On some relations of SCA-related properties of S-box under the Hamming weight leakage mode

Alejandro Freyre Echevarría, Ramses Rodríguez Aulet, Alejandro García Gómez

***Abstract*— Physical implementations of cryptographic algorithms are vulnerable to so-called side-channel attacks, in which sensitive information can be recovered through the analysis of the leakages produced by the operating device. In the particular case of block ciphers, substitution boxes are often the target of such attacks, as they are the main nonlinear component of the cipher. Literature survey contains some definitions of theoretical properties to measure the resistance provided by substitution boxes with respect to the imminent threat of side-channel attacks. The fundamental questions we board in this paper are: are all these properties related? And if so, what can we tell of their relation? We pretend to bring some clarification to this subject using some well-known side-channel related properties of S-box.**

***Tóm tắt*— Việc triển khai vật lý các thuật toán mật mã dễ bị tấn công bởi các cuộc tấn công kênh kề, trong đó thông tin nhạy cảm có thể được khôi phục thông qua phân tích các rò rỉ do thiết bị điều hình tạo ra. Trong trường hợp cụ thể của mật mã khối, các hộp thay thế thường là mục tiêu của các cuộc tấn công như vậy, vì chúng là thành phần phi tuyến tính của mật mã. Bài báo này khảo sát một số định nghĩa về các thuộc tính lý thuyết để kiểm tra khả năng bảo vệ được cung cấp bởi các hộp thay thế liên quan đến mối đe dọa sắp xảy ra của các cuộc tấn công kênh kề. Các câu hỏi cơ bản mà nhóm tác giả đặt ra trong bài báo này là: tất cả các thuộc tính này có liên quan với nhau không? Và nếu đúng như vậy, chúng ta có thể nói gì về mối quan hệ của chúng? Nhóm tác giả sẽ làm sáng tỏ các vấn đề này bằng cách sử dụng một số thuộc tính liên quan đến kênh kề nổi tiếng của S-box.**

***Keywords*— S-box; side-channel attacks; S-box properties; Pearson's correlation coefficient; chi-squared test.**

***Từ khoá*— S-box; Tấn công kênh kề; thuộc tính S-box; hệ số tương quan của Pearson; chi bình phương.**

This manuscript is received on December 02, 2022. It is commented on December 16, 2022 and is accepted on December 18, 2022 by the first reviewer. It is commented on December 17, 2022 and is accepted on December 20, 2022 by the second reviewer.

I. INTRODUCTION

Side-channel attacks (SCA) represent a threat to the security of hardware implementations of block ciphers. In these algorithms, substitution box (S-box) is often the only source of nonlinearity during the encryption process and therefore they are usually the main target of a side-channel attack. Although there exist several countermeasures against SCA like masking [1], the scientific community has explored the possibility of substitution boxes having built-in resistance to such attacks.

The cryptographic properties of S-box measure their resistance under several known attack scenarios which include linear [2], differential [3] and algebraic [4] cryptanalysis. In this fashion, it may be understandable that one tries to encapsulate the resistance of the S-box w.r.t side-channel attacks by means of theoretical properties. The papers presenting the notions of SNR-DPA [5] and transparency order [6] were pioneers in this topic. With the progressive advances in the field of power side-channel analysis, it was necessary to define new properties for S-box that attempt to measure their resistance in these scenarios. This paper describes the properties related to the Hamming weight leakage model, as the prosecution of the research presented in [7]. It is worth remarking that we do restrict the analysis to theoretical properties of bijective S-box related to power side-channel attacks instead of analyzing classical cryptographic properties such as nonlinearity or differential uniformity.

II. PRELIMINARIES

Let denote as $\mathbb{F}_2 = \{0,1\}$ the finite field with two elements; V_n is the *n*-dimensional vector space over $\mathbb{F}_2$. One S-box S is a mapping from V_n to V_m, *i.e.* $S: V_n \to V_m$, where S can be decomposed as the parallelization of m *n-variable* Boolean functions $S = (f_1, f_2, \dots, f_m)$ known as coordinate functions of *S*. In the majority of cases, the cryptographic properties of S-box depend on all the linear combinations of its coordinated functions, i.e. the component functions of the S-box [8, 9]. In the case of side-channel properties, they are related to a particular leakage model like Hamming weight or Hamming distance, which are dependent on the notion of Hamming weight of a vector.

