Performance Comparison: Software vs. Hardware Implementation of Novel S-Box Designed to Resist Power Analysis Attack

Performance Comparison: Software vs. Hardware Implementation of Novel S-Box Designed to Resist Power Analysis Attack

Mattia Mirigaldi[1], Maurizio Martina[2], and Guido Masera[2]

Politecnico di Torino, Italy
name.surname@polito.it

Abstract. The Advanced Encryption Standard (AES) is the only approved symmetric encryption algorithm by security agencies such as the National Institute of Standards and Technology (NIST). The algorithm is designed to be fast and robust against cryptanalysis attacks. However, the original design lacks of any countermeasure against a novel class of attacks: side-channel attacks. This vulnerability necessitates the implementation of supplementary security measures to guarantee AES security in a deployment scenario. This paper explores a solution that targets the AES Substitution Box (S-Box) structure. The original S-Box is replaced with novel structures inherently more resistant to power-based side channel attacks. This concept is demonstrated by testing six different novel S-Box implementations. Each is subjected to real experiments via a correlation power analysis attack on an AES hardware implementation. A complete comprehension of their effectiveness is gained by comparing the results found to those derived from the AES SW implementation. The solution investigated leverages the inherent mathematical properties of the S-Box to provide a lightweight countermeasure against power analysis side-channel attacks with zero implementation cost.

Keywords: AES, S-Box, Side channel attacks, power analysis, CPA

1 Introduction

In 2001, the National Institute of Standards and Technology (NIST) selected the Rijndael algorithm as the new encryption standard. Following the competition, the Rijndael algorithm was designated as the Advanced Encryption Standard (AES). Due to its robustness and efficiency, AES has become the de facto standard in various applications, from encrypting government communications to protecting sensitive data on-edge devices. Attempting to break AES or other cryptographic algorithms by searching for weaknesses in the algorithm itself is highly complex and rather unsuccessful.

However, a new class of attacks known as side-channel attacks has emerged. These attacks focus on identifying weaknesses in the physical implementation of devices rather than the mathematical algorithms. It is well established that the secret processed by a chip can be recovered by observing its physical parameters, such as timing, power consumption, and electromagnetic emissions.

The standardized AES design lacks any countermeasures against side-channel attacks, making it particularly vulnerable to power analysis. Mitigating these vulnerabilities requires additional protective measures. Several solutions have been proposed, including constant-time algorithms, masking techniques, and secure hardware designs. However, these solutions have a performance impact - i.e. increase of area or reduction of speed - on real-embedded devices.
The necessity of lightweight countermeasures has prompted a shift in focus from an implementation/physical layout perspective to a mathematical one. This approach treats the resistance to side-channel attacks in a similar way as the resistance to classical cryptanalysis. In the case of AES, the substitution box (S-Box) is the most vulnerable component to side-channel attacks, as evidenced by early research papers [1] [2] [3]. As discussed in [4], the S-Box can be modified to possess higher inherent side-channel resilience, resulting in a countermeasure with no area overhead or performance impact on the AES implementation.
However, the author highlights that the theoretical metrics used to strengthen the power analysis resistance of an S-Box, such as the Transparency Order (TO) or the Confusion Coefficient (CC), cannot capture the complexity of a side-channel attack. Building on this concept, this paper presents an empirical evaluation of the latest S-Box implementations resistant to power analysis.
Their efficacy is assessed within an AES hardware implementation synthesized on an Artix-7 FPGA. The power traces are captured with a Picoscope 5000 series oscilloscope and fed to a correlation power analysis algorithm [5] to evaluate their resistance. Finally, to provide a comprehensive evaluation, the results are compared with those from an earlier study where the S-Boxes were tested within the AES software implementation on an STM32.

Organization. The rest of the paper is organized as follows: **Section 2** provides an overview of the AES algorithm, the cryptanalysis resistance, and the correlation power analysis attack. **Section 3** explains the attack model and covers the experimental setup employed. Lastly in **Section 4** the results obtained are discussed and compared with the results obtained with the AES software implementation. Finally, some concluding remarks are presented in **Section 5**.

