Improving DPA Resistance of S-boxes: How far can we go?

Barış Ege, Kostas Papagiannopoulos, Lejla Batina
Digital Security Group - ICIS
Radboud University Nijmegen

Stjepan Picek
Faculty of Electrical Engineering and Computing
University of Zagreb

***Abstract*—Side-channel analysis (SCA) is an important issue for numerous embedded cryptographic devices that carry out secure transactions on a daily basis. Consequently, it is of utmost importance to deploy efficient countermeasures. In this context, we investigate the intrinsic side-channel resistance of lightweight cryptographic S-boxes. We propose improved versions of S-boxes that offer increased power analysis resistance, whilst remaining secure against linear and differential cryptanalyses. To evaluate the side-channel resistance, we work under the Confusion Coefficient model [1] and employ heuristic techniques to produce those improved S-boxes. We evaluate the proposed components in software (AVR microprocessors) and hardware (SASEBO FPGA). Our conclusions show that the model and our approach are heavily platform-dependent and that different principles hold for software and hardware implementations.**

I. Introduction and Previous work

Starting with the seminal paper of Kocher et al. [2], the topic of differential power analysis (DPA) has been attracting interest from both the industry and the academia. Its popularity stems from the effectiveness of these attacks in recovering the secret keys of smart devices, even when they are protected with state-of-the-art cryptographic algorithms. DPA and physical attacks in general exploit the link between the secret data processed in a device and some unintentional leakage in the physical implementation (side-channel information). Side-channel information can be extracted from a multitude of physical mediums such as power consumption, timing variations and electromagnetic emanations. This physical information allows the adversary to perform the so-called side-channel attacks, often with devastating effects on the device security.

Given the high impact of side-channel analysis, the research community has developed a plethora of countermeasures, ranging from device-based solutions often categorized as *hiding* (noise amplification, power supply filter, EM shield) to algorithmic-based solutions such as *masking* [3]. In a similar context, this work first evaluates the SCA vulnerabilities of basic building blocks i.e. S-boxes. Specifically, we investigate the current S-boxes used by lightweight ciphers such as PRESENT [4] and PRINCE [5] and suggest improved versions that are more resistant to DPA, while maintaining resistance to traditional cryptanalytic techniques. Our final goal is to establish an innovative algorithmic countermeasure that would favor certain choices of S-boxes by exploiting the *intrinsic* side-channel resistance of cryptographic primitives.

This work was supported in part by the Technology Foundation STW (project 12624 - SIDES), The Netherlands Organization for Scientific Research NWO (project ProFIL 628.001.007) and the ICT COST action IC1204 TRUDEVICE.

We have identified two main obstacles when crafting a side-channel resistant cryptographic primitive: the *theoretical–physical tradeoff* and the *resistance quantification* problem.

Theoretical–physical tradeoff. The resistance of a cryptographic algorithm to theoretic attacks such as linear [6] and differential [7] cryptanalysis is a well studied area. However, it has been shown that the *inherent* side-channel resistance of a cipher component is inversely proportional to the component's resistance against linear and differential attacks [8], [9]. The tradeoff is linked to the non-linearity property: having strong non-linearity increases the theoretical security, whilst making side-channel cryptanalysis easier. As a result, non-linear cipher components such as the S-box present good targets for a side-channel attack.

Resistance quantification. The quantification problem lies in finding a reliable and stand-alone metric of the S-box's behavior under SCA. Several works in the literature attempt to quantify the resistance of a block cipher implementation against power analysis. Guilley and Pacalet propose Signal to Noise Ratio in DPA as the first proposal to measure the level of leakage expected from a design [8]. Given the prevalence of S-boxes as non-linear cipher building blocks, Prouff proposes "transparency order", attempting to evaluate different S-boxes w.r.t. DPA resistance. This metric attracted attention from researchers, yet the attainable level of improvement (in terms of side-channel security) seems to be platform-dependent. Elaborating on this conclusion, Mazumdar et al. have generated new S-boxes following the transparency order definition. They performed an experimental verification on an FPGA [10], [11] and their work presented a substantial improvement in the number of measurements required until the recovery of the secret key. On the other hand, Picek et al. showed that a such increase in the level of security is not observed when considering 8×8 S-boxes in software implementations [12]. The situation is somewhat different when 4×4 S-boxes are examined, since it is possible to achieve much bigger differences in the transparency order values [13]. Yet again, a closer look at the practical analysis shows that the increase in security against DPA does not go hand-in-hand with an improved transparency order. Finally, Chakraborty et al. presented limitations to Prouff's "transparency order" and proposed amendments to the metric [14].