Definition 1. *The Hamming weight of a Boolean vector $x \in V_n$, denoted as $w_{\mathcal{H}}(x)$, is the number of nonzero positions in x.*

For any given sub-key *k* and a piece of plain text *t* to be encrypted using *k* one can define the Hamming distance leakage model as:

$$\mathcal{HD} = w_{\mathcal{H}}\big(\beta \oplus \mathrm{F}(t \oplus k)\big) \qquad (1)$$

where F is the function leaking information about the sub-key *k* and β is a logic pre-charge of the encryption algorithm, *e.g.* the state of the register before proceeding to execute $\mathrm{F}(t \oplus k)$.

When β is assumed to be equal to 0 then the Hamming distance power model is simplified to the Hamming weight leakage model:

$$\mathcal{HW} = w_{\mathcal{H}}\big(\mathrm{F}(t \oplus k)\big) \qquad (2)$$

It is worth remarking that in both leakage models, the function F is associated with the substitution box [7] (e.g. *SubBytes* function in AES [10]). Thus, it may be reasonable to introduce at this point the properties of S-box related to these models which are the subject of analysis in this paper.

The properties of modified transparency order [11] (MTO) and revised transparency order [12] (RTO) were defined for devices leaking in the Hamming distance power model, *i.e.* the logic pre-charge β is considered. Although the authors of [11, 12] focus on the study of these properties under the Hamming weight leakage model. In addition, the property of confusion coefficient variance [13] was defined for devices leaking in the Hamming weight power model only. Next, we present the mathematical definition of each of these properties as well as a brief explanation of the same.

The confusion coefficient [14, 15], gives a probabilistic model that encompasses the three main parameters of a side-channel attack: the device under test, the number of traces, and the algorithm under examination. The model manages to separate these elements allowing the freedom to explore the cipher design space by focusing only on the cipher algorithm.

While moving through correlation power analysis (CPA) related models using the confusion coefficient, the vector containing all confusion coefficients concerning a CPA attack under the Hamming weight power model contains all possible coefficients for every key combination and its frequency distribution is a possible characterizer of side-channel behavior. Picek et.al. [13] remark that increasing the variance of the confusion coefficient vector leads to more resistance against CPA attacks. The confusion coefficient variance (CCV) of an S-box S is defined, for each $\mu, k_1, k_2 \in V_n$ and $k_1 \neq k_2$ as [13]:

$$\kappa(S) = \mathrm{Var}\Big(\mathrm{E}\Big[\Big(w_{\mathcal{H}}\big(S(\mu \oplus k_1)\big) - w_{\mathcal{H}}\big(S(\mu \oplus k_2)\big)\Big)^2\Big]\Big) \qquad (3)$$

where one can identify μ as the piece of plaintext and k_1, k_2 are two different sub-key guesses.

After an evaluation of the notion of transparency order introduced in [6], Chakraborty *et. al* presented the property of a modified transparency order which extends the basic definition of transparency order to the most general case of $n \times m$ S-box [11]. For any balanced S-box $S: V_n \to V_m$, the MTO property is defined as:

$$\max_{\beta \in V_m} \left(\mathrm{m} - \frac{1}{2^{2\mathrm{n}} - 2^{\mathrm{n}}} \sum_{\mathrm{a} \in \mathrm{V}_{\mathrm{n}}^{*}} \sum_{j=1}^{m} \left| \sum_{i=1}^{m} (-1)^{(\beta_i \oplus \beta_j)} C_{S_i,S_j}(a) \right| \right) \tag{4}$$

where $a = k_c \oplus k_g$ for a given key k_c and the key guess k_g, and $C_{\mathrm{S_i,S_j}}(\mathrm{a})$ denote the cross-correlation function of the corresponding coordinate functions of S as defined in [9]. The value of MTO assumes the worst case scenario for the defender and the best for the attacker [11]. However, Chakraborty et. al overlook the same definitional flaw as the original transparency order which made MTO take a variant of multi-bit differential power analysis (DPA) as remarked by Li et. al. in [12]. Consequently, this flaw was boarded in [12] with the revision of the modified transparency order resulting in the definition of the new RTO property for S-box:

$$\max_{\beta \in V_m} \left(\mathrm{m} - \frac{1}{2^{2\mathrm{n}} - 2^{\mathrm{n}}} \sum_{\mathrm{a} \in \mathrm{V}_{\mathrm{n}}^{*}} \left| \sum_{j=1}^{m} \sum_{i=1}^{m} (-1)^{(\beta_i \oplus \beta_j)} C_{S_i,S_j}(a) \right| \right) \tag{5}$$

