IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received December 29, 2021, accepted January 19, 2022, date of publication January 25, 2022, date of current version February 2, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3145990

Improved Objective Functions to Search for 8 × 8 Bijective S-Boxes With Theoretical Resistance Against Power Attacks Under Hamming Leakage Models

ISMEL MARTÍNEZ-DÍAZ[1], **ALEJANDRO FREYRE-ECHEVARRÍA**[1], **OMAR ROJAS**[2,3], **GUILLERMO SOSA-GÓMEZ**[2], **AND CARLOS MIGUEL LEGÓN-PÉREZ**[1]

[1]Instituto de Criptografía, Universidad de La Habana, Havana 10400, Cuba
[2]Facultad de Ciencias Económicas y Empresariales, Universidad Panamericana, Zapopan, Jalisco 45010, Mexico
[3]Faculty of Economics and Business, Universitas Airlangga, Surabaya 60115, Indonesia

Corresponding author: Guillermo Sosa-Gómez (gsosag@up.edu.mx)

ABSTRACT Many research focuses on finding S-boxes with good cryptographic properties applying a heuristic method and a balanced, objective function. The design of S-boxes with theoretical resistance against Side-Channel Attacks by power consumption is addressed with properties defined under one of these two models: the Hamming Distance leakage model and the Hamming Weight leakage model. As far as we know, a balanced search criterion that considers properties under both, at the same time, remains an open problem. We define two new optimal objective functions that can be used to obtain S-boxes with good cryptographic properties values, keeping high theoretical resistance for the two leakage models; we encourage using at least one of our objective functions. We apply a Hill Climbing heuristic method over the S-box's space to measure which objective function is better and to compare the obtained S-boxes with the S-boxes in the actual literature. We also confirm some key relationships between the properties and which property is more suitable to be used.

INDEX TERMS S-box, hamming leakage model, transparency order, cryptography, power attack.

I. INTRODUCTION

Substitution boxes (S-boxes) are a principal component of block ciphers [1]. Since they are involved in the encryption/decryption process, S-boxes represent a target of Side-Channel Attacks (SCA) by power consumption. Some S-box properties have been defined to measure the theoretical resistance against these types of attacks. These properties can be classified into two groups according to the leakage model of the power consumption. The first, Hamming Distance (HD) model, includes properties like Modified Transparency Order (MTO) [3] and Revised Transparency Order (RTO) [10]. For the second group, Hamming Weight (HW) leakage model, properties like Transparency Order (TO) [2],[1] Confusion Coefficient Variance (CCV) [7], Modified Transparency Order for the zero logic precharge (MTO_0) [8] and Revised Transparency Order for the zero logic precharge (RTO_0) [10] can be found in the literature.

Strong linear correlations between CCV, TO, MTO_0 and RTO_0 over the S-box space were found in [16]. More recently, other relations have been proved for MTO, RTO, and CCV [21]–[23], increasing the importance of these theoretical metrics. Some researchers obtained S-boxes with optimized values of the aforementioned properties [5], [12]–[15], [20]. In most cases, heuristic methods were applied to S-box's design, following the approach of use the search as a cryptological tool [24]. Therefore, the design of S-boxes with optimal theoretical resistance towards both Hamming power models is an open issue that we addressed in this work.

Our main contribution is the definition of a new optimal objective function that considers properties under both: the Hamming Distance power model and the Hamming Weight power model. The resultant S-boxes of our research have low MTO, low MTO_0, low RTO, low RTO_0, and high CCV.

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

[1] The TO was defined under HD power model, but the deficiencies found in its formula [3] move it under HW power model

