

# Comparing Sboxes of Ciphers from the Perspective of Side-Channel Attacks

Liran Lerman and Olivier Markowitch and Nikita Veshchikov  
Quality and Security of Information Systems,  
Université libre de Bruxelles, Belgium  
{liran.lerman, olivier.markowitch, nikita.veshchikov}@ulb.ac.be

**Abstract**—Side-channel attacks exploit physical characteristics of implementations of cryptographic algorithms in order to extract sensitive information such as the secret key. These physical attacks are among the most powerful attacks against real-world crypto-systems. This paper analyses the non-linear part (called Sboxes) of ciphers, which is often targeted by implementation attacks. We analyse Sboxes of several candidates that were submitted to the competition on authenticated encryption (CAESAR) as well as several other ciphers. We compare theoretical metrics with results from simulations and with real experiments. In this paper, we demonstrate that, in some contexts, the theoretical metrics provide no information on the resiliency of the Sboxes against side-channel attacks.

## I. INTRODUCTION

Cryptanalysis confronts symmetric-key cryptographic primitives by attempting to circumvent their security feature. Theoretical cryptanalysis, which relies only on the mathematical basis of the cryptographic algorithm, try to extract the secret information in a black-box manner (e.g., by taking into account the plaintexts and the ciphertexts of block-ciphers). Since the ground-breaking work of Kocher [1], the cryptanalysts also examine physical characteristics (called leakages or traces) related to the execution of the implementation of cryptographic algorithms. The rationale is that there is a relationship between the manipulated data (e.g., the secret key), the executed operations and the physical properties observed during the execution of the cryptographic algorithm by a device. A side-channel attack represents a process that exploits leakages in order to extract sensitive information such as the key. We focus on side-channel attacks based on the power consumption leakage as this physical property is pretty easy to measure.

The evaluation metrics of cryptographic algorithms against physical attacks represent an active research area. Several metrics exist such as the (improved) transparency order [2] and the confusion coefficient [3]. The various evaluation metrics and the impressively growing number of leakage resilient cryptographic primitives highlight that we still lack knowledge on what represents a primitive resilient to physical attacks. See for example the recently published paper of Taha *et al.* [4] on a side-channel resilient key generator that was successful attacked by Dobraunig *et al.* [5] few months later.

In this paper, through several experiments, we demonstrate that the two well known metrics lack accuracy to evaluate

the resistance of cryptographic primitives against side-channel attacks. The serious consequences of such result is that (1) the evaluation laboratories of cryptographic implementations still require to apply side-channel attacks in order to discover the security level provided by cryptographic devices, and (2) the new cryptographic primitives taking into account these evaluation metrics during the design process may be compromised in front of side-channel attacks.

The rest of the paper is organised as follows. Section II contains preliminary notions on physical attacks and on theoretical metrics evaluating the resiliency of Sboxes against side-channel attacks. Section III provides the results based on the theoretical metrics (in Section III-A), on simulated scenarios (in Section III-B), and on a real device (in Section III-C). Finally, Section IV concludes the paper.

## II. PRELIMINARY NOTIONS

Let  $\mathbb{F}_2^n$  be the vector space that contains all the  $n$ -bit binary vectors. Let  $F$  be a substitution box (denoted Sbox). Sboxes provide the confusion property in cryptographic primitives by substituting values from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2^m$  (denoted an Sbox  $n \times m$ ). The Sbox can be seen as a vector of  $m$  Boolean functions  $[F_1, F_2, \dots, F_m]$  where each Boolean function represents a mapping from  $\mathbb{F}_2^n$  to  $\mathbb{F}_2$ .

Several side-channel attacks exist such as the Correlation Power Analysis (CPA) [6], template attacks [7], and machine learning based attacks [8]. Due to its simplicity and efficiency, in the following, we focus on the CPA approach, leaving the other techniques as a future work. CPA recovers the secret key from a cryptographic device by selecting the key that maximises the dependence between the actual leakage and the estimated leakage based on the assumed secret key. More precisely, CPA selects the secret key  $\hat{k}$  such that:

$$\hat{k} \in \arg \max_{k \in \mathcal{K}} \left\| \rho \left( \widehat{\mathcal{T}}_{(k)}, \mathcal{T} \right) \right\|, \quad (1)$$

where  $\|x\|$  symbolises the absolute value of  $x$ ,  $\rho(\mathcal{X}, \mathcal{Y})$  represents the Pearsons correlation between two lists  $\mathcal{X}$  and  $\mathcal{Y}$ , and:

- $\mathcal{T} = [{}^{(1)}T, \dots, {}^{(N_a)}T]$  represents a list of  $N_a$  traces measured when the target device manipulates the Sbox,
- $\widehat{\mathcal{T}}_{(k)} = [\widehat{L}(F(k \oplus p_{[1]}), \dots, \widehat{L}(F(k \oplus p_{[N_a]}))]$  refers to a list of estimated leakages (with a leakage model  $\widehat{L}$ )

parameterised with the output of the Sbox combining (with the exclusive-or operation denoted  $\oplus$ ) an estimated key  $k$  and known plaintext  $p_{[i]}$  associated to  $(i)T$ .

