

# Empirical Evaluation of the Resilience of Novel S-Box Implementations Against Power Side-Channel Attacks

**Supervisor**

Paolo Ernesto Prinetto

**Candidate**

Samuele Yves Cerini

April 5, 2021

The ever increasing pervasiveness of *IoT* devices and embedded systems mandates a systematic use of cryptography to protect everyday communications and personal data. The same factor has enabled for a plethora of attacks aimed at the weaknesses in the physical device implementations. Side-channel analysis falls in this category.

This class of attacks are carried out by observing physical parameters emitted by a hardware component such as the time taken for a cryptographic operation, the power consumption required, or the electromagnetic and acoustic emissions. The ultimate goal is to recover the secret keys used to ensure the confidentiality, integrity and authenticity of communications. This thesis targets, in the specific, side-channel power analysis. Any attack conducted with this methodology exploits the observation of the power consumption required during the operational activity of the device, in order to deduce the data treated internally during the execution. In this case, the attack specifically targets the power leaks related to the cryptographic key handled by the internal block cipher software (or hardware) implementation.

The widely known Spectre and Meltdown attacks demonstrated that side-channel analysis can be exploited, in conjunction with other techniques, to target consumer-grade Personal Computers, up to large scale mainframes. Recent Proof of Concepts demonstrated the feasibility of these attacks using Web technologies like JavaScript, proving the pervasiveness this class of attacks can leverage in real-world scenarios.

Although these egregious cases demonstrate the applicability of these attacks in everyday operations, side-channel analysis has received attention from academic research for at least two decades. Following the work presented by Kocher on differential power analysis, a plethora of publications have

repeatedly demonstrated the effectiveness of attacks targeting cryptographic implementations on physical devices. Today, side-channel attacks are considered part of cryptanalysis techniques in the same way as linear and differential analysis.

The impact that these attacks had on the most common cryptographic implementations (such as **AES**, **RSA**, etc.) led to a race to research countermeasures that could provide an increased level of security. In general, it has been observed that the greater the security provided by a particular solution, the greater its impact on the device performance. While this may not be a problem for some implementations, others, such as smartcards and other small embedded devices, cannot tolerate such a performance impact.

The need for lighter countermeasures has shifted the interest of academia from the implementation/physical level to the logical and mathematical one, the same in which encryption algorithms are specified. Therefore, resistance against side-channel attacks like power analysis are now being treated as a design parameter for new block cipher algorithms. Most of the newer proposals are directly targeting **S-Box** structures, being already the main component able to provide the necessary *confusion* and nonlinearity properties. Many theoretical metrics have been proposed in order to quantify the resistance of a certain cryptographic component against side-channel analysis, such as the transparency order (TO) and the confusion coefficient (CC). Various publications observed, however, that these metrics are in opposition with properties like nonlinearity and differential uniformity, used to denote the resistance against classical cryptanalysis.

These observations lead the academic research to slowly abandon the use of algebraic methodologies. These methods are indeed able to produce **S-Box** structures with excellent properties against linear and differential analysis, but are unable to widely explore the entire solution space. The goal is to search for good trade-offs among these two main classes of properties, slightly sacrificing the former to improve the latter. Among the many proposed, heuristic and chaos-based methods are the newest and most prolific.

The work proposed in this thesis aims at empirically verify the side-channel resistance claimed by the latest **S-Box** proposal, crafting an attack based exclusively on power analysis and leveraging one of the most promising and powerful tools available: *ChipWhisperer*<sup>TM</sup>. The attack is conducted on a software implementation of the **AES-128** algorithm, targeting an **XMEGA** 8-bit AVR microcontroller by *Atmel* and therefore providing a real-world attack scenario.

The analysis is conducted choosing six different **S-Box** structures, selected among the newer proposals from both the heuristic based methodologies and the chaos-based ones. One of the structures under analysis is the one provided by the original **AES** specification. To test each structure, the code

implementation of AES-128 is modified automatically at compilation time, the power traces related to the implementation execution are collected and the attack is performed. Four main iterations of the attack have been proposed, each with an increasing number of power measurements accomplished. An empirical metric has been leveraged to assess the resistance against side-channel power analysis of the structures under attack.

The results obtained and the graphs built leveraging the collected data confirm the ability of some of the latest **S-Box** proposal to provide a significantly higher resistance to side-channel analysis, acting as a lightweight countermeasure against this class of attacks. Indeed, two of the structures designed to optimize the confusion coefficient (CC) denoted a significant improvement, in some cases increasing the trace requirements to achieve a successful attack up to a factor of 10. The analysis also highlighted that, as expected, structures that were designed without taking into account side-channel resistance indicators performed poorly. For instance, no improvement was observed over the standard AES **S-Box**, as the secret key was revealed with an extremely reduced number of power traces.

One of the main goals of this thesis work has been placed on defining a reproducible and fully automatic attack environment. The proposed source code allows to conduct a detailed analysis, allowing, even for future purposes, to test different **S-Box** structures and collect detailed data about the attack. Future work may leverage the code provided in an attempt to build for a comprehensive, characterization capable of correlating the available theoretical metrics to real-world results.

The source code, the data and the results obtained are made accessible in the following link <https://github.com/Mrcuve0/Thesis-Work>.