The central idea of our objective function came from the linear correlations between CCV vs. MTO_0, and CCV vs. RTO_0 found in [16], where the well-studied metric CCV arise as the link to glue the other two properties. Correlation aligns the metrics under the Hamming Weight power model, expanding the comparison presented by Lerman *et al.* in [8]. The results we addressed using the hill-climbing method -a basic meta-heuristic [18]- and the proposed optimal objective function reinforces the correlation notion under the same model of power consumption. Also, we give a tip to compare the MTO and RTO properties, about the comment given in [10] that RTO is more suitable to represent the S-box's resistance against power attacks under the Hamming Distance leakage model. Furthermore, the results show that the MTO_0 -and in the most better way, the RTO_0- can substitute the CCV as the most important metric under the Hamming Weight power model. From the perspective of classical cryptanalysis, this research does not attempt to optimize other important properties of S-boxes like Non-Linearity (NL) and Differential Uniformity (DU) [4]. Still, we provide a certain analysis of the values of these properties using our results. The analysis confirms the inverse relation between the Confusion Coefficient (CC) -a theoretical indicator against single-bit Differential Power Attack (DPA)-, and Differential Uniformity [9]; including the conjecture that S-boxes with high theoretical resistance against SCA by power consumption have poor Non-Linearity [2], [5].

The remainder of this paper is organized as follows. In **Section II**, we enunciate basic concepts that helps to understand the paper. Next, in **Section III**, we present the optimal objective function, and we analyze the properties values of the obtained S-boxes. Finally, we briefly resume this work and give some new lines of research in the **Conclusions**.

II. PRELIMINARIES AND METHODS

The general scheme of any symmetric cryptographic algorithm works as follow: Given a key K, a plain-text X, an encryption function Ec and a decryption function Dc, the cipher-text X' can be created as $X' = Ec(X, K)$ and the plain-text will be recovered as $X = Dc(X', K)$. Substitution boxes play their role as components of Ec and/or Dc.

An S-box is a mapping from the vector space $\{0, 1\}^n$ into the vector space $\{0, 1\}^m$. In the particular case of actual block ciphers, it is common that $m = n$. In this work we denote an S-box as a bijective vector boolean function $F : \{0, 1\}^n \to \{0, 1\}^n$.

A. SIDE-CHANNEL ANALYSIS BY POWER CONSUMPTION

In the encryption (decryption) process on a computer device given N known plain-texts (cipher-texts) $X(i)$, a power consumption is captured as a set of traces over time $T_{\dot{k}}(X(i))$. Those traces, and a hypothetical model of power consumption, are used to obtain every sub-key $\dot{k}$ of the secret key K. Both the traces and the leakage model exploit the evaluation of the S-box.

The main SCA attack is the DPA [1], which performs statistical analysis (calculate the difference of means) to retrieve the secret sub-keys from the power consumption of cryptography devices. A *single-bit* differential trace $\Delta_{k,\dot{k}}(N, j)$ can be calculated by the expression:

$$\Delta_{k,\dot{k}}(N, j) \tag{1}$$

$$= \frac{\sum_{i=1}^{N} V(X(i), k, j) T_{\dot{k}}(X(i))}{\sum_{i=1}^{N} V(X(i), k, j)} - \frac{\sum_{i=1}^{N} (1 - V(X(i), k, j)) T_{\dot{k}}(X(i))}{\sum_{i=1}^{N} (1 - V(X(i), k, j))} \tag{2}$$

where k is a guessed sub-key from which the attacker attempts to reveal the real sub-key $\dot{k}$. In the real attack k takes all the possible values. There is a statistical correlation between the differential trace and the real power consumption. V is a leakage binary function that depends on the known plain-text and the selected $j - th$ bit.

The power leakage models used more often in side-channels attacks by power consumption are the Hamming Distance model and the Hamming Weight model [1]. The Hamming Distance model is interpreted as the result of the function $HW(\beta \oplus F(in \oplus k))$, where β is a logic pre-charge of the cipher device, in represents the input text, and k the sub-key used in the encryption process. The Hamming weight function $HW(z)$, $z \in \{0, 1\}^m$, computes the number of ones in the boolean vector z of m components. In case of $\beta = \{0\}^m$, the model resulting of the function $HW(F(in \oplus k))$, is renamed as Hamming Weight model.

B. PROPERTIES OF S-BOXES

In this subsection we review some relevant properties of S-boxes with respect to classical and side-channel attacks.