In this paper, we investigate whether a single S-box can be generated to resist side-channel analysis in both software and hardware platforms. Our results prove this being a complex question and the differences in the ways we model leakages for software and hardware imply the variability in the "measured"

978-1-4799-8391-9/15/$31.00 ©2015 IEEE

SCA resistance for the two cases.

The paper is organized as follows: we discuss the theoretical background in Sect. II and describe the resistance quantification and the generation of the improved S-box. We continue with the experimental results on AVR ATmega microcontroller and SASEBO FPGA board in Sect. III. We conclude in Sect. IV.

II. Background

Analyzing individual S-boxes requires an evaluation metric/model that clearly separates the effect of the physical characteristics of the device under attack (such as noise) from the algorithmic effect of the cipher/component that we target. For this purpose, we use the Confusion Coefficient model as proposed by Fei et al. [1], [15].

The suggested model is closely related to the selection function (sometimes also called the sensitive variable) that we use to perform the attack. In this work, we attack a software, lookup-table-based implementation of a PRESENT-like[1] cipher. We use a 4×4 S-box, our target intermediate value is the S-box output and the power model we use is the Hamming weight (HW) of the intermediate value. Thus, the selection function f is the following:

$$f(input, key) = HW(Sbox(input \oplus key)) \quad (1)$$

Given two different keys k_1, k_2, where $k_1 \neq k_2$, Fei et al. [1] define the confusion coefficient κ:

$$\kappa(k_1, k_2) = E[(f(input, k_1) - f(input, k_2))^2] \quad (2)$$

where E denotes the expected value of $(f(input, k_1) - f(input, k_2))^2$ over all possible inputs. The resulting $\kappa(k_1, k_2)$ describes the effect of an algorithmic confusion: a large value indicates that it is easy to distinguish between keys k_1, k_2 if you perform a side-channel attack with the selection function f. In general, the coefficient $\kappa(k_i, k_j)$ demonstrates the probability of distinguishing between two keys.

In order to fully characterize the behavior of the selection function f (and as a result the behavior of the S-box), we need to compute all possible values of κ. After acquiring all possible κ values, we proceed in crafting the *frequency distribution of the confusion coefficients* for the chosen S-box.

For a given size of the target selection function (e.g. the HW of the 4-bit S-box output specified in Eqn. (1), the mean of the frequency distribution remains constant. According to Heuser et al. [9], highly non-linear components lead to a frequency distribution with low variance, compared to linear elements, which demonstrate high variance. As a result, in order to improve side-channel resistance, we need to search for S-boxes whose frequency distributions demonstrate high variance. To this end, we employ heuristic techniques (for full description see [16]) such as genetic algorithms that generate new S-boxes with high distribution variance, yet sufficient resistance to linear and differential cryptanalysis.

[1]We refer to the cryptographic primitive as PRESENT-like because we create 2 instances of the cipher: one with the original PRESENT S-box and one with the improved S-box.

TABLE I. Variance of the confusion coefficient computed for different S-boxes.

	PRESENT	Phantom	New
$var(\kappa)$	0.6600	1.3880	1.3629

Following the heuristics we have generated two "improved" S-boxes the so-called "Phantom" and "New" that are defined as follows:

Phantom = {6, 4, 7, 8, 0, 5, 2, 10, 14, 3, 13, 1, 12, 15, 9, 11}
New = {15, 11, 8, 4, 2, 0, 14, 13, 9, 3, 1, 5, 12, 10, 7, 6}

The first "improved" S-box demonstrates an increased variance of the frequency distribution (see Table I), when compared to the original S-box, while it remains in the "optimal" S-box classes as defined by Leander et al. [17]. The improved S-box actually exhibits increased resistance (resembling the behavior of a linear element). However, it results in ghost peaks during our SCA (see Section III), thus, we refer to it as the "Phantom S-box".