The designers of cryptographic devices measure the resistance of an implementation against CPA by using (among others) the first order Success Rate (SR) [9]. The success rate (also known as the success probability) represents the probability that the physical attack extracts the secret key.

Following the work of Prouff on the transparency order [10], Chakraborty *et al.* mention that the improved Transparency Order metric (TO) evaluates the resiliency of an Sbox against side-channel attacks [2]. More precisely, the lower the TO metric, the lower the success probability to extract the secret key based on leakages associated to the SBox. Mathematically, the improved transparency order metric on an Sbox  $F$  (denoted  $TO(F)$ ) equals to

$$\max_{\beta \in \mathbb{F}_2^m} \left( m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^m \left\| \sum_{i=1}^m (-1)^{\beta_i \oplus \beta_j} \mathcal{C}_{F_i, F_j}(a) \right\| \right), \quad (2)$$

where  $\beta_i$  represents the value of the  $i$ -th bit of  $\beta$ , and

$$\mathcal{C}_{F_i, F_j}(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{F_i(x) \oplus F_j(x \oplus w)}. \quad (3)$$

The TO metric assumes that the leakage depends on  $HW(\beta \oplus F(a))$  where  $HW$  is the Hamming weight and  $\beta$  denotes the initial content of the register before updating with  $F(a)$ . Equation 2 iterates over all values of  $\beta \in \mathbb{F}_2^m$  in order to dissociate the transparency order metric from a specific device. The value of  $\beta$  maximising Equation 2 represents the worst case context when implementing the SBox (independently of the considered device). However, in practice, the strategy of the adversary depends on the target device. As a result, in our experiment, we also calculate the TO with  $\beta$  equal to zero which corresponds to our context in which the (analysed) microcontroller leaks the Hamming weight of the manipulated value. In the following, we denote  $TO_{max}$  when we go through all values of  $\beta$ , and  $TO_0$  when we fix  $\beta$  equal to 0.

In 2012, Fei *et al.* introduced another metric, called confusion coefficient (CC) and denoted  $\kappa$ , in order to evaluate the resistance of Sboxes against side-channel attacks [11], [3]. The CC metric computes a matrix containing in the  $i$ -th row and in the  $j$ -th column (denoted  $\kappa(k_i, k_j)$ ) the distance of the output of the SBox between the  $i$ -th and the  $j$ -th value of the key (denoted respectively  $k_i$  and  $k_j$ ), i.e.

$$\kappa(k_i, k_j) = E_p \left[ (L(F(k_i \oplus p)) - L(F(k_j \oplus p)))^2 \right], \quad (4)$$

where  $L$  represents the leakage function and  $E$  is the mean operator. The CC metric resumes this matrix by computing the variance (denoted  $\sigma^2[\cdot]$ ) of its values in the  $i$ -th row and the  $j$ -th column such that  $i < j$ , i.e.

$$CC = \sigma^2[\bar{\kappa}] = \sigma^2[\kappa(k_i, k_j) \mid \forall i < j], \quad (5)$$

where  $\bar{\kappa}$  denotes the list  $[\kappa(k_i, k_j) \mid \forall i < j]$ .

According to the authors of the CC metric [3], the Sbox with lower (standard) deviation of  $\kappa$  leads to a higher resistance of the Sbox against physical attacks. However, Picek *et al.* [12] as

well as Stoffelen [13] report that the higher the CC metric, the higher the resistance of the Sbox against side-channel attacks. Results of our experiments highlight that theoretical metrics (CC as well as TO) lack accuracy to evaluate the resistance of Sboxes against side-channel attacks.

### III. EVALUATION OF SBOXES

In 2013, the open cryptographic “*Competition for Authenticated Encryption: Security, Applicability, and Robustness*” (CAESAR) was launched by Bernstein in order to find a suitable portfolio of authenticated encryption with associated data primitives<sup>1</sup>. In this paper, we evaluate Sboxes used by CAESAR candidates as well as several additional well-known Sboxes. More precisely, we focus on the following 23 Sboxes:

- $4 \times 4$  Sboxes of Joltik [14], Prøst [15], Minalpher [16], PRESENT [17], Evolved<sub>CC</sub> [12] and Evolved<sub>TO</sub> [18];
- $5 \times 5$  Sboxes of ASCON [19], ICEPOLE [20], Keccak (Ketje, Keyak) [21], PRIMATE [22] and SC2000<sup>2</sup> [23];
- $6 \times 4$  Sboxes of DES [24] (labeled  $DES_i$ , with  $1 \leq i \leq 8$ );
- $8 \times 8$  Sboxes of SCREAM<sub>v3</sub> [25], STRIBOB [26], AES [27] and AES<sub>CC</sub> [12].

Picek *et al.* obtained the Sboxes Evolved<sub>CC</sub> and AES<sub>CC</sub> by using genetic algorithms optimising the confusion coefficient [12]. Later, the same authors built the Sbox Evolved<sub>TO</sub> using genetic algorithms optimising the (improved) transparency order [18].