2 Background

2.1 AES

The Advanced Encryption Standard (AES or Rijndael algorithm) is a symmetric encryption algorithm and is the sole standard defined by the NIST. It is a block cipher, whereby the input is transformed by the secret key into an output of the same size. The size is defined as the block size, and in the case of AES it is 128 bits. The transformation occurs in rounds, with the number of rounds dependent on the key size (128/192/256 bits, corresponding to 10/12/14 rounds). The encryption key is expanded through a key schedule algorithm into a series of round keys (each 128 bits long). The AES algorithm pseudocode is provided in Algorithm 1. The *AddRoundKey* operation performs a Boolean XOR between each input byte and a key byte, making it a per-byte process. This allows a

side-channel attacker to isolate and study the impact of a single key byte on the intermediate state, thereby narrowing the attack space to only 256 guesses.

Algorithm 1 AES pseudocode algorithm

Input: Plaintext state array *State* of size 128 bits, encryption key *key*, number of rounds n_r

Output: Ciphertext *cp* of size 128 bits

```
AddRoundKey(State, RoundKey_0);                                  First Round
for round = 0 to n_r − 1 do
    SubBytes(State)                  ▷ substitute each byte;     Main Round
    ShiftRows(State)                 ▷ rotates bytes in a word;
    MixColumns(State)                ▷ combine bytes in a column;
    AddRoundKey(State, RoundKey_i)   ▷ XOR the round key;
end
SubBytes(State);                                                 Last Round
ShiftRows(State);
AddRoundKey(State, RoundKey_nr);
```

2.2 cryptanalysis

Cryptanalysis leverages mathematical techniques to analyze the cryptographic scheme and identify potential algorithm vulnerabilities at a logical level.
The metrics that define cryptanalysis resistance are:

- **Nonlinearity:** defined in [6], it evaluates the deviation of the crypto function from affine functions (functions of the form $f(x) = Ax + b$). Higher nonlinearity means better resistance to linear cryptanalysis.
- **Differential Uniformity:** defined in [6], it evaluates how uniformly changes in the input are reflected as uniform changes in the output. This is measured through the Differential Distribution Table (DTT). A lower differential uniformity value indicates better resistance to differential cryptanalysis.
- **Confusion coefficient:** defined in [1], it measures the confusion introduced by a cryptographic function; in Shannon's terms, confusion is the ability to mix the input bits to obscure the relationship between input and output.

2.3 Correlation Power Analysis

Correlational power analysis (CPA) [5] is a statistical technique that correlates device power consumption with the value of the intermediate state we are interested in recovering. The underlying assumption is that the data processed by the device predictably contributes to its overall power consumption. This leakage can be represented by a leakage model, with the two most commonly used ones being:

- **Hamming Weight (HW):** This model assumes that the power consumed by a device is proportional to the number of bits set to '1' in the state.
- **Hamming Distance (HD):** This model correlates power consumption with the number of bit transitions between consecutive states, offering a more accurate representation of dynamic power consumption than the HW.

Pearson's correlation coefficient is used to relate the actual measured power consumption with the predicted power consumption [7]. Given N collected power traces, where each trace T_i consists of S sample points, the correlation coefficient of n-th key candidate, with power estimation $h_{i,n}$, can be computed as follows:

$$\rho(n) = \frac{\sum_{i=1}^{N}[(h_{i,n} - \overline{h_i})(T_{i,n} - \overline{T_i})]}{\sqrt{\sum_{i=1}^{N}(h_{i,n} - \overline{h_i})^2}\sqrt{\sum_{i=1}^{N}(T_{i,n} - \overline{T_i})^2}}$$

Here, $\overline{T}$ is the mean value of the measured power traces, and $\overline{h}_n$ is the mean value of the predicted power consumption for the n-th key candidate.
The most likely subkey candidate is the one with the highest correlation.

3 Proposed approach

The proposed analysis consists of evaluating each of the selected SBox structures individually. The AES-128 RTL implementation is modified by replacing the standard SBox structure with the one under attack.
The attack consists of two phases:

- **Online capture:** The AES IP is synthesized on the target board. Once programmed, the board executes AES encryption and triggers the oscilloscope to capture the power consumption of the DUT during the encryption process
- **Offline analysis:** The captured power traces are fed to a correlation power analysis algorithm. Based on the leakage model provided, the CPA algorithm can statistically infer the secret key.