The "New" S-box, on the other hand, does not result in ghost peaks in a software setting and in fact has a lower variance of the distribution of the confusion coefficient when compared to the Phantom S-box (see Table I). Nevertheless, when implemented on hardware, this S-box yielded the best results in our experiments presented in Section III.

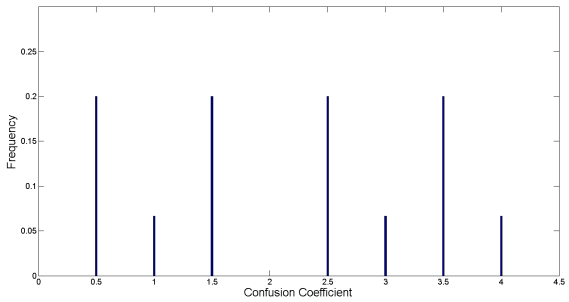

Fig. 1. Confusion coefficient frequency distribution for the improved PRESENT S-box

III. Results and Experiments

In this section, we investigate experimentally if the "Phantom" S-box (first introduced by Picek et al. [16]) provides increased security in a real world setting (software and hardware). Rather than implementing only the S-box lookup for testing purposes, we take the more realistic approach of embedding the S-box in PRESENT cipher [4]. Note that the confusion coefficient (and its distribution) is computed using the selection function of a given cryptographic algorithm. In section II we demonstrated that it is possible to use heuristics in order to generate S-boxes resistant to a *specific* selection function. Namely, the "Phantom" S-box was tailor-made to be resistant to the selection function f that is used in attacks on software PRESENT implementations. Thus, it is of direct interest to verify whether this holds in AVR software implementations (III-A) and also investigate its behavior in an FPGA context (III-B).

Our choice of PRESENT is motivated by its standardization as a lightweight block cipher with a 4×4 S-box [18]. PRESENT employs the substitution permutation network (SPN) design: the S-Layer is formed of 4×4 S-box lookups to provide non-linearity, and the P-Layer is a bit permutation that ensures diffusion.

A. Software (AVR)

For software analysis, we chose an AVR smartcard with an ATmega163 microcontroller. We used Riscure Power Tracer 3 to communicate with the smartcard and extract the power consumption traces using a LeCroy WaveRunner 610Zi Oscilloscope. We acquired 2 500 traces and using the low-noise measurements supplied by the Power Tracer, run 50 independent experiments (with 50 traces each) to generate the guessing entropy plot presented in Figure 2. The ATmega163 microcontroller leaks the Hamming weight of the intermediate values and naturally, we choose the selection function f as specified in Eqn. (1).

As shown in Figure 2, the "Phantom" [16] behavior prevents the attack to be 100% successful. The phantom behavior can be summarized as follows: for a given phantom $n \times n$ S-box, there exists a constant c_p such that when two inputs to the S-box have the XOR difference of c_p in between, sum of Hamming weight values of the outputs will add up to n. In the current case, since the Hamming weight of the S-box outputs add up to 4, the attacker cannot be certain that the top candidate is in fact the correct one without precise knowledge of how the target device leaks data. An example to the mentioned property of the phantom S-box, where $c_p = \texttt{0x9}$, is as follows:

$$\begin{aligned} Inp_1 &= \texttt{0x4} \\ Inp_2 &= \texttt{0x4} \oplus \texttt{0x9} = \texttt{0xC} \\ Out_1 = S(Inp_1) &= \texttt{0x0} \rightarrow \mathrm{HW}(\texttt{0x0}) = 0 \\ Out_2 = S(Inp_2) &= \texttt{0xF} \rightarrow \mathrm{HW}(\texttt{0xF}) = 4. \end{aligned}$$

In other words, phantom behavior of an S-box sometimes implies wrong conclusions in terms of SCA resistance for the reason outlined above.