In addition to the previous listed Sboxes, we created new  $8 \times 8$  Sboxes based on  $4 \times 4$  Sboxes. More precisely, we take into account the fact that an engineer can apply two Sboxes  $4 \times 4$  of the same primitive (which is equivalent to an  $8 \times 8$  Sbox) when the device applies the same  $4 \times 4$  Sbox on two 4-bit words of the same byte at once in order to substitute a byte. We call these (meta-)Sboxes Prøst <sub>$\times 2$</sub> , Minalpher <sub>$\times 2$</sub>  and PRESENT <sub>$\times 2$</sub> .

#### A. Results based on theoretical metrics

Table I reports the theoretical metrics CC and TO for each of the Sboxes<sup>3</sup>. The first observation on the TO metric is that big Sboxes lead to high coefficient and, as a result, lead to higher success probability of side-channel attacks. This result is expected since (1) the larger the Sbox the higher the nonlinearity, and (2) the higher the nonlinearity the higher the success probability as shown by Prouff [10]<sup>4</sup>. Interestingly, CC metric does not show such result, leading to a first contradiction between the two metrics.

Another observation relates to the order provided by the different metrics when sorting the Sboxes (of the same size) from the most resistive Sboxes to the least resistive. For example, in case of DES Sboxes, we have the following

<sup>1</sup><https://competitions.cr.ypt.to/caesar.html>

<sup>2</sup>The SC2000 also uses  $6 \times 6$  and  $4 \times 4$  Sboxes while we analysed the  $5 \times 5$  Sbox.

<sup>3</sup>Numbers for CC differ from the numbers by Stoffelen [13] since he assumed a fixed correct key while we computed CC for the entire range using the same algorithm as Picek *et al.* [12].

<sup>4</sup>Heuser *et al.* emphasised that the robustness of a function against SCA is not directly related to its non-linearity, but to its resistance to differential cryptanalysis [28].

| Size         | Sbox                    | TO         |        | CC                  |                   |
|--------------|-------------------------|------------|--------|---------------------|-------------------|
|              |                         | $TO_{max}$ | $TO_0$ | $\sigma^2[\bar{k}]$ | $\sigma[\bar{k}]$ |
| $8 \times 8$ | AES                     | 6.916      | 6.869  | 0.111               | 0.334             |
|              | AES <sub>CC</sub>       | 6.916      | 6.828  | 0.149               | 0.386             |
|              | SCREAM <sub>v3</sub>    | 6.854      | 6.792  | 0.122               | 0.349             |
|              | STRIBOB                 | 6.877      | 6.815  | 0.098               | 0.313             |
|              | Minalpher <sub>x2</sub> | 4.329      | 3.827  | 1.710               | 1.308             |
|              | PRESENT <sub>x2</sub>   | 4.643      | 3.765  | 1.710               | 1.308             |
|              | Prøst <sub>x2</sub>     | 4.643      | 4.580  | 1.051               | 1.025             |
| $6 \times 4$ | DES <sub>1</sub>        | 3.097      | 2.853  | 0.247               | 0.497             |
|              | DES <sub>2</sub>        | 2.960      | 2.960  | 0.136               | 0.369             |
|              | DES <sub>3</sub>        | 2.919      | 2.867  | 0.209               | 0.457             |
|              | DES <sub>4</sub>        | 2.984      | 2.984  | 0.172               | 0.414             |
|              | DES <sub>5</sub>        | 3.018      | 2.938  | 0.234               | 0.484             |
|              | DES <sub>6</sub>        | 3.004      | 2.665  | 0.363               | 0.602             |
|              | DES <sub>7</sub>        | 2.986      | 2.986  | 0.123               | 0.350             |
|              | DES <sub>8</sub>        | 3.115      | 2.927  | 0.164               | 0.405             |
| $5 \times 5$ | ASCON                   | 2.839      | 2.839  | 0.502               | 0.709             |
|              | ICEPOLE                 | 3.548      | 3.548  | 0.190               | 0.436             |
|              | Keccak                  | 3.871      | 3.871  | 0.115               | 0.338             |
|              | PRIMATE                 | 3.613      | 3.581  | 0.308               | 0.555             |
|              | SC2000                  | 3.548      | 3.363  | 0.260               | 0.510             |
| $4 \times 4$ | Evolved <sub>CC</sub>   | 2.500      | 1.533  | 1.388               | 1.178             |
|              | Evolved <sub>TO</sub>   | 1.900      | 1.700  | 1.262               | 1.124             |
|              | Joltik                  | 2.567      | 2.567  | 0.158               | 0.397             |
|              | Minalpher               | 2.300      | 2.033  | 0.660               | 0.812             |
|              | PRESENT                 | 2.467      | 2.000  | 0.660               | 0.812             |
|              | Prøst                   | 2.467      | 2.433  | 0.309               | 0.555             |

TABLE I: Modified Transparency Order (TO) and Confusion Coefficient (CC) metrics applied on Sboxes.

order according to (1) CC sorted according to Fei *et al.* [3] (denoted  $CC_{Fei}$ ), (2) CC sorted according to Picek *et al.* [12] and Stoffelen [13] (denoted  $CC_{Picek}$ ), (3)  $TO_0$ , and (4)  $TO_{max}$ :

