Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

Tipo de artículo: Artículo originales
Temática: Seguridad informática
Recibido: 07/11/2022 | Aceptado: 27/12/2022 | Publicado: 17/02/2023

Revisiting the built-in resistance of S-Boxes against Correlation Power Analysis

Revisión de la resistencia incorporada de las S-Cajas contra el análisis por correlación de potencias

Alejandro Freyre Echevarría 0000-0002-0537-9430[1*]
Ramsés Rodríguez Aulet 0000-0001-7653-324X[2]

[1]Instituto de Criptografía. Universidad de la Habana. freyreealejandro@gmail.com
[2]Instituto de Criptografía. Universidad de la Habana. ramsesrusia@yahoo.com
[*]Autor para correspondencia: (freyreealejandro@gmail.com)

En memoria de Nelson Díaz Pérez.
Padre, hermano y amigo.

ABSTRACT

The design of substitution boxes having built-in resistance against side-channel attacks is an active field of research. In the course of the last ten years several theoretical properties of substitution boxes to measure this resistance have been enunciated being the confusion coefficient variance one of the most relevant. The majority of the substitution boxes generated under the confusion coefficient variance criteria shows, indeed, a certain level of resistance against a correlation power analysis, however they are conceived only for the encryption process while its inverse, which is used for decryption, is often not taken into account. This may result in a vulnerability of the algorithm during the decryption process. In this paper we conduct an analysis of the built-in resistance of 8-bit substitution boxes and their inverses in a side-channel scenario using the state of the art results in this topic. Moreover, we introduce a new method for generating high nonlinear substitution boxes having theoretical built-in resistance against correlation power analysis as well as their inverses.

Keywords: S-Boxes; correlation power analysis; confusion coefficient variance; heuristic method.

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

RESUMEN

El diseño de S-Cajas con resistencia incorporada contra ataques de canal lateral es un campo activo de investigación. En el transcurso de los últimos diez años se han enunciado varias propiedades teóricas de las S-Cajas para medir esta resistencia siendo la varianza del coeficiente de confusión una de las más relevantes. La mayoría de las S-Cajas generadas bajo el criterio de varianza del coeficiente de confusión muestran, de hecho, un cierto nivel de resistencia frente a un análisis por correlación de potencias, sin embargo, están concebidas solo para el proceso de cifrado mientras que su inversa, que se utiliza para el descifrado, a menudo no es considerada. Esto puede resultar en una vulnerabilidad del algoritmo durante el proceso de descifrado. En este artículo llevamos a cabo un análisis de la resistencia incorporada de las S-Cajas de 8 bits y sus inversas en un escenario de canal lateral utilizando los resultados del estado del arte en este tema. Además, presentamos un nuevo método para generar S-Cajas altamente no lineales que tienen una resistencia teórica incorporada contra el análisis por correlación de potencias, así como sus inversas.

Palabras clave: S-Cajas; análisis por correlación de potencia; varianza del coeficiente de confusión; método heurístico.

Introduction

Side-channel attacks Rijsdijk et al. (2021); Picek et al. (2021); Randolph and Diehl (2020); Sayakkara et al. (2019); Zaid et al. (2021) have proven to be effective towards symmetric cryptographic algorithms which by mathematical definition are resistant to classical cryptanalytic techniques such as linear Matsui (1993), differential Biham and Shamir (1991) or algebraic Armknecht (2004) cryptanalysis. In the majority of cases, side-channel attacks take advantage of the leakages made by the main nonlinear component of most implementations of block ciphers, the substitution box or simply S-Box. Through the years, the scientific community define a set of theoretical cryptographic properties for S-Boxes which attempt to measure the built-in resistance of these components in a side-channel scenario. Examples of such properties are SNR(DPA) Guilley et al. (2004), transparency order Prouff (2005), confusion coefficient variance Picek et al. (2014) modified transparency order Chakraborty et al. (2017), revised transparency order Li et al. (2020) and non-absolute indicator Carlet et al. (2020). Although they cannot be count as a countermeasure, like masking Golić and Tymen (2002); Bilgin et al. (2020), S-boxes having a good value of these properties show some resistance

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

against power attacks.