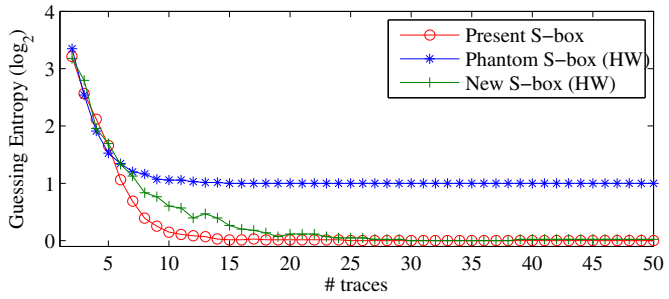

Fig. 2. Guessing entropy with respect to the number of processed traces.

B. Hardware (FPGA)

For Hardware analysis we chose to use the SASEBO board with a XILINX Virtex-II Pro (XC2VP7) FPGA for running the PRESENT design. The block diagram of the design we implemented in FPGA is given in Fig. 3. As shown in the figure, the data register is updated at each round only once. This makes the selection function g slightly more complicated than the one used in the software case. When attacking from the input, rather than simply computing the Hamming weight of the S-box output, we need to put the values through the P-layer and compute which bit positions in the data register are affected. Then, we compute the Hamming distance (HD) between the old and new register state, in order to estimate the power consumption

$$\begin{aligned} g(input, key) = HD(R_{old}, R_{new}) = \\ HD(R_{old}(0, 16, 32, 48), P(S(R_{old}(0, 1, 2, 3) \oplus key). \end{aligned} \quad (3)$$

We emphasize again the fact that the improved S-box was crafted for the software selection function f, based on the Hamming weight leakage assumption.

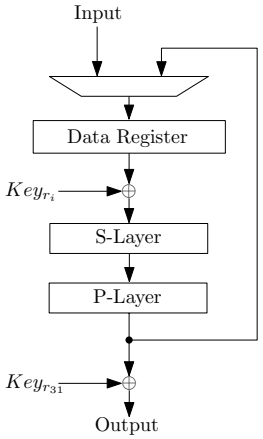

Fig. 3. Block diagram of the implemented PRESENT cipher core.

For the experiments, we acquired a total of 150 000 traces for the new S-box we generated, 70 000 traces for the phantom S-box, and 50 000 traces for the original PRESENT using a LeCroy WaveRunner 610Zi oscilloscope. To compute the guessing entropy diagram [19], ten separate attacks are run and the results obtained from the attacks are summarized in Figure 4. As it is clearly visible in the figure, the behavior

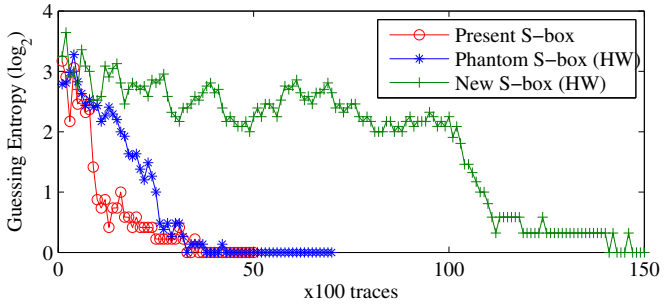

Fig. 4. Guessing entropy with respect to the number of processed traces.

of the phantom S-box in an FPGA implementation is rather similar compared to the behavior of the original PRESENT S-box. Thus, we observe that an S-box crafted to reduce the Hamming weight leakage has negligible effect when applied in a context where Hamming distance leakage is prevalent. On

the other hand, the new S-box given in Section II acts rather different when compared to phantom and original PRESENT S-boxes. From these experiments we can deduce that improved security (in terms of SCA resistance) for a particular leakage model does not necessarily imply adequately improved security in another setting.

IV. Conclusion

In this work, we have investigated the security of an S-box, which is generated to provide improved side-channel security in a software setting, when it is taken out of context and analysed in a hardware setting. The results show that in the case of PRESENT-like SPN-ciphers, security in software environment does not imply security in a hardware environment. On the contrary, when an S-box with a lower confusion coefficient variance (in terms of Hamming weight leakage) is generated, one may get improved security on an FPGA. Hence, the search for the "silver bullet" when it comes to DPA resistant S-boxes which provide security in both software and hardware remains an open problem.