Through the notion of RTO the authors fix the flaws detected in the definitions of transparency order and modified transparency order. Furthermore, the authors conclude that the soundness of RTO is demonstrated through simulated and practical experiments which confirm that RTO is a valuable criterion to evaluate the DPA resistance of S-box. Further information about these properties can be found in [11-13].

III. MEASURING THE RELATION BETWEEN SCA PROPERTIES

Recently, the master's thesis of Cerini conducted an empirical evaluation of the resistance of novel S-box implementations against power side-channel attacks [16]. Such a thesis concludes that S-box optimized for the confusion coefficient variance are indeed more resistant to correlation power analysis than other design strategies presented in the literature which correspond to the simulation results achieved by Freyre in [17]. In addition, the results introduced in [7] indicate the existence of some relations between the properties of confusion coefficient variance and the new definitions of transparency order. Although the authors of the paper did not show the existing relation.

In this paper we study the aforementioned relations by means of the Chi-squared test [18] and the well-known Pearson's correlation coefficient. We also present the dependence trajectories of the properties by selecting one as the base property for improvement and measuring the values of the others as the first improves. For the cases of MTO and RTO we use the logic pre-charge $\beta = 0$ which reduces the leakage model from Hamming distance to Hamming weight.

A. Creation of the dependence trajectories between properties

To construct the dependency trajectories between two properties we fix a maximum of N upgrade points. At each point we check that the base property, e.g. confusion coefficient variance, is at least equals to the best value of such property. We assume as the initial best value of the base property the original value of the property for the input S-box. Then, if we are in the presence of an upgrade point, we also calculate the value of the property to be analyzed as long as the base property is improved. Notice that after the N upgrade points are passed we create two vectors of N elements each, the first containing the improvements of the base property and the second containing the behavior of the analyzed property as shown in Algorithm 1.

It is worth remarking that the *swap mutation* performed on Algorithm 1 constructs a new S-box by swapping the outputs of *S* corresponding to the input values of *x* and *y*.

```
input : A pseudo-random n-bit bijective S-box
        S;
input : The function F1, i.e, the base property;
input : The function F2, i.e, the analyzed
        property;
input : The number of upgrade points N
output: The trajectories of F1 and F2
// Initialization
f1 ← []  // the trajectory of F1
f2 ← []  // the trajectory of F2
best ← F1(S)

// Computation of the
trajectories
while N > 0 do
    Randomly select two different inputs of S
    S' ← SwapMutation(S, x, y)
    f1' ← F1(S')
    if f1' is better or equal than best then
        best ← f1'
        S ← S'
        f1.Add(f1')
        f2.Add(F2(S))
        N ← N − 1
    end
end
return f1, f2
```

Figure 1. Algorithm 1: Pseudo-code for computing the trajectories of the properties

Algorithm 1 was repeated for 1000 different input candidates on each search space of bijective S-box from 5×5 to 8×8 using parameter N equals to 25, 50, 75 and 100 for each S-box dimension respectively.

B. Chi-squared test and Pearson's correlation coefficient

The statistical tests we conduct in this paper are intended to response two fundamental questions: the existence of a relation between MTO, RTO and CCV, and the nature of such relation. Through the Chi-squared test we analyze the dependence between a pair of properties and, if successful, determine the linearity of the relation by means of the Pearson's correlation coefficient.