There exist several papers in the literature survey which study the effect of these properties in the practical resistance of S-Boxes against a side-channel attack Picek et al. (2014); Lerman et al. (2016); Díaz (2019); Freyre-Echevarría et al. (2020); Li et al. (2021). Hence, one may think that generating a substitution box that is, in some way, resistant to side-channel attacks solves the problem, however it is not the case. Most of the aforementioned papers, with the exception of the work from Lerman et al. (2017) for the case of small size S-Boxes, take into account the inverse S-Box, i.e. the one used in the decryption process, therefore a side-channel attack can exploit the leakages made by such S-Box, since as far as we know it is not optimized to be resistant in a side-channel scenario.

In this paper we present an analysis of the built-in resistance of 8-bit S-Boxes to Correlation Power Analysis (CPA) under the Hamming weight leakage model using the confusion coefficient variance as the target property of our study. We show that the S-Boxes referred in the literature have weak inverses w.r.t the CPA attack reflected in their poor confusion coefficient variance. To practically test these S-Boxes, we conduct the corresponding CPA attack on the encryption and decryption process of the AES algorithm Daemen and Rijmen (2020) supporting our experiments in the simulated power traces obtained through the SILK leakage simulator from Veshchikov (2014). Finally, we introduce some methods which ensure that both, the S-Box and its inverse, will have a built-in resistance to CPA, also guaranteeing good values of their mathematical properties like nonlinearity and differential uniformity.

1 Preliminaries

Let denote as $\mathbb{F}_2 = \{0,1\}$ the finite field with two elements; $\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$. One S-Box S is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, i.e. $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$, where S can be decomposed as the parallelization of $\mathbf{m}$ n-variable Boolean functions $S = (f_1, f_2, \cdots, f_m)$ known as coordinate functions of S. We say that S is balanced when each value $x \in \mathbb{F}_2^m$ appears the same number of 2^{n-m} times. When $n = m$, it is usual that S is a bijective mapping from $\mathbb{F}_2^n$ to itself, i.e, that each output appears exactly once. Such S-Boxes are permutations on $\mathbb{F}_2^n$ Carlet et al. (2010). In this paper we study the case of bijective 8-bit S-Boxes only, although our results can be extended to other S-Box dimensions.

Given any bijective S-Box $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$, its inverse S-box, is the S-Box $S^{-1} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that if $S(x) = y$ then $S^{-1}(y) = x$, having $x, y \in \mathbb{F}_2^n$. We say that S is an involutive mapping from $\mathbb{F}_2^n$ to itself iif $S^{-1} = S$, i.e.

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

$S(S(x)) = x, \forall\, x \in \mathbb{F}_2^n$.

Basic properties of S-Boxes

The Walsh-Hadamard transform of one S-Box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is defined as Carlet et al. (2010):

$$\mathscr{W}_S(x,y) = \sum_{z \in \mathbb{F}_2^n} (-1)^{\langle y, S(z)\rangle \oplus \langle x,z\rangle} \tag{1}$$

where $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2^{m*} = \mathbb{F}_2^m \setminus \{0\}$ and $\langle a,b\rangle = \oplus_{i=1}^{k} a_i b_i$ is the inner product of the vectors $a,b \in \mathbb{F}_2^k$. Here, $(\oplus)$ represents the addition modulo two or bitwise e**X**clusive **OR** (XOR).

The nonlinearity of S is related to the maximum absolute value of its Walsh-Hadamard transform Carlet et al. (2010):

$$\mathscr{N}_S = 2^{n-1} - \frac{1}{2} \max_{x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^{m*}} |\mathscr{W}_S(x,y)| \tag{2}$$

For any S-box $S : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and any $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^m$ one can define Nyberg (1991):

$$\delta(x,y) = \#\{z \in \mathbb{F}_2^n : S(x \oplus z) \oplus S(z) = y\} \tag{3}$$

where the multi-set $\Delta_S = \{x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m : \delta(x,y)\}$ represents the differential spectrum of S, and its maximum:

$$\delta_S = \max_{x \neq 0, y} \delta(x,y) \tag{4}$$

is called the differential uniformity of S.