3.1 S-Box Variants

The attack is carried out on six different S-Boxes, including the standard Rijndael S-Box used as a reference. The other S-Boxes are selected from recent publications for their claimed resistance to side-channel analysis. Three reference S-Boxes are presented in [8] and specifically target resistance to power-analysis attacks. The fifth selected S-Box was originally proposed by Özkaynak [9] and tested by Açikkapi [10] with an attack similar to the one presented in this current work, but tested within the AES software implementation. Finally, the last reference S-Box [11] exhibits strong properties against cryptanalysis but lacks specific design criteria for side-channel resistance.

3.2 Leakage model

The power measured on the Device Under Test (DUT) is the sum of multiple contributions: the power consumption depending on the target secret data $Sdata$ (P_{Sdata}), the power noise due to the measurement setup (P_{Noise}) and power deriving from the other operations processed by the DUT ($P_{algoNoise}$).

$$P_{total}(Sdata, t) = P_{Noise}(t) + P_{algoNoise} + P_{Sdata}(Sdata, t) \quad (1)$$

In the case where the internal algorithm or architecture is known, i.e. a white/grey box implementation, it is possible to identify the point at which the measured

power is highly dependent on known inputs and the internal state of the cryptographic algorithm we are trying to recover. This can be done by measuring the Signal to Noise Ratio (SNR). The SNR measures the 'quality' of the power trace obtained for a deterministic input over the noise. As shown in Fig. 1, the

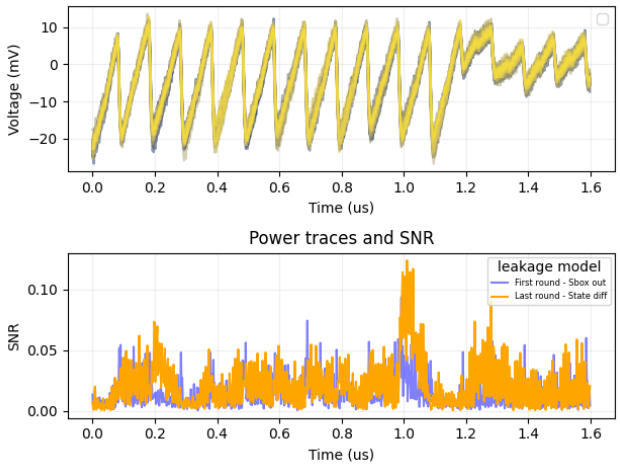

Fig. 1: Power traces and SNR of leakage models (*Sbox_out* and *State_diff*)

SNR depending on the ciphertext is maximum in the *Last Round*. There is also information leakage due to the plaintext in the *First Round*, but it is less evident than the aforementioned one. This is to be expected since in ASIC there is a significant power leakage when the intermediate state is stored in a register, and in the *Last Round* of AES, there is no $MixColumns$ operation, which allows attacking a single key byte at a time.
The power signature of the *Last Round* is proportional to the state difference between the 9th and 10th rounds: hence, it depends solely on the key (the target) and the known ciphertext. When dealing with state differences, it is convenient to use the Hamming distance as the leakage model [5].

4 Experiments and results

4.1 Experimental setup

The attack is performed on the CW305 platform from NewAE's ChipWhisperer [1], which is designed for side-channel analysis on FPGAs. This board mounts a Xilinx Artix-7 FPGA, power measurement points for the core voltage ($VCCINT$), and a USB interface for programming and communication with the architecture or IP implemented on the FPGA. The implemented AES core runs at 10MHz and is memory mapped; its register file can be configured through a set of Python APIs that permit also to start the processing.
The device employed to capture the DUT's power is a Picoscope digital oscilloscope (5000 model). It waits for the trigger and, once received, it starts to