We apply the Chi-squared test following the procedure described below:

1. The significance value is $\alpha = 0.001$.
2. The null hypothesis assumes that the properties are independent.
3. Define non-overlapping incremental intervals of the same size for each property in accordance with its real values.
4. Construct a matrix where rows and columns are the number of intervals defined for the properties being analyzed, such that the matrix contains at *i-th* row and *j-th* column the number of times that the values of the property p_1 were in the *i-th* interval and the values of the property p_2 was in the *j-th* interval respectively. See the following example:

	p_2^1	p_2^2	p_2^3
p_1^1	$v_{1,1}$	$v_{1,2}$	$v_{1,3}$
p_1^2	$v_{2,1}$	$v_{2,2}$	$v_{2,3}$
p_1^3	$v_{3,1}$	$v_{3,2}$	$v_{3,3}$

5. The matrix is filled on the update steps of Algorithm 1.
6. The degrees of freedom of the experiment are $(r-1)(c-1)$ where r and c are the number of rows and columns of the matrix respectively.

The rejection of the null hypothesis of the Chi-squared test implies that exist a dependence between the analyzed properties. In such case, we use Pearson's correlation coefficient to check if the properties are linearly dependent or not. Notice that if Pearson's correlation coefficient is approximately equal to 0 it implies that properties are linearly independent, but it does not discard that properties are related.

To calculate the Pearson's correlation coefficient, we use the average of all trajectories generated by Algorithm 1 for the selected pair of properties on each S-box search space.

C. Chi-squared test and Pearson's correlation coefficient

Once terminated all the executions of Algorithm 1 we conduct the corresponding Chi-squared tests using the collected data as explained in the preceding subsection. In all cases the null hypothesis was rejected, *i.e.* all properties are dependent on each other. In what follows, we explain the analysis of the generated trajectories as well as the results for the Pearson's correlation test.

For the first block of experiments we have decided to use the confusion coefficient variance as a basis to measure the behavior of

the remaining SCA-related properties. Our initial hypothesis assumes that as confusion coefficient variance gets maximized, both, MTO and RTO with logic precharge β get minimized.

TABLE 1. PEARSON'S CORRELATION BETWEEN SCA-RELATED PROPERTIES USING CONFUSION COEFFICIENT VARIANCE AS BASE PROPERTY FOR IMPROVEMENTS

Dimension	MTO	RTO
5x5	-0.9989	-0.9976
6x6	-0.9988	-0.9966
7x7	-0.9993	-0.9958
8x8	-1.000	-0.9978

In Table 1, we show the resulting correlation the average trajectories generated for the confusion coefficient variance and the modified transparency order (resp. revised transparency order). As we expected, the strong inverse correlation between the confusion coefficient variance and the remaining properties indicates that the assumed hypothesis is correct and the improvement of the confusion coefficient variance has great influence on the improvement of the remaining properties under the Hamming weight leakage model, although one may notice that the confusion coefficient variance seems to have better influence over the property of modified transparency order than it does for revised transparency order. In this fashion we were able to achieve a perfect inverse relation between the trajectories of confusion coefficient variance and modified transparency order for S-box of dimension 8×8. Finally, the plots of the average trajectories for each S-box dimension are shown in Figure 1.

As we remark in the beginning of the paper, the results from [7] point to the existence of a relation between all side-channel related properties under the Hamming weight leakage model. We already show that such relation exists, however it is restricted, up to this moment, in the case when the confusion coefficient variance is improved. Thus, we pretend to show with the next experimental results that improving any of the SCA-related properties of S-box relative to the Hamming weight leakage model will lead to the improvement of the remaining.

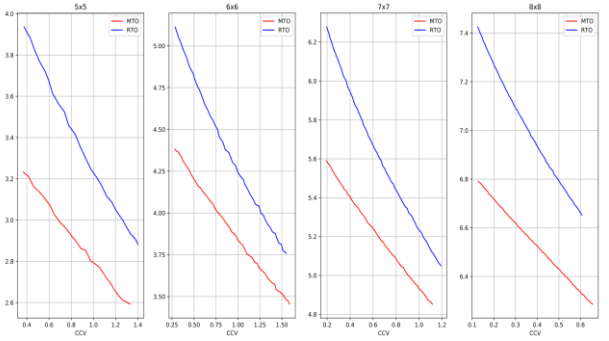


Figure 2. Average trajectories of SCA-related properties using confusion coefficient variance as base property for improvements