- $CC_{Fei}$ : DES<sub>7</sub>, DES<sub>2</sub>, DES<sub>8</sub>, DES<sub>4</sub>, DES<sub>3</sub>, DES<sub>5</sub>, DES<sub>1</sub>, DES<sub>6</sub>;
- $CC_{Picek}$ : DES<sub>6</sub>, DES<sub>1</sub>, DES<sub>5</sub>, DES<sub>3</sub>, DES<sub>4</sub>, DES<sub>8</sub>, DES<sub>2</sub>, DES<sub>7</sub>;
- $TO_0$ : DES<sub>6</sub>, DES<sub>1</sub>, DES<sub>3</sub>, DES<sub>8</sub>, DES<sub>5</sub>, DES<sub>2</sub>, DES<sub>4</sub>, DES<sub>7</sub>;
- $TO_{max}$ : DES<sub>3</sub>, DES<sub>2</sub>, DES<sub>4</sub>, DES<sub>7</sub>, DES<sub>6</sub>, DES<sub>5</sub>, DES<sub>1</sub>, DES<sub>8</sub>.

We can notice that all metrics provide different ordering of Sboxes based on their resistance against side-channel attacks, meaning that the metrics are not equivalent.

### B. Experimental results on simulations

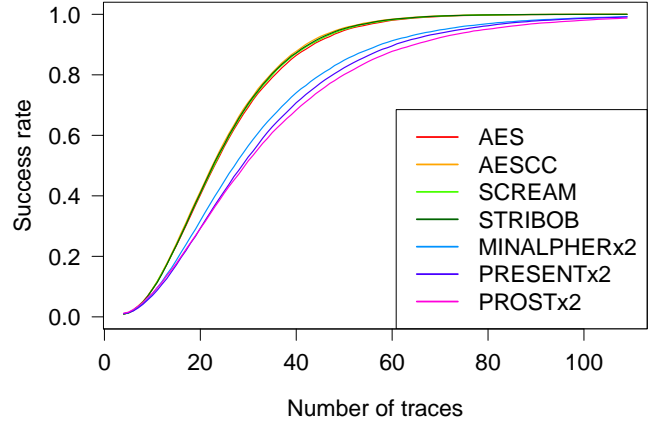
In order to have a fair comparison of all Sboxes, we implement them in the same way by using look-up tables<sup>5</sup>. As a result, each simulated leakage relates to the following operation:

$$r = F(k \oplus p), \quad (6)$$

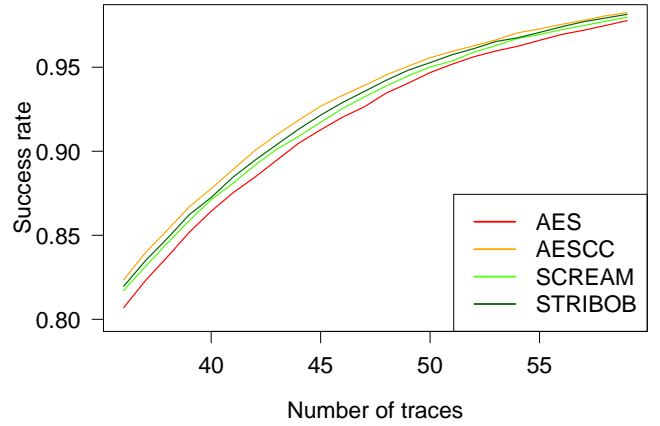
where  $k \in \{0,1\}^n$  is the secret key,  $p \in \{0,1\}^n$  is the plaintext and  $r \in \{0,1\}^m$  is the result of the computation. We calculate the success rate of CPA by repeating the attack 50000 times with different simulated leakages and different random plaintexts.

We use SILK [29] simulator in order to generate simulated power leakages. In our experiments we use the Hamming

<sup>5</sup>We implemented each of the three  $8 \times 8$  meta-Sboxes (that were built from  $4 \times 4$  Sboxes) with a single look-up table of 256 values.



(a) Success rate.



(b) Zoom.

Fig. 1: Success rate of CPA on  $8 \times 8$  Sboxes using simulations.

weight as the leakage function and we set the simulator to produce 1 point per instruction. We vary the noise variance from 0 to 20, but for the sake of space we report here only the case when the noise variance equals to 3. All other scenarios result in the same type of outcome with slower rise of the success rate.

Figure 1 shows the success rate of the CPA on simulated leakages against  $8 \times 8$  Sboxes. According to this results, all  $8 \times 8$  meta-Sboxes are more difficult to attack than other  $8 \times 8$  Sboxes as expected since these meta-Sboxes are more linear. These results accord with the outcome of the theoretical metrics.

Figure 1 also reports that the difficulty of attacking an Sbox differs from the outcome of the theoretical metrics. For example, the classification of  $8 \times 8$  Sboxes from the most difficult to attack to the least difficult are the following:

- $CC_{Picek}$ : AES<sub>CC</sub>, SCREAM<sub>v3</sub>, AES, STRIBOB;
- $TO_0$ : SCREAM<sub>v3</sub>, STRIBOB, AES<sub>CC</sub>, AES;
- $TO_{max}$ : AES & AES<sub>CC</sub>, STRIBOB, SCREAM<sub>v3</sub>;
- SR of CPA: AES, SCREAM<sub>v3</sub>, STRIBOB, AES<sub>CC</sub>.