[1] https://www.newae.com/products/nae-cw305

SBox	Power analysis resistance		Cryptanalysis resistance		
	PGE < 10		**Non**	**Differential**	**Confusion**
	AES HW	AES SW [13]	**Linearity**	**Uniformity**	**Coefficient**
Rijandael	∼ 800 traces	∼ 55 traces	112.0	4/256	0.111
$Freyre_1$ [8]	∼ 1190 traces	∼ 190 traces	100.0	8/256	4.500
$Freyre_2$ [8]	∼ 2000 traces	∼ 520 traces	100.0	8/256	4.492
$Freyre_3$ [8]	∼ 1340 traces	∼ 43 traces	102.0	8/256	1.934
$Ozkaynak_1$ [9]	∼ 1750 traces	∼ 49 traces	106.7	10/256	0.103
$Hussain_6$ [11]	∼ 1290 traces	∼ 46 traces	112.0	4/256	0.111

Table 1: Trade-off between the cryptanalytic properties and PGE threshold

measure the $VCCINT$ probe with a sampling frequency f_s of $390\,\mathrm{MS\,s^{-1}}$.
The AES-128 encryption process commences with the writing of the plaintext and the start bit in the register file via the Python API. Concurrently, the trigger is provided to the oscilloscope. Once the traces have been acquired, the offline analysis phase starts and the correlation power analysis algorithm is performed. This returns a ranked list of subkey candidates, ordered according to the estimated probability, which is derived from the statistical test results.

4.2 Results discussion

The results presented here are derived from the analysis of 2500 executions. The likelihood of identifying the correct subkey increases with the number of traces analyzed, as noise can be more effectively filtered out.
Two metrics [1] are used to evaluate side-channel resistance:

- **Partial Guessing Entropy (PGE):** This metric measures the distance, in terms of ranking positions, of the correct subkey from the top-ranked subkey candidates. A higher inherent resistance of the SBox results in a lower ranking of the correct subkey.
- **Correlation:** It is the value obtained by Pearson's linear correlation function and ranges from a minimum of 0 to a maximum of 1.

An empirical indicator of secret key disclosure is when the PGE is below 10, as proposed by O'Flynn and Chen [12]. When $PGE < 10$, all 16 correct key bytes are within the top 10 positions, enabling an attacker to easily recover the secret key through a reduced key search with brute force. The results obtained and the comparison with the ones found with the AES software implementation [13] are presented in Table 1. The table also shows the cryptanalytic properties of each SBox. As observed by Prouff [1] the SBox properties that strengthen its resistance to power-analysis attacks contrast with those used to design cryptanalysis secure SBox. Carlet et al. [4] highlighted that mitigating side-channel attacks by reducing Hamming weight and distance of the SBox transformation results in

zero nonlinearity, thus severely compromising cryptanalysis resistance.
As anticipated, the original AES S-Box demonstrates vulnerability to correlation power analysis revealing nearly the whole key after just 800 executions.
The S-Box with the best outcome is $Feyre_2$. The structure design exhibits superior side-channel resistance compared to the other S-Boxes, while simultaneously satisfying nonlinearity and differential properties.
To gain a deeper understanding of the power analysis attack trend, it is helpful to compare the PGE and correlation trend of the original AES S-Box (Rijndael) with those from $Freyre_2$. As illustrated in Figure 2, for the Rijndael S-Box, 15 out of the 16 subkeys were entirely revealed after about 650 traces. At this point, 15 subkeys exhibited a PGE value equal to 0, indicating the correct key candidates were leading the ranking. Concerning the correlation trend of the Rijndael S-Box, it can be observed that the correct subkeys are clearly distinguished from the incorrect ones. This indicates that the attack can reconstruct the secret key used. In contrast, the $Freyre_2$ S-Box exhibits a tangled representation of all potential subkey candidates.