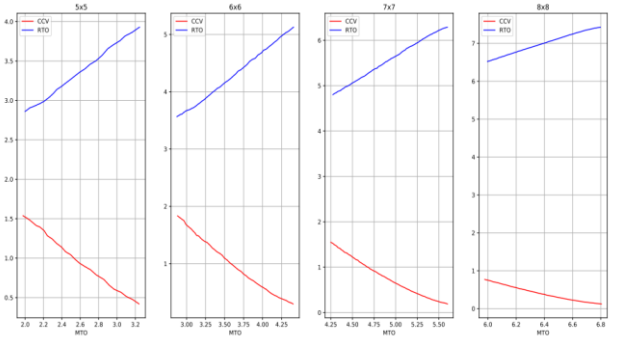


Figure 3. Average trajectories of SCA-related properties using modified transparency order as base property for improvements

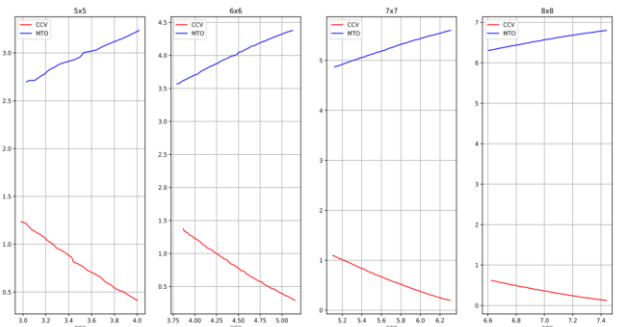


Figure 4. Average trajectories of SCA-related properties using revised transparency order as base property for improvements

Figures 3 and 4 show the average trajectories of the remaining side-channel related properties when modified and revised transparency orders are improved respectively. One may clearly distinguish the behavior of the confusion coefficient variance (red plot) since, by definition, its improvement condition is opposed to MTO and RTO properties. Nonetheless, in

both figures the maximum value of the confusion coefficient variance and the minimum value of the revised transparency order (resp. modified transparency order) were achieved when the base property reported its best value. Moreover, like the property of confusion coefficient variance, there exists a high correlation that can be expressed in terms of the Pearson's correlation coefficient as presented in Table 2.

TABLE 2. PEARSON'S CORRELATION BETWEEN SCA-RELATED PROPERTIES USING MTO (LEFT)/RTO (RIGHT) AS BASE PROPERTY FOR IMPROVEMENTS

Property	**MTO**		**RTO**	
Dimension	CCV	RTO	CCV	MTO
5×5	-0.9983	-0.9989	-0.9983	0.9966
6×6	-0.9964	-0.9992	-0.9982	0.9986
7×7	-0.9939	-0.9995	-0.9978	0.9989
8×8	-0.9938	0.9992	-0.9976	0.9983

From the results presented in tables 1 and 2, and the average trajectories of the SCA-related properties of S-box in figures 1 to 3 we can now affirm that under the Hamming weight power model all the properties of S-box maintain a strong linear relation and therefore the improvement of one implies the improvement of the remaining. The work from Li *et. al.* [19] experimentally verifies our conclusions about the properties of the revised transparency order and confusion coefficient using different lightweight S-box from literature survey.

Finally, it may be reasonable to think that any S-box optimized for one of the properties should present a better practical resistance to side-channel analysis as shown in [16, 17] for the confusion coefficient variance. However, it is also necessary to study the reason for the improvement of one property with respect to others due to the necessity of knowing the effort to obtain equivalent S-box in the sense of side-channel resistance when the selected property is the target for improvements and the others will be implicitly upgraded.

IV. CONCLUSIONS

In this paper, we conducted a statistical analysis that reveals the linear dependence of the theoretical properties of S-box related to side-channel attacks. It is shown by means of the average trajectories of these properties and their Pearson's correlation coefficient that such linear relation is strong. Our result ensures that the generation of S-box with theoretical built-in side-channel resistance in the Hamming weight power model can be accomplished disregarding the property selected in the design phase.

REFERENCES

[1] Golić, J. D., & Tymen, C. (2002, August). Multiplicative masking and power analysis of AES. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 198-212). Springer, Berlin, Heidelberg.

[2] Matsui, M. (1993, May). Linear cryptanalysis method for DES cipher. In Workshop on the Theory and Application *of Cryptographic Techniques* (pp. 386-397). Springer, Berlin, Heidelberg.