Note also that the Sbox AES<sub>CC</sub> (taking into account the CC metric in order to improve its resistance against side-channel

attacks) leads to the worst resistance against CPA.

We can also notice a strong discordance between theoretical metrics and simulations for other Sboxes. For example, here is the ranking for  $5 \times 5$  Sboxes (see Figure 3):

- $CC_{Picak}$ : ASCON, PRIMATE, SC2000, ICEPOLE, Keccak;
- $TO_0$ : ASCON, SC2000, ICEPOLE, PRIMATE, Keccak;
- $TO_{max}$ : ASCON, ICEPOLE & SC2000, PRIMATE, Keccak;
- SR of CPA: SC2000, Keccak, PRIMATE, ASCON, ICEPOLE.

All theoretical metrics highlight the Sbox of ASCON as the best against side-channel attacks, and the Sbox of Keccak as the worst from the same perspective. However, this order differs from the results reported by CPA in which SC2000 is the most resistant Sbox while ICEPOLE provides the worst result.

In addition to this discordance, Figure 4 show that the curves of success rate of some  $4 \times 4$  Sboxes cross each other. More precisely, the success rate curve related to Prøst crosses the success rate curves of Minalpher, PRESENT and Joltik. Furthermore, the curve of Evolved $CC$  crosses the curve of Evolved $TO$ . In other words, Joltik is harder to attack than Prøst with a small set of leakages while the results is inverted with a larger number of leakages. It is worth to note that these results cannot be represented using any theoretical metrics based on a single scalar value. In brief, all these results highlight that theoretical metrics (such as TO and CC) do not match actual attacks when the leakage model matches the leakage function (representing the worst case scenario i.e., when the adversary knows how the device leaks information).

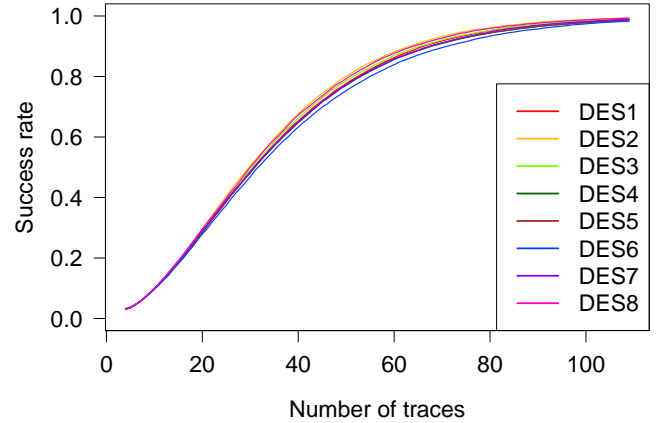
### C. Experimental results on a real device

In order to confirm our simulated results, we acquired real power leakages on a popular 8-bit microcontroller ATmega-328P. The acquisition was done using a digital oscilloscope that acquires  $250 \times 10^6$  samples per second. The measurements were performed on a small  $10 \Omega$  resistor that was inserted between the ground pin of the microcontroller and the power supply of 5 V. We implemented and attacked the following Sboxes:

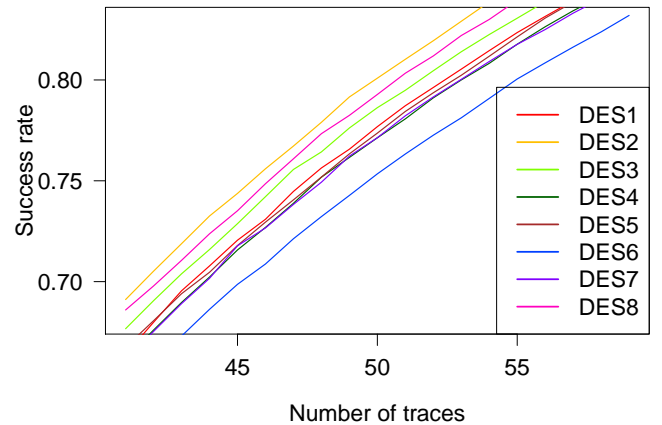
- $8 \times 8$  Sboxes of AES, SCREAM $_{v3}$  and STRIBOB;
- $4 \times 4$  Sboxes of Minalpher, PRESENT and Prøst.

We used the same codes of the implemented Sboxes that were used by SILK (analysed in the previous section). Furthermore, we applied the same physical attack (CPA). We estimate the success rate by repeating the physical attack 10000 times (with different sets of power leakages).

Figures 6 and 7 show the success rate of our attack on real implementations. We can note that experimental results that use simulations fit well the results that use real measurements. Figure 7 shows that Sboxes of AES, SCREAM $_{v3}$  and STRIBOB are indeed similar, as shown by results that use simulations (see Figure 1). Figures 6 and 4 report the same order between  $4 \times 4$  Sboxes of Minalpher, PRESENT and Prøst and also show that curve of the success rate of Prøst indeed crosses the curve related to PRESENT. However, the



(a) Success rate.