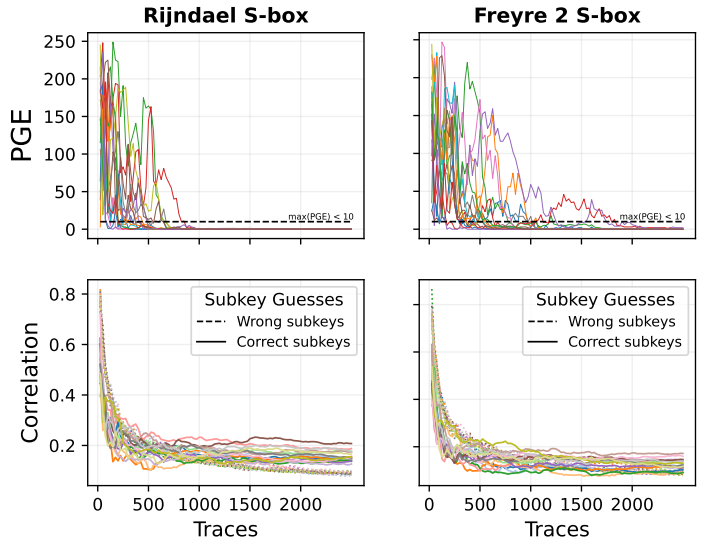

Fig. 2: Trend of PGE and correlation for *Rijndael* S-Box and $Freyre_2$ S-Boxes

5 Conclusion

Given the increasing demand for lightweight side-channel countermeasures, this paper explores novel S-Box designs that meet these needs without compromising performance or implementation area.
The attack on the AES hardware implementation highlighted the inadequate performance of the original AES S-Box in resisting side-channel attacks. This paper demonstrates that S-Box structures not designed with side-channel resistance in mind fail to provide adequate protection. Among the tested designs,

the $Freyre_2$ S-Box demonstrated the highest side-channel resistance, improving resistance by a factor 2.5 in hardware and by a factor 10 in software compared to the original S-Box. Interestingly, designs with higher Confusion Coefficients (CC) showed better resistance to power analysis attacks.
The $Freyre_2$ solution effectively mitigates attacks by increasing the time required to compromise the device, thus enhancing security. The trade-off between cryptanalysis and side-channel resistance represents a viable design strategy for lightweight side-channel countermeasures.

Acknowledgments. This work was funded by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

1. Prouff, Emmanuel. "DPA attacks and S-Boxes." International Workshop on Fast Software Encryption. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.
2. Carlet, Claude. "On highly nonlinear S-boxes and their inability to thwart DPA attacks." International Conference on Cryptology in India. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.
3. Guilley, et al. "Differential power analysis model and some results." Smart Card Research and Advanced Applications VI: IFIP 18th World Computer Congress TC8/WG8. 8 TC11/WG11. 2 Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS) 22–27 August 2004 Toulouse, France. Springer US, 2004.
4. Carlet, et al. "Trade-offs for S-boxes: Cryptographic properties and side-channel resilience." Applied Cryptography and Network Security: 15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017, Proceedings 15. Springer International Publishing, 2017.
5. Kocher, Paul, et al. "Introduction to differential power analysis." Journal of Cryptographic Engineering 1 (2011): 5-27.
6. De Canniere, et al. "An introduction to block cipher cryptanalysis." Proceedings of the IEEE 94.2 (2006): 346-356.
7. Prouff, et al. "Theoretical and practical aspects of mutual information based side channel analysis." Applied Cryptography and Network Security: 7th International Conference, ACNS 2009, Paris-Rocquencourt, France, June 2-5, 2009. Proceedings 7. Springer Berlin Heidelberg, 2009.
8. Freyre-Echevarría, Alejandro, et al. "Evolving nonlinear S-boxes with improved theoretical resilience to power attacks." IEEE Access 8 (2020): 202728-202737.
9. Özkaynak, Fatih. "Construction of robust substitution boxes based on chaotic systems." Neural Computing and Applications 31.8 (2019): 3317-3326.
10. Açikkapi, et al. "Side-channel analysis of chaos-based substitution box structures." IEEE Access 7 (2019): 79030-79043.
11. Hussain, Iqtadar, et al. "An efficient approach for the construction of LFT S-boxes using chaotic logistic map." Nonlinear Dynamics 71 (2013): 133-140.
12. O'Flynn, Colin, and Zhizhang Chen. "Synchronous sampling and clock recovery of internal oscillators for side channel analysis and fault injection." Journal of Cryptographic Engineering 5 (2015): 53-69.
13. Cerini, Samuele Yves. Empirical evaluation of the resilience of novel s-box implementations against power side-channel attacks. Available at https://webthesis.biblio.polito.it/18156/ Diss. Politecnico di Torino, 2021.