1) SIDE-CHANNEL RELATED PROPERTIES

The Confusion Coefficient metric was first introduced in [6]. This metric is computed for sub-keys k_i and k_j as:

$$\kappa(k_i, k_j) = E[(W(k_i) - W(k_j))^2] \tag{3}$$

where W represents the leakage function of the encryption process, given an arbitrary input and the sub-key k. Later on, in [7], the Confusion Coefficient Variance (CCV) was introduced, using the confusion coefficient (3) and the Hamming Weight power model, to simulate the leakages $W(k_i)$ and $W(k_j)$. The formula, for all sub-keys k_i, k_j, $k_i \neq k_j$ and all input text in, is:

$$CCV(F) = Var(E[(HW(F(in \oplus k_i)) - HW(F(in \oplus k_j)))^2]) \tag{4}$$

Then, the Transparency Order (TO) was introduced in [2]. This property tries to catch the intrinsic S-box resistance against DPA attacks under the Hamming Distance power model. Although the deficiencies found in its formula deduction [3], where the original formulation was reduced, and the property does not reflect anymore the resistance under

Hamming Distance power model, the metric still can be used to measure the theoretical resistance of an S-box against DPA under the Hamming Weight model in a fast way [11].

In [3], the TO was modified because of some deficiencies in its definition. The newly created property was known as Modified Transparency Order (MTO), and it takes into account the cross-correlation spectrum of the coordinate functions of the S-box $F = (f_1, \ldots, f_m)$, denoted by

$$C_{f_i,f_j}(\alpha) = \sum_{x \in \{0,1\}^n} (-1)^{f_i(x) \oplus f_j(x \oplus \alpha)}.$$

The property is computed as:

$$MTO(F) = max_{\beta \in \{0,1\}^m}(MTO(F, \beta)) \tag{5}$$

where

$$MTO(F, \beta)$$
$$= m - \frac{1}{2^{2^n} - 2^n} \sum_{\alpha \in \{0,1\}^n - \{0\}^n} \sum_{j=1}^{m} \Big| \sum_{i=1}^{m} (-1)^{\beta_i \oplus \beta_j} C_{F_i,F_j}(\alpha) \Big|.$$

The Modified Transparency Order represents the theoretical resistance against a Side-Channel Attack by Power Consumption under the Hamming Distance power model. In particular, when $MTO(F)$ uses only $\beta = \{0\}^m$ and discards all other possible β values, it's denoted by (MTO_0 or $MTO(F, \{0\}^m)$), and the Hamming Distance model is reduced to the Hamming Weight power model. The MTO property assumes a DPA *multi-bit* attack (see expression (1)) in the form of

$$\sum_j |\Delta_{k,\dot{k}}(N, j)|.$$

In the same fashion as MTO, the Revised Transparency Order represents the theoretical resistance against Side-Channel Attack by Power Consumption under the Hamming Distance power model and tries to solve the TO deficiencies. But like TO, it assumes the DPA *multi-bit* in the form of

$$\Big| \sum_j \Delta_{k,\dot{k}}(N, j) \Big|.$$

(see expression 1). The property is computed as follow:

$$RTO(F) = max_{\beta \in \{0,1\}^m}(RTO(F, \beta)) \tag{6}$$

where

$$RTO(F, \beta)$$
$$= m - \frac{1}{2^{2^n} - 2^n} \sum_{\alpha \in \{0,1\}^n - \{0\}^n} \Big| \sum_{j=1}^{m} \sum_{i=1}^{m} (-1)^{\beta_i \oplus \beta_j} C_{F_i,F_j}(\alpha) \Big|.$$

When $RTO(F)$ uses only $\beta = \{0\}^m$ and discards all other β values, it's denoted by (RTO_0 or $RTO(F, \{0\}^m)$) and the Hamming Distance model is reduced to the Hamming Weight model.

2) LOCAL SEARCH TRAJECTORIES OVER S-BOX SPACE

Running a local search method to optimize one S-box property can produce a trajectory of points if a second property is also measured at each climbing. This trajectory can be used to study correlations between the two properties across the solution space. As an statistical methodology, this particular use of meta-heuristic was first used in [16], finding strong linear correlations between CCV vs MTO_0, and CCV vs RTO_0.

3) NON-LINEARITY AND DIFFERENTIAL UNIFORMITY

The Walsh-Hadamard transform of a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ (an special case of S-box, when $m = 1$) is defined as:

$$WH_f(w) = \sum_{x \in \{0,1\}^n} \hat{f}(x)\hat{L_w}(x), \tag{7}$$

where $\hat{f}$ represents the polar form of the Boolean function f and $\hat{L_w}$ is a linear function specified by w [1]. The maximum value of Walsh-Hadamard transform for a Boolean function f is denoted by

$$WH_{max}(f) = max_{w \in \{0,1\}^n} \|WH_f(w)\|, \tag{8}$$

in which $\| \ldots \|$ represents the absolute value.