(b) Zoom.

Fig. 2: Success rate of CPA on  $6 \times 4$  Sboxes using simulations.

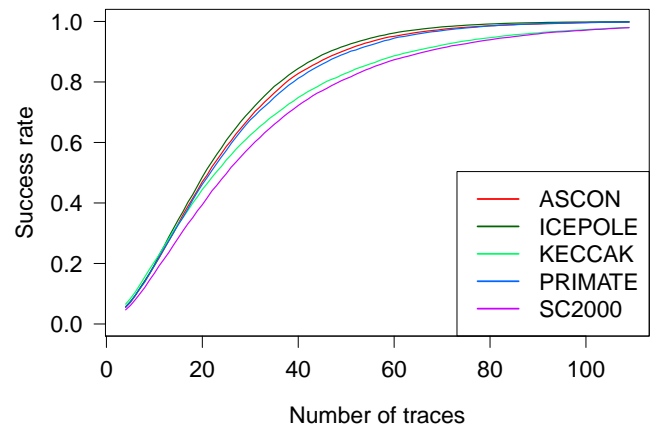


Fig. 3: Success rate of CPA on  $5 \times 5$  Sboxes using simulations.

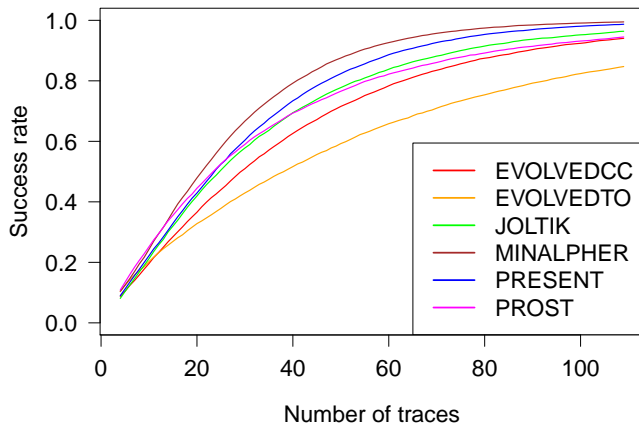


Fig. 4: Success rate of CPA on  $4 \times 4$  Sboxes using simulations.

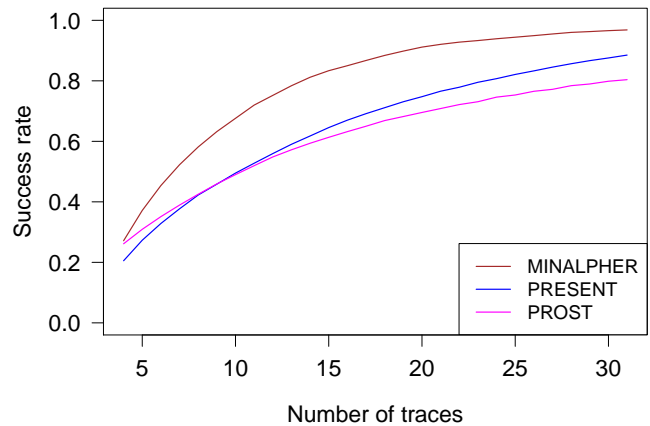


Fig. 6: The success rate of CPA on  $4 \times 4$  Sboxes implemented in on a microcontroller.

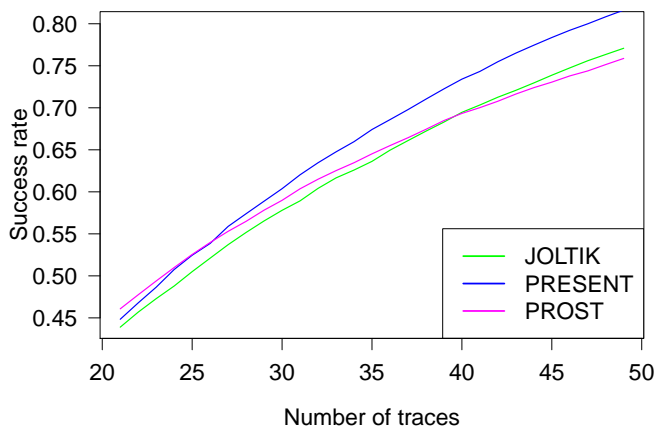


Fig. 5: Zoom on the success rate of CPA on  $4 \times 4$  Sboxes. The success rate curve of Prøst intersects the curve of Joltik.

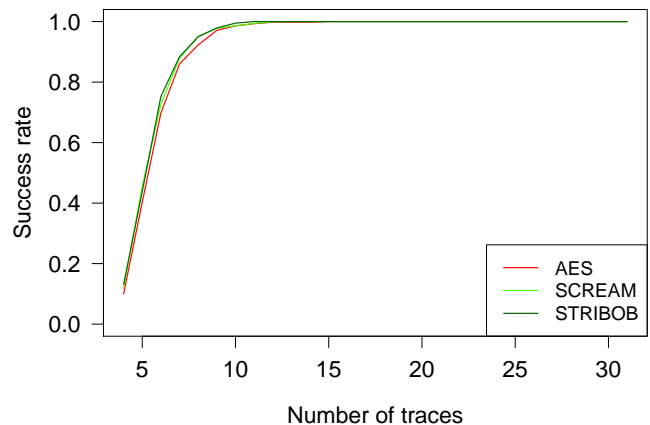


Fig. 7: The success rate of CPA on  $8 \times 8$  Sboxes implemented in on a microcontroller.

experimental results on real leakages differ from the outcome of the theoretical metrics (as already reported in the previous section using simulated leakage scenarios).