[3] Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY, 4(1), 3-72.

[4] Armknecht, F. (2004, February). Improving fast algebraic attacks. In International Workshop on Fast Software Encryption (pp. 65-82). Springer, Berlin, Heidelberg.

[5] Guilley, S., Hoogvorst, P., & Pacalet, R. (2004). Differential power analysis model and some results. In *Smart card research and advanced applications VI* (pp. 127-142). Springer, Boston, MA.

[6] Prouff, E. (2005, February). DPA attacks and S-box. In *International Workshop on Fast Software Encryption* (pp. 424-441). Springer, Berlin, Heidelberg.

[7] Martınez-Dıaz, I., & Freyre-Echevarría, A. S-box with theoretical resistance against power attacks under Hamming leakage models. In *V Seminario Científico Nacional de Criptografía*. Sociedad Cubana de Matemática y Computación, 2020

[8] Canteaut, A. (2016). Lecture notes on cryptographic Boolean functions. *Inria, Paris, France, 3*.

[9] Carlet, Claude, Yves Crama, and Peter L. Hammer. "Vectorial Boolean Functions for Cryptography." (2010): 398-470.

[10] Daemen, J., & Rijmen, V. (2002). *The design of Rijndael* (Vol. 2). New York: Springer-Verlag.

[11] Chakraborty, K., Sarkar, S., Maitra, S., Mazumdar, B., Mukhopadhyay, D., & Prouff, E. (2017). Redefining the transparency order. *Designs, codes and cryptography*, *82*(1), 95-115.

[12] Li, H., Zhou, Y., Ming, J., Yang, G., & Jin, C. (2020). The notion of transparency order, revisited. *The Computer Journal*, *63*(12), 1915-1938.

[13] Picek, S., Papagiannopoulos, K., Ege, B., Batina, L., & Jakobovic, D. (2014, December). Confused by confusion: Systematic evaluation of DPA resistance of various s-box. In *International Conference on Cryptology in India* (pp. 374-390). Springer, Cham.

[14] Ding, A. A., Zhang, L., Fei, Y., & Luo, P. (2014, September). A statistical model for higher order DPA on masked devices. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 147-169). Springer, Berlin, Heidelberg.

[15] Fei, Y., Luo, Q., & Ding, A. A. (2012, September). A statistical model for DPA with novel algorithmic confusion analysis. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 233-250). Springer, Berlin, Heidelberg.A

[16] Prinetto, P. E., & Cerini, S. Y. Empirical Evaluation of the Resilience of Novel S-Box Implementations Against Power Side-Channel Attacks.

[17] Freyre Echevarría, A. (2020). *Evolución híbrida de S-cajas no lineales resistentes a ataques de potencia* Dept. Ciencia de la Computación, Univ. de La Habana, Havana, Cuba.

[18] Medvedev, Yu.I., Ivchenko, G.I., Statistical Mathematics. URSS, 2014.

[19] Li, H., Yang, G., Ming, J., Zhou, Y., & Jin, C. (2021). Transparency order versus confusion coefficient: a case study of NIST lightweight cryptography S-box. *Cybersecurity*, *4*(1), 1-20.

ABOUT THE AUTHORS

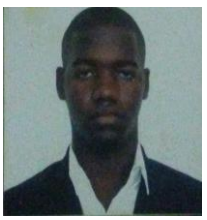
Alejandro Freyre Echevarría

Workplace: Institute of Cryptography, University of Havana.

Email: freyreealejandro@gmail.com

Education: Graduated from Computer Science in 2020; in process to receive his Master's degree.

Recent research interests: Symmetric cryptography; Post-quantum cryptography.



Ramses Rodríguez Aulet

Workplace: Institute of Cryptography, University of Havana.

Email: ramsesrusia@yahoo.com

Education: Graduated from Mathematics in 2017; received his Master's degree in 2020.

Recent research interests: Symmetric cryptography; Post-quantum cryptography.

Alejandro García Gómez

Workplace: Institute of Cryptography, University of Havana.

Email: alejandrogg08189@gmail.com

Education: He obtained the BSc. degree in 2021.

Recent research interests: Symmetric and asymmetric cryptography.