The Non-Linearity (NL) of a Boolean function f is defined as:

$$NL(f) = \frac{1}{2}(2^n - WH_{max}(f)). \tag{9}$$

Then, the Non-Linearity of an S-Box $F = (f_1, \ldots, f_m)$ is the lowest value of Non-Linearity among the non-trivial linear combinations of its coordinate functions.

The Differential Uniformity (DU) of an S-Box F is calculated as follows

$$DU(F) = max_{a \in \{0,1\}^n, a \neq \{0\}^n, b \in \{0,1\}^m} DU(a, b), \tag{10}$$

where $DU(a, b) = |\{x \in \{0, 1\}^n | F(x \oplus a) \oplus F(x) = b\}|$.

C. HILL CLIMBING ALGORITHM

Hill climbing is a meta-heuristic method. In the general scheme [18], the method starts from a random initial solution s^*, it creates a neighborhood solution $\dot{s}$ using an operator, and moves to it if the objective function σ decreases (or increases in case of maximization). This action is repeated until a given threshold number of iterations is reduced to zero (see Algorithm 1).

A common used *operator* applied with this method is the swap *operator* [19]. Given a solution s^* as a permutation and two random positions $i, j; i \neq j$ the swapped solution $\dot{s}$ is defined as:

$$\dot{s} = swap(s^*) = \begin{cases} \dot{s}(i) \leftarrow s^*(j) \\ \dot{s}(j) \leftarrow s^*(i) \\ \dot{s}(x) \leftarrow s^*(x), \forall x | x \neq i, x \neq j. \end{cases} \tag{11}$$

Algorithm 1 General Scheme of the Hill Climbing Algorithm

```
Require: $thresholdnumber$, $operator$
Ensure: $s^*$ // Local optimum
s* ← random()
search ← true
while $thresholdnumber > 0$ do
    $\dot{s} \leftarrow operator(s^*)$
    if $\sigma(\dot{s}) < \sigma(s^*)$ then
        $s^* \leftarrow \dot{s}$
    end if
    $thresholdnumber \leftarrow thresholdnumber - 1$
end while
return $s^*$
```

III. IMPROVED OBJECTIVE FUNCTIONS. EXPERIMENT, RESULTS AND DISCUSSION

To apply Algorithm 1, we set the *thresholdnumber* to 3000 and we use a swap *operator* over a solution (S-box) represented as a permutation array of values ranging from 0 to $2^n - 1$. We also set the S-box space to 8 × 8 or 8-bit S-box space. For every objective function that we present, we run Algorithm 1 30 times, and we measure the minimum, the maximum, the average and the standard deviation over the cryptographic properties.

A. NEW OBJECTIVE FUNCTION BASED ON MTO

First, we define a new objective function based in MTO property as follows:

$$\sigma_1(F) = MTO_0 + max_{\beta \in \{0,1\}^m}(MTO(F, \beta)). \qquad (12)$$

Equation (12) can be qualified as optimal from a computational point of view because it uses the MTO_0 value from the MTO formula to obtain the $\sigma_1(F)$ value, in other words, the computational effort to compute MTO is almost the same to compute σ_1.

$$max_{\beta \in \{0,1\}^m}(MTO(F, \beta)),$$

then the $MTO(F, \{0\}^m)$ value is already calculated and can be reused to obtain the $\sigma_1(F)$ value. In order to optimize both, the theoretical resistance under the Hamming Distance model and the Hamming Weight model, the function σ_1 tries to address the multi-objective optimization problem in a linear scalarization fashion. We gather the values of the properties MTO, MTO_0, RTO, RTO_0, CCV, NL and DU for all S-boxes once all the experiments are concluded. The average values and the standard deviation of the obtained S-boxes are shown in Table 1.

