1x_0 + x_2 + x_3x_0 + x_3x_1x_0 + x_3x_2 + x_3x_2x_0$$
$$invs_{2,0} = x_0 + x_1 + x_2 + x_2x_1 + x_3x_1$$
$$invs_{3,3} = x_0 + x_1 + x_2 + x_2x_0 + x_2x_1x_0 + x_3x_0 + x_3x_1x_0 + x_3x_2$$
$$invs_{3,2} = x_1x_0 + x_2x_0 + x_2x_1 + x_3x_0 + x_3x_1 + x_3x_1x_0 + x_3x_2 + x_3x_2x_0$$
$$invs_{3,1} = x_1 + x_2 + x_2x_1 + x_2x_1x_0 + x_3 + x_3x_0 + x_3x_2x_0 + x_3x_2x_1$$
$$invs_{3,0} = x_0 + x_2 + x_2x_1 + x_3 + x_3x_0 + x_3x_1 + x_3x_2x_1$$
$$invs_{4,3} = x_1 + x_1x_0 + x_2 + x_3x_0 + x_3x_1x_0 + x_3x_2$$
$$invs_{4,2} = 1 + x_0 + x_1 + x_1x_0 + x_2 + x_2x_0 + x_2x_1x_0 + x_3 + x_3x_1 + x_3x_1x_0$$
$$invs_{4,1} = x_1x_0 + x_2 + x_2x_0 + x_3 + x_3x_0 + x_3x_2x_0$$
$$invs_{4,0} = 1 + x_0 + x_1 + x_2 + x_3 + x_3x_0 + x_3x_1x_0 + x_3x_2 + x_3x_2x_0$$
$$invs_{5,3} = 1 + x_1 + x_1x_0 + x_2 + x_2x_1x_0 + x_3x_0$$
$$invs_{5,2} = x_0 + x_1x_0 + x_2 + x_3x_1 + x_3x_1x_0 + x_3x_2x_0$$
$$invs_{5,1} = x_0 + x_1 + x_2x_0 + x_2x_1 + x_2x_1x_0 + x_3 + x_3x_0 + x_3x_1x_0$$
$$invs_{5,0} = x_0 + x_2x_1 + x_3 + x_3x_1x_0$$
$$invs_{6,3} = 1 + x_1 + x_1x_0 + x_2 + x_2x_1 + x_2x_1x_0 + x_3 + x_3x_0 + x_3x_1x_0 + x_3x_2 + x_3x_2x_1$$
$$invs_{6,2} = 1 + x_0 + x_1 + x_2x_1 + x_3x_1 + x_3x_1x_0 + x_3x_2 + x_3x_2x_1$$
$$invs_{6,1} = 1 + x_1 + x_2 + x_2x_0 + x_3$$
$$invs_{6,0} = 1 + x_0 + x_1x_0 + x_2x_0 + x_2x_1 + x_2x_1x_0 + x_3 + x_3x_1x_0 + x_3x_2x_1$$
$$invs_{7,3} = x_1x_0 + x_2 + x_2x_1x_0 + x_3x_0 + x_3x_1 + x_3x_1x_0$$
$$invs_{7,2} = x_1 + x_2x_0 + x_3 + x_3x_1x_0 + x_3x_2 + x_3x_2x_0$$
$$invs_{7,1} = 1 + x_0 + x_2 + x_2x_1 + x_3 + x_3x_0 + x_3x_1 + x_3x_2x_0 + x_3x_2x_1$$
$$invs_{7,0} = 1 + x_0 + x_1 + x_2x_1 + x_3x_1 + x_3x_1x_0 + x_3x_2 + x_3x_2x_1$$

It can be seen that from the above para the output bits $invs_{0,2}$, $invs_{1,3}$, $invs_{2,0}$, $invs_{6,1}$ are functions of the input bits with nonlinear order 2.

**Conclusion:** We find that there is some discrepancy between the properties of the actual S-boxes of Serpent and the claims of the designers. It is surprising that this has not been pointed out by any body so long. This leads the revisiting the Security of the serpent.

**Acknowledgment:** The authors thank Director and Associate Director of CAIR, DRDO for their constant support and encouragement for this work.

# References

[1] *http://www.cl.cam.ac.uk/ rja14/serpent.html.*

[2] Anderson, R., Biham, E., Knudsen, L,R. *Serpent: A Proposal for the Advanced Encryption Standard*, NIST AES Proposal (1998).