Confusion coefficient variance

The confusion coefficient Fei et al. (2012, 2014), 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 related models using the confusion coefficient, the vector

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

containing all confusion coefficients concerning 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.* Picek et al. (2014) 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 $\mu, \mathsf{k_a}, \mathsf{k_b} \in \mathbb{F}_2^n$ and $\mathsf{k_a} \neq \mathsf{k_b}$ as:

$$\kappa(\mathsf{S}) = \mathsf{Var}(\mathsf{E}[(\mathsf{w}_{\mathscr{H}}(\mathsf{S}(\mu \oplus \mathsf{k_a})) - \mathsf{w}_{\mathscr{H}}(\mathsf{S}(\mu \oplus \mathsf{k_b})))^2]) \tag{5}$$

where one can identify μ as the piece of plain text, $\mathsf{k_a}, \mathsf{k_b}$ are two different sub-key guesses and $\mathsf{w}_{\mathscr{H}}$ denotes the Hamming weight of a vector in $\mathbb{F}_2^n$.

2 Analysis on the state of the art S-Boxes

Most of the side-channel analysis referred in literature survey target the 128-bit unprotected implementation of AES. Although such attacks are effective to fully recover the 128-bit key, for larger key sizes the complexity of the attack substantially raise Wurcker (2019). However, the work from Wurcker Wurcker (2019) introduce a method to recover 192/256 bit keys on AES from the knowledge of the first and last round keys with a high probability of success. Hence attacking both, first round of encryption and first round of decryption, one can obtain the pieces of the key from which Wurcker's method can retrieve an AES key larger than 128 bits. Since it have no significance towards our results we perform our experiments using a 128-bit key for AES algorithm, for the sake of simplicity.

As we aforementioned, the target of a side-channel attack is often the leakages produced by the S-Boxes while information is processed by the encryption algorithm. To prevent such leakages, some S-Boxes have been tuned to be, in some sense, resistant to side-channel attacks. In addition, is proven that one the S-Box and its inverse, maintain equal values of nonlinearity and differential uniformity Carlet et al. (2010), which means that the mathematical resistance of both remains the same for encryption and decryption process. However, a different scenario is shown when it comes to side-channel resistance.

In Table 1 we present the confusion coefficient variance values of different S-Boxes which were optimized to have a high value of this property as well as the confusion coefficient variance value of their respective inverses. The gap between both values is clearly distinguishable for the lecturer since as one is to high the other poorly exceed **0.1**. As shown in Picek et al. (2014); Díaz (2019); Freyre-Echevarría (2020); Prinetto and Cerini (2021) the original S-Boxes present some level of resistance to the CPA attack and therefore it will be

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

Table 1 - Comparison of the confusion coefficient variance of various S-Boxes and their respective inverses.

Reference	$\kappa(S)$	$\kappa(S^{-1})$
Picek et al. (2014)	4.057	0.105
Díaz (2019)	6.649	0.111
Freyre-Echevarría et al. (2020)	4.500	0.136
Freyre-Echevarría (2020)	4.355	0.101

harder for the attacker to fully recover the key. In counterpart, the results in Table 1 w.r.t. the inverse S-Boxes lead to the following question: *can we attack the decryption process instead?* Unfortunately the answer is *yes* and then the encryption key can be recovered from the knowledge of the last round key of the algorithm obtained by attacking the decryption process where S-Boxes are weak.

In the next subsection we introduce the experimental results made on the inverse S-Boxes referred in Table 1 using the SILK leakage simulator Veshchikov (2014) where simulated power traces were collected while both encryption and decryption processes were running.

2.1 CPA attack on the decryption process

In our simulated experiments we target the leakages made by the *SubBytes* (resp. *InvSubBytes*) transformation of AES relating each of the leakages to the function

$$y = \mathsf{F}(k \oplus x)$$

where $x, y, k \in \mathbb{F}_2^n$, k is the corresponding sub-byte of the key and F is the action of the corresponding S-Box for the encryption or decryption process. We set up the SILK simulator to work in the Hamming weight power model measuring the Hamming weights of the outputs of each transformation of AES. To establish the fairest comparison of the targeted S-Boxes we use the following configuration of SILK:

- Key: `0x8091a2b3c4d5e6f708192a3b4c5d6e7f`.
- Instruction overlapping: 0.
- Leakage points per instruction: 1.
- Leakage distribution function: $\frac{l \cdot sin(t)}{2}$, where l denotes the leakage at instant t of time.
- Noise variance of the system: 3 as suggested in Lerman et al. (2016).