Table 1 shows a low average value of MTO (6.71) in comparison with the values obtained in [17] (6.86) and in [14] (6.88). The average value of CCV is high as expected, given the correlation with the MTO_0 minimization, also higher than the value obtained in [7] (4.057). The standard deviation of the MTO values and MTO_0 values are low, but the standard deviation of the CCV values is high, which is not good for the solution's stability in meta-heuristic search.

TABLE 1. Descriptive statistics of the properties of S-boxes obtained using σ_1 objective function.

Property	Min.	Max.	Ave.	Std.
MTO	6.43	6.88	6.71	0.13
MTO_0	2.99	3.63	3.27	0.17
RTO	7.37	7.52	7.46	0.04
RTO_0	3.23	5.36	3.81	0.57
CCV	2.68	5.79	4.84	0.75
NL	34	86	58.6	17.67
DU	12	16	12.93	1.26

The average value of NL is low and the average value of DU is high, which are not good in terms of cryptography designs. However, we remark that our search did no try to optimize them.

B. NEW OBJECTIVE FUNCTION BASED ON RTO

We also define another variant of the objective function using the RTO property. The function is given by

$$\sigma_2(F) = RTO_0 + max_{\beta \in \{0,1\}^m}(RTO(F, \beta)). \qquad (13)$$

The function σ_2 is also optimal from a computational point of view because we can apply the same principle that we apply for function σ_1. Table 2 shows the results using the objective function σ_2. The average CCV value is higher and the standard deviation lower than the results obtained using the objective function σ_1. This represent a better correlation between RTO_0 and CCV, when the RTO_0 values are decreased then the CCV values further increased. All the standard deviations are better that the ones shown in Table 1. The NL shows good average results and a low standard deviation, which implies that, although the NL value is low, the RTO property is more suitable for a trade-off for S-box design.

TABLE 2. Descriptive statistics of the properties of S-boxes obtained using σ_2 objective function.

Property	Min.	Max.	Ave.	Std.
MTO	6.78	6.86	6.82	0.02
MTO_0	3.23	3.56	3.37	0.08
RTO	7.41	7.45	7.43	0.01
RTO_0	3.23	3.56	3.37	0.08
CCV	4.95	5.72	5.46	0.19
NL	84	90	87.33	2.12
DU	10	14	11.53	1.01

In both cases, the NL and DU metrics were denigrated. The MTO, MTO_0, RTO, RTO_0 and CCV, show good values.

C. BEST S-BOXES

The best S-boxes obtained by apply Algorithm 1 with each objective function (F_{σ_1} and F_{σ_2}) are shown in the Appendixes I and II respectively. Table 3 shows a comparison between ours S-boxes and others S-boxes in the literature. For a visual understanding of the balance between properties, see Fig. 1, a radar chart where each axis represents a property and the point values are in percent of the best value showed in the Table 3; example, the red radial quadrilateral of the AES's S-box has 100% on non-linearity but low percent on the other

TABLE 3. Comparison between S-boxes obtained using σ_1 and σ_2 objective functions with others S-boxes in the literature.

Source	Random start	Balanced search	MTO	MTO_0	NL	CCV
AES Rijndael	-	-	6.92	6.87	112	0.11
[20]	No	Yes (MTO; NL)	6.38	6.34	102	0.39
[15]	Yes	Yes (CCV; NL)	6.92	4.63	100	4.5
This paper σ_2	Yes	Yes (RTO; RTO_0)	6.83	3.23	90	5.72
This paper σ_1	Yes	Yes (MTO; MTO_0)	6.73	3.08	58	5.79
[12]	Yes	No	6.88	3.23	32	6.65

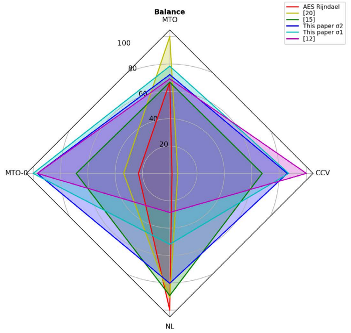

FIGURE 1. Percent of the properties values with their better values.

properties, so its balance is not good. The S-box presented in [20] has the best MTO value and also the best balance between MTO and NL, however the values of MTO_0 and CCV are not good, representing a poor resistance against side-channels attacks under the Hamming Weight leakage model. In [15], Freyre *et al.* found the S-box with best balance between CCV and NL, but it lacks in similar issue of the previous S-box, the MTO value is not good (same as the MTO value of AES Rijandel), which represent a poor resistance against side-channels attacks under the Hamming Distance leakage model. An S-box with a high CCV value is presented in [12], also the MTO_0 value is good because the two properties are defined under the Hamming Weight leakage model; this S-box carries the worst NL value and the MTO is not so good. Finally, our S-boxes show the best balance between MTO, MTO_0 and CCV values; the NL values are not good because the property was not included in the objective functions as we remark in this work.