#### IV. CONCLUSIONS

In this paper, we analysed two well known theoretical metrics (called transparency order and confusion coefficient) aiming to characterise the resistance of 26 Sboxes against adversaries exploiting physical leakages. We then compared the outcome of these metrics with simulated and real leakages measured on a (software) cryptographic device. All the experiments indicate that (1) it is still unclear how an evaluator can sort Sboxes in terms of resiliency against side-channel attacks, (2) the outcomes of transparency order differ from the results of confusion coefficient, and (3) the outcomes of the theoretical metrics do not always reflect the success rate of a side-channel attack when considering simulated and real leakages. In front of our results, the design of cryptographic primitives (e.g.,  $AES_{CC}$ ) based on these theoretical metrics may render the system still vulnerable to physical attacks.

Future works include (1) the evaluation of the resistance of Sboxes against other physical attacks, (2) comparing the evaluation metrics in front of different types of devices (such as FPGA and ASIC) leaking information in a different way (represented by different leakage functions), (3) finding theoretical metric that fits the reality better (by better understanding the lack of precision of existing metrics), and (4) the exploration of theoretical metrics that can be applied on Sboxes resilient to side-channel attacks (that exploit countermeasures such as masking [30], [31]).

#### ACKNOWLEDGEMENTS

The research of L. Lerman is funded by the Brussels Institute for Research and Innovation (Innoviris) for the SCAUT project.

