DPA Resilience of Rotation-Symmetric S-boxes

Muhammet Ali Evci¹ and Selçuk Kavut²

¹ Cyber Security Institute, Informatic and Information Security Research Center, TÜBİTAK, 41400, Kocaeli, Turkey
mali.evci@tubitak.gov.tr
² Department of Electronics Engineering, Gebze Institute of Technology – GYTE, 41400, Kocaeli, Turkey
skavut@gyte.edu.tr

Abstract. We regenerate the S-boxes that achieve the best possible trade-off between nonlinearity and differential uniformity in the class of 6×6 rotation-symmetric S-boxes (RSSBs) that are bijective, and then classify them in terms of transparency order. We find that although the transparency order \( \geq 5.638 \) for the inverse function over \( \mathbb{F}_{2^6} \), which can also be considered as rotation-symmetric, there exist RSSBs with the same nonlinearity and differential uniformity as those of the inverse function, having transparency order as low as 5.238. Motivated by this, we perform a steepest-descent-like iterative search algorithm in the class of 8×8 RSSBs and attain S-boxes with nonlinearity 104, differential uniformity 6, and transparency orders noticeably better than that of the AES S-box. Finally, replacing the AES S-box with those found by the search algorithm, we implement differential power analysis (DPA) attacks on SASEBO-GII and give a comparison of the results.

1 Introduction

In most of the block cipher cryptosystems, the S-boxes (substitution boxes) are the only nonlinear components, and hence the strength of these cryptosystems depends heavily on the cryptographic properties of the S-boxes. On one hand, most of these properties such as nonlinearity, differential uniformity, and algebraic degree protects the cryptosystem against linear [12], differential [1], and higher order differential [10] cryptanalyses respectively, which are independent from the hardware design of the S-boxes. On the other hand, the side channel analysis (SCA) relies on the hardware’s leakages such as the timing of operations [8], power consumption [9], and electromagnetic radiation [19], and therefore the cryptographic primitives used in a cryptosystem should also be resistant against SCA. In this direction, the resistance of an S-box to side channel attacks is quantified in [18] which introduces the notion of transparency order of an S-box. Then, it was shown [3] that some highly nonlinear S-boxes (including the AES S-box) constructed using power maps over \( \mathbb{F}_{2^n} \) have bad transparency orders. However, there are still no construction methods of the S-boxes with low transparency order, which achieve high nonlinearity, low differential uniformity, and high algebraic degree. Recently, a constrained random search is
performed \[13\] yielding 8×8 S-boxes with lower transparency orders than that of the AES S-box. Subsequently, a search in the class of rotation-symmetric S-boxes (RSSBs) is carried out in \[14\], which improves both transparency order and nonlinearity results in \[13\]. Then, in \[17\], using genetic algorithms the transparency order obtained in \[14\] is noticeably improved at the price of weaker nonlinearity and differential uniformity. In this paper, we improve the traditional cryptographic properties such as nonlinearity, differential uniformity, and absolute indicator along with the transparency order when compared with those in the literature.

Let \( s : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n} \) be an S-box. Then, in a normal basis over \( \mathbb{F}_{2^n} \), the S-boxes for which \( (s(\alpha))^2 = s(\alpha^2) \), \( \forall \alpha \in \mathbb{F}_{2^n} \), can be considered as rotation-symmetric \[20\]. It was shown \[20\] that the S-boxes described as a sum of power maps and exponentiations over finite fields are linearly equivalent to RSSBs. Hence, most of the S-box constructions, including the inverse function \[16\] (used as S-box in the AES), can be regarded as RSSBs, which demonstrates the fact that the class of RSSBs contains cryptographically desirable nonlinear S-boxes.

In \[7\], the bijective RSSBs of size 6×6 achieving the best possible trade-off between nonlinearity and differential uniformity in the class, i.e., with nonlinearity 24 and differential uniformity 4, are classified in terms of absolute indicator and algebraic degree. We regenerate those S-boxes and compute their transparency orders, which shows the existence of the S-boxes with significantly low transparency orders among them. Motivated by this, we perform a search in the class of 8×8 RSSBs that are bijective utilizing a steepest-descent-like iterative search algorithm \[6\], and find S-boxes with transparency order better than that of the AES S-box, attaining the other cryptographic properties comparable to those of the AES S-box. Further, using SASEBO-GII (Side-channel Attack Standard Evaluation Board-GII), we implement differential power analysis (DPA) \[9\] attacks on AES containing these S-boxes and compare their DPA resistance using the success rate \[22\] as our SCA security metric.

The remainder of this paper is organized as follows. In the following section, we survey the basic definitions and cryptographic criteria of S-boxes. In Section 3, we find the affine transformations under which the transparency order is invariant, and present the transparency orders of 6×6 RSSBs in \[7\] with nonlinearity 24 and differential uniformity 4. In Section 4, the cryptographic properties of the 8×8 RSSBs generated by the steepest-descent-like iterative search algorithm are given and compared with those of the S-boxes in the literature. Section 5 presents the implementation results of the DPA attacks on SASEBO-GII. Finally, we conclude the paper in Section 6.

2 Preliminaries

2.1 Cryptographic Properties

An \( n \times m \) S-box \( F \) is defined as a mapping \( F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m \), which is called \( n \)-variable Boolean function if \( m = 1 \). Most of the block cipher cryptosystems use the S-boxes with \( n = m \). The S-box \( F \) can be considered as a combination