IV. CONCLUSION

Our results show that the objective functions that we propose can be used to search for 8 × 8 bijective S-boxes with high theoretical resistance against Side-Channels Attacks under both leakage models: Hamming Weight and Hamming Distance. We also show that Revised Transparency Order is a more accurate metric than Modified Transparency Order to measure Side-Channel resistance to power attacks, because its improvement has less impact on the Non-Linearity degradation. A new line of investigation will be a trade-off using our new optimal objective functions to optimize Non-Linearity and Delta Uniformity properties.

APPENDIX I. BEST S-BOX FOUND USING σ_1

MTO = 6.73; CCV = 5.79; MTO_0 = 3.08; RTO = 7.49 and RTO_0 = 3.23.

F_{σ_1} = {50, 73, 32, 192, 190, 46, 109, 29, 170, 174, 199, 47, 23, 74, 212, 98, 160, 105, 56, 9, 247, 124, 122, 201, 203, 244, 243, 229, 13, 26, 16, 148, 112, 24, 85, 133, 103, 253, 86, 237, 126, 123, 110, 116, 152, 149, 197, 69, 150, 44, 25, 88, 233, 205, 250, 182, 223, 31, 156, 202, 34, 130, 161, 225, 162, 168, 113, 43, 207, 119, 218, 118, 173, 191, 246, 227, 136, 14, 89, 51, 66, 80, 99, 97, 155, 61, 248, 30, 157, 188, 171, 78, 0, 19, 145, 27, 131, 35, 10, 18, 195, 92, 217, 158, 94, 211, 87, 251, 53, 37, 42, 8, 194, 11, 64, 142, 154, 184, 185, 55, 220, 95, 79, 107, 169, 135, 137, 128, 238, 125, 114, 206, 164, 36, 193, 7, 146, 72, 82, 178, 189, 111, 228, 115, 235, 181, 219, 108, 40, 6, 39, 84, 166, 134, 76, 96, 255, 239, 198, 254, 177, 59, 252, 93, 196, 90, 200, 28, 100, 67, 132, 81, 172, 214, 63, 234, 102, 230, 139, 221, 65, 41, 70, 68, 58, 77, 20, 45, 232, 242, 236, 117, 222, 91, 143, 121, 75, 141, 3, 176, 22, 153, 49, 147, 151, 226, 213, 249, 54, 186, 175, 245, 21, 5, 52, 208, 106, 209, 4, 104, 210, 62, 167, 183, 215, 163, 216, 204, 12, 1, 48, 71, 38, 224, 101, 17, 159, 240, 120, 180, 127, 57, 231, 241, 2, 129, 83, 165, 33, 138, 140, 144, 15, 187, 60, 179}

APPENDIX II. BEST S-BOX FOUND USING σ_2

RTO = 7.44; CCV = 5.72; RTO_0 = 3.23; MTO = 6.84 and MTO_0 = 3.23.