## REFERENCES

- [1] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, ser. Lecture Notes in Computer Science, N. Kobitz, Ed., vol. 1109. Springer, 1996, pp. 104–113.
- [2] K. Chakraborty, S. Sarkar, S. Maitra, B. Mazumdar, D. Mukhopadhyay, and E. Prouff, "Redefining the transparency order," in *WCC2015-9th International Workshop on Coding and Cryptography 2015*, 2015.
- [3] Y. Fei, A. A. Ding, J. Lao, and L. Zhang, "A statistics-based success rate model for dpa and cpa," *Journal of Cryptographic Engineering*, vol. 5, no. 4, pp. 227–243, 2015.
- [4] M. M. I. Taha, A. Reyhani-Masoleh, and P. Schaumont, "Keymill: Side-channel resilient key generator," *IACR Cryptology ePrint Archive*, vol. 2016, p. 710, 2016. [Online]. Available: <http://eprint.iacr.org/2016/710>
- [5] C. Dobraunig, M. Eichlseder, T. Korak, and F. Mendel, "Side-channel analysis of keymill," *Cryptology ePrint Archive, Report 2016/793*, 2016, <http://eprint.iacr.org/2016/793>.
- [6] J. Coron, P. C. Kocher, and D. Naccache, "Statistics and secret leakage," in *Financial Cryptography, 4th International Conference, FC 2000 Anguilla, British West Indies, February 20-24, 2000, Proceedings*, ser. Lecture Notes in Computer Science, Y. Frankel, Ed., vol. 1962. Springer, 2000, pp. 157–173.
- [7] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, ser. Lecture Notes in Computer Science, B. S. K. Jr., Ç. K. Koç, and C. Paar, Eds., vol. 2523. Springer, 2002, pp. 13–28.
- [8] L. Lerman, G. Bontempi, and O. Markowitch, "Power analysis attack: an approach based on machine learning," *International Journal of Applied Cryptography*, vol. 3, no. 2, pp. 97–115, 2014.
- [9] F. Standaert, T. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," in *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009, Proceedings*, ser. Lecture Notes in Computer Science, A. Joux, Ed., vol. 5479. Springer, 2009, pp. 443–461.
- [10] E. Prouff, "DPA attacks and s-boxes," in *Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers*, ser. Lecture Notes in Computer Science, H. Gilbert and H. Handschuh, Eds., vol. 3557. Springer, 2005, pp. 424–441.
- [11] Y. Fei, Q. Luo, and A. A. Ding, "A statistical model for DPA with novel algorithmic confusion analysis," in *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012, Proceedings*, ser. Lecture Notes in Computer Science, E. Prouff and P. Schaumont, Eds., vol. 7428. Springer, 2012, pp. 233–250.
- [12] 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 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings*, ser. Lecture Notes in Computer Science, W. Meier and D. Mukhopadhyay, Eds., vol. 8885. Springer, 2014, pp. 374–390.
- [13] K. Stoffelen, "Intrinsic side-channel analysis resistance and efficient masking," 2015, Master Thesis. [Online]. Available: [http://www.ru.nl/publish/pages/769526/z\\\_thesis\\\_ko\\\_stoffelen.pdf](http://www.ru.nl/publish/pages/769526/z\_thesis\_ko\_stoffelen.pdf)
- [14] J. Jean, I. Nikolić, and T. Peyrin, "Joltik v1.3," Aug 2015, CAESAR submission. [Online]. Available: <http://competitions.cr.yt.to/round2/joltikv13.pdf>
- [15] E. B. Kavun, M. M. Lauridsen, G. Leander, C. Rechberger, P. Schwabe, and T. Yalçın, "Prøst v1.1," Jun 2014, CAESAR submission. [Online]. Available: <http://competitions.cr.yt.to/round1/proestv11.pdf>
- [16] Y. Sasaki, Y. Todo, K. Aoki, Y. Naito, T. Sugawara, Y. Murakami, M. Matsui, and S. Hirose, "Minalpher v1.1," Aug 2015, CAESAR submission. [Online]. Available: <http://competitions.cr.yt.to/round2/minalpherv11.pdf>
- [17] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: an ultralightweight block cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, ser. Lecture Notes in Computer Science, P. Paillier and I. Verbauwhede, Eds., vol. 4727. Springer, 2007, pp. 450–466.
- [18] S. Picek, B. Mazumdar, D. Mukhopadhyay, and L. Batina, "Modified transparency order property: Solution or just another attempt," in *Security, Privacy, and Applied Cryptography Engineering - 5th International Conference, SPACE 2015, Jaipur, India, October 3-7, 2015, Proceedings*, ser. Lecture Notes in Computer Science, R. S. Chakraborty, P. Schwabe, and J. A. Solworth, Eds., vol. 9354. Springer, 2015, pp. 210–227.
- [19] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "ASCON v1.1," Aug 2015, CAESAR submission. [Online]. Available: <http://competitions.cr.yt.to/round2/asconv11.pdf>
- [20] P. Morawiecki, K. Gaj, E. Homsirikamol, K. Matusiewicz, J. Pieprzyk, M. Rogawski, M. Srebrny, and M. Wójcik, "ICEPOLE v2," Aug 2015, CAESAR submission. [Online]. Available: <http://competitions.cr.yt.to/round2/icepolev2.pdf>
- [21] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "The keccak reference," 2011, Submission to NIST (Round 3). [Online]. Available: <http://keccak.noekeon.org/Keccak-reference-3.0.pdf>
- [22] E. Andreeva, B. Bilgin, A. Bogdanov, A. Luykx, F. Mendel, B. Mennink, N. Mouha, and Q. W. an Kan Yasuda, "PRIMATEs v1.02," Sept 2014, CAESAR submission. [Online]. Available: <http://competitions.cr.yt.to/round2/primatesv102.pdf>
- [23] T. Shimoyama, H. Yanami, K. Yokoyama, M. Takenaka, K. Itoh, J. Yajima, N. Torii, and H. Tanaka, "The block cipher SC2000," in *Fast Software Encryption, 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001, Revised Papers*, ser. Lecture Notes in Computer Science, M. Matsui, Ed., vol. 2355. Springer, 2001, pp. 312–327.
- [24] F. FIPS, "46-3: Data encryption standard (des)," *National Institute of Standards and Technology*, vol. 25, no. 10, pp. 1–22, 1999.
- [25] V. Grosso, G. Leurent, F.-X. Standaert, K. Varici, A. Journault, F. Durvaux, L. Gaspar, and S. Kerckhof, "SCREAM Side-Channel Resistant Authenticated Encryption with Masking," Aug 2015, CAESAR submission. [Online]. Available: <http://competitions.cr.yt.to/round2/screamv3.pdf>
- [26] M.-J. O. Saarinen and B. B. Brumley, "STRIBOBr2: "WHIRLBOB"," Aug 2015, CAESAR submission. [Online]. Available: <http://competitions.cr.yt.to/round2/stribobr2.pdf>
- [27] N. F. Pub, "197: Advanced encryption standard (aes)," *Federal Information Processing Standards Publication*, vol. 197, pp. 441–0311, 2001.
- [28] A. Heuser, O. Rioul, and S. Guilley, "A theoretical study of kolmogorov-smirnov distinguishers - side-channel analysis vs. differential cryptanalysis," in *Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014, Revised Selected Papers*, ser. Lecture Notes in Computer Science, E. Prouff, Ed., vol. 8622. Springer, 2014, pp. 9–28.
- [29] N. Veshchikov, "SILK: high level of abstraction leakage simulator for side channel analysis," in *Proceedings of the 4th Program Protection and Reverse Engineering Workshop, PPREW@ACSAC 2014, New Orleans, LA, USA, December 9, 2014*, M. D. Preda and J. T. McDonald, Eds. ACM, 2014, pp. 3:1–3:11. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2689702>
- [30] L. Goubin and J. Patarin, "DES and differential power analysis (the "duplication" method)," in *Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, Proceedings*, ser. Lecture Notes in Computer Science, Ç. K. Koç and C. Paar, Eds., vol. 1717. Springer, 1999, pp. 158–172.
- [31] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, ser. Lecture Notes in Computer Science, M. J. Wiener, Ed., vol. 1666. Springer, 1999, pp. 398–412.