References

[1] Y. Fei, A. A. Ding, J. Lao, and L. Zhang, "A Statistics-based Fundamental Model for Side-channel Attack Analysis," *IACR Cryptology ePrint Archive*, vol. 2014, p. 152, 2014.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology - CRYPTO'99*, ser. LNCS, no. 1666. Springer-Verlag, 1999, pp. 388–397.

[3] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.

[4] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," in *Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems CHES '07*, ser. LNCS. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 450–466.

[5] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. Thomsen, and T. Yalçin, "PRINCE : A Low-Latency Block Cipher for Pervasive Computing Applications," in *Advances in Cryptology: ASIACRYPT 2012*, ser. LNCS. Springer Berlin Heidelberg, 2012, vol. 7658, pp. 208–225.

[6] M. Matsui and A. Yamagishi, "A new method for known plaintext attack of FEAL cipher," in *Proceedings of EUROCRYPT'92*, ser. LNCS. Berlin, Heidelberg: Springer-Verlag, 1993, pp. 81–91.

[7] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," in *Proceedings of CRYPTO '90*, ser. LNCS. London, UK: Springer-Verlag, 1991, pp. 2–21.

[8] S. Guilley and R. Pacalet, "Differential Power Analysis Model and Some Results," in *In proceedings of CARDIS 2004*. Kluwer Academic Publishers, 2004, pp. 127–142.

[9] A. Heuser, S. Guilley, and O. Rioul, "A Theoretical Study of Kolmogorov-Smirnov Distinguishers: Side-Channel Analysis vs. Differential Cryptanalysis," *IACR Cryptology ePrint Archive*, vol. 2014, p. 8, 2014.

[10] B. Mazumdar, D. Mukhopadhay, and I. Sengupta, "Constrained Search for a Class of Good Bijective S-Boxes with Improved DPA Resistivity," *Information Forensics and Security, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2013.

[11] B. Mazumdar, D. Mukhopadhyay, and I. Sengupta, "Design and implementation of rotation symmetric S-boxes with high nonlinearity and high DPA resilience," in *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*, 2013, pp. 87–92.

[12] S. Picek, B. Ege, L. Batina, D. Jakobovic, L. Chmielewski, and M. Golub, "On Using Genetic Algorithms for Intrinsic Side-channel Resistance: The Case of AES S-box," in *Proceedings of the First Workshop on Cryptography and Security in Computing Systems*, ser. CS^2 '14. New York, USA: ACM, 2014, pp. 13–18.

[13] S. Picek, B. Ege, K. Papagiannopoulos, L. Batina, and D. Jakobovic, "Optimality and beyond: The case of 4x4 s-boxes," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2014, Arlington, VA, USA, May 6-7, 2014*, 2014, pp. 80–83.

[14] K. Chakraborty, S. Maitra, S. Sarkar, B. Mazumdar, and D. Mukhopadhyay, "Redefining the Transparency Order," Cryptology ePrint Archive, Report 2014/367, 2014, http://eprint.iacr.org/.

[15] Y. Fei, Q. Luo, and A. A. Ding, "A Statistical Model for DPA with Novel Algorithmic Confusion Analysis," in *Proceedings of the 14th International Workshop on Cryptographic Hardware and Embedded Systems CHES '12*, ser. LNCS, 2012, pp. 233–250.

[16] S. Picek, K. Papagiannopoulos, B. Ege, L. Batina, and D. Jakobovic, "Confused by confusion: Systematic evaluation of dpa resistance of various s-boxes," in *Progress in Cryptology – INDOCRYPT 2014*, ser. Lecture Notes in Computer Science, W. Meier and D. Mukhopadhyay, Eds. Springer International Publishing, 2014, pp. 374–390.

[17] G. Leander and A. Poschmann, "On the Classification of 4 Bit S-Boxes," in *Arithmetic of Finite Fields*, ser. LNCS. Springer Berlin Heidelberg, 2007, vol. 4547, pp. 159–176.

[18] ISO/IEC 29192-2:2012, "Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers," 2012.

[19] F.-X. Standaert, T. G. Malkin, and M. Yung, "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks," in *Proceedings of the 28th Annual International Conference on Advances in Cryptology: The Theory and Applications of Cryptographic Techniques EUROCRYPT '09*, ser. LNCS. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 443–461.