F_{σ_2} = {1, 17, 12, 196, 67, 200, 2, 193, 131, 43, 34, 10, 195, 170, 116, 26, 199, 172, 53, 139, 217, 214, 201, 93, 71, 101, 51, 190, 141, 223, 109, 62, 159, 111, 207, 188, 75, 169, 243, 31, 174, 233, 238, 83, 63, 246, 59, 231, 21, 64, 90, 6, 156, 48, 152, 36, 41, 24, 37, 0, 138, 144, 112, 162, 245, 125, 47, 107, 203, 180, 255, 155, 147, 242, 92, 171, 115, 186, 127, 205, 7, 85, 133, 25, 108, 40, 33, 130, 19, 20, 99, 160, 35, 76, 49, 142, 164, 153, 86, 89, 74, 4, 106, 80, 240, 3, 96, 192, 44, 149, 11, 204, 206, 103, 166, 58, 126, 189, 178, 167, 226, 235, 227, 57, 225, 183, 247, 181, 151, 253, 254, 221, 118, 61, 77, 241, 114, 249, 198, 117, 163, 79, 94, 154, 136, 50, 97, 228, 69, 134, 70, 137, 54, 176, 113, 73, 98, 38, 102, 177, 14, 65, 202, 88, 13, 5, 28, 16, 104, 8, 146, 140, 56, 23, 209, 145, 122, 219, 78, 124, 232, 158, 55, 157, 119, 123, 237, 45, 236, 191, 212, 250, 82, 42, 168, 148, 184, 100, 66, 32, 46, 129, 52, 224, 208, 210, 39, 128, 105, 182, 29, 252, 91, 143, 87, 60, 230, 220, 185, 222, 95, 239, 121, 234, 187, 248, 218, 110, 211, 150, 173, 244, 30, 215, 229, 197, 179, 251, 213, 175, 22, 72, 15, 132, 81, 120, 216, 135, 9, 161, 27, 18, 165, 194, 84, 68}

REFERENCES

[1] H. Van Tilborg, Ed., *Encyclopedia of Cryptography and Security*. New York, NY, USA: Springer, 2011, doi: 10.1007/978-1-4419-5906-5.

[2] E. Prouff, "DPA attacks and S-boxes," in *Proc. Int. Workshop Fast Softw. Encryption*. Berlin, Germany: Springer, 2005, pp. 424–441.

[3] K. Chakraborty, S. Sarkar, S. Maitra, B. Mazumdar, D. Mukhopadhyay, and E. Prouff, "Redefining the transparency order," *Designs, Codes Cryptogr.*, vol. 82, nos. 1–2, pp. 95–115, Jan. 2017.

[4] K. Nyberg, "Differentially uniform mappings for cryptography," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1993, pp. 55–64.

[5] S. Picek, "Applications of evolutionary computation to cryptology," Ph.D. dissertation, Fac. Elect. Eng. Comput. Dept. Electron., Microelectron., Comput. Intell. Syst., Univ. Zagreb, Zagreb, Croatia, 2015.

[6] Y. Fei, Q. Luo, and A. A. Ding, "A statistical model for DPA with novel algorithmic confusion analysis," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2012, pp. 233–250.

[7] S. Picek, K. Papagiannopoulos, B. Ege, L. Batina, and D. Jakobovic, "Confused by confusion: Systematic evaluation of DPA resistance of various S-boxes," in *Proc. Int. Conf. Cryptol. India*. Cham, Switzerland: Springer, 2014, pp. 374–390.

[8] L. Lerman, O. Markowitch, and N. Veshchikov, "Comparing sboxes of ciphers from the perspective of side-channel attacks," in *Proc. IEEE Asian Hardw.-Oriented Secur. Trust (AsianHOST)*, Dec. 2016, pp. 1–6.

[9] A. Heuser, O. Rioul, and S. Guilley, "A theoretical study of Kolmogorov-Smirnov distinguishers," in *Proc. Int. Workshop Constructive Side-Channel Anal. Secure Design*. Cham, Switzerland: Springer, 2014, pp. 9–28.

[10] H. Li, Y. Zhou, J. Ming, G. Yang, and C. Jin, "The notion of transparency order, revisited," *Comput. J.*, vol. 63, no. 12, pp. 1915–1938, Dec. 2020.

[11] I. M. Díaz and C. M. Legón, "Acelerando el cálculo del orden de transparencia," COMPUMAT. Sociedad Cubana de Matemática y Computación, 2017.

[12] I. M. Díaz, "Búsqueda local de S-cajas con alta varianza del coeficiente de confusión," M.S. thesis, Facultad de Matemática y Computación, Universidad de la Habana, Havana, Cuba, 2019.

[13] B. Mazumdar and D. Mukhopadhyay, "Construction of rotation symmetric S-boxes with high nonlinearity and improved DPA resistivity," *IEEE Trans. Comput.*, vol. 66, no. 1, pp. 59–72, Jan. 2017.

[14] S. Picek, B. Yang, and N. Mentens, "A search strategy to optimize the affine variant properties of S-boxes," in *Proc. Int. Workshop Arithmetic Finite Fields*. Cham, Switzerland: Springer, 2016, pp. 208–223.

[15] A. Freyre-Echevarria, I. Martinez-Diaz, C. M. L. Perez, G. Sosa-Gomez, and O. Rojas, "Evolving nonlinear S-Boxes with improved theoretical resilience to power attacks," *IEEE Access*, vol. 8, pp. 202728–202737, 2020.

[16] I. Martínez-Díaz and C.-M. Legón, "Local search trajectories over S-box space," 2020, *arXiv:2004.07635*.

[17] S. Picek, B. Mazumdar, D. Mukhopadhyay, and L. Batina, "Modified transparency order property: Solution or just another attempt," in *Proc. Int. Conf. Secur., Privacy, Appl. Cryptogr. Eng.* Cham, Switzerland: Springer, 2015, pp. 210–227.

[18] M. Lones, "Sean Luke: Essentials of metaheuristics," *Genet. Program. Evolvable Mach.*, vol. 12, pp. 333–334, Sep. 2011, doi: 10.1007/s10710-011-9139-0.

[19] E. G. Talbi, *Metaheuristics: From Design to Implementation*, vol. 74. Hoboken, NJ, USA: Wiley, 2009.

[20] Xu, Youle, and Qichun Wang., "Searching for balanced S-boxes with high nonlinearity, low differential uniformity, and improved DPA-resistance," in *Proc. Int. Conf. Inf. Secur.* Cham, Switzerland: Springer, 2020, pp. 95–106.

[21] Y. Zhou, Y. Wei, H. Zhang, and W. Zhang, "On the modified transparency order of-functions," *Secur. Commun. Netw.*, vol. 2021, Jan. 2021, Art. no. 6640099.

[22] Y. Zhou, J. Hu, X. Miao, Y. Han, and F. Zhang, "On the confusion coefficient of Boolean functions," *J. Math. Cryptol.*, vol. 16, no. 1, pp. 1–13, Aug. 2021.

[23] Y. Zhou, Y. Wei, H. Zhang, L. Li, E. Pasalic, and W. Wu, "Transparency order of (n, m)-functions—Its further characterization and applications," in *Information Security* (Lecture Notes in Computer Science), vol. 13118, J. K. Liu, S. Katsikas, W. Meng, W. Susilo, and R. Intan, Eds. Cham, Switzerland: Springer, 2021, doi: 10.1007/978-3-030-91356-4_8.

[24] J. A. Clark, "Metaheuristic search as a cryptological tool," Ph.D. dissertation, Dept. Comput. Sci., Fac. Sci., Univ. York, York, U.K., 2002.

ISMEL MARTÍNEZ-DÍAZ received the M.Sc. degree in computer science from the University of Havana, in 2019. His current research interests include methauristics and mathematical objects design.

ALEJANDRO FREYRE-ECHEVARRÍA was born in Havana, Cuba, in 1994. He received the Bachelor of Science degree in computer sciences, in July 2020. He defended his thesis for the grade of Bachelor of Science degree. He has been an Active Researcher with the Institute of Cryptography, University of Havana, since 2018. His research interests include cryptographic boolean functions and S-boxes, side-channel attacks, and combinatorial optimization algorithms.

OMAR ROJAS received the Ph.D. degree in mathematics from La Trobe University, Australia. He is a Titular Professor interested in applied mathematics and Professor in Universidad Panamericana.

GUILLERMO SOSA-GÓMEZ received the bachelor's degree in mathematics and the master's degree in applied mathematics from Central University, Cuba, and the Doctor of Science degree from the Mathematics Research Center, A.C. (CIMAT). He works in the areas of code theory, heuristics, smart business, cryptography, blockchain, algebraic geometry, and computer security.

CARLOS MIGUEL LEGÓN-PÉREZ received the Ph.D. degree in mathematical sciences and the M.Sc. degree in cryptography from the University of Havana, in 1997 and 2019, respectively. His current research interests include graphical authentication, cryptographic randomness, probabilistic models, information theory, and side channels attack's, such as DPA and biased fault.

• • •