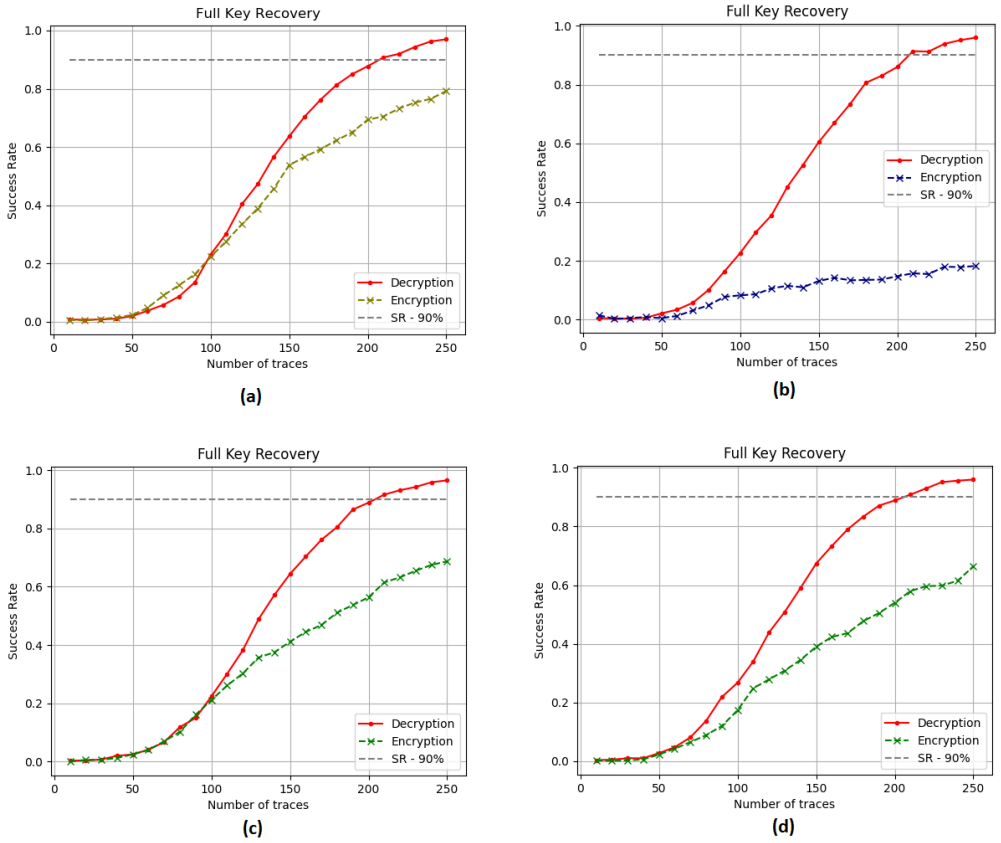

Fig. 1 - Comparison between the results of the correlation power analysis on the encryption and decryption process of AES-128 using the S-Boxes from Table 1: **(a)** Picek et al. (2014), **(b)** Díaz (2019), **(c)** Freyre-Echevarría (2020), **(d)** Freyre-Echevarría et al. (2020)

- Simulated power traces collected: 250.
- Number of experiments per S-Box: 50.

It worth to remark that the side-channel leakage is statistically dependent on the intermediate values which involved certain information about the secret key, which make the last recoverable from the analysis of the measured data Carlet et al. (2017). However we do not consider necessary to use diffent keys in our experiments given that confusion coefficient variance encapsulate all possible combinations of plain text and sub-key guesses as shown in equation (5). While in the first attack we try to recover the 128-bit key used in the encryption process, in the second attack we search for the last round key of the algorithm since the

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

encryption key is recoverable from the knowledge of one of the intermediate round keys. Once conducted the corresponding side-channel experiments on each S-Box from Table 1 and its respective inverse we use the notion of first order Success Rate (**SR**) Standaert et al. (2009) to evaluate the results of the correlation power analysis w.r.t the full recovery of the key as shown in Figure 1.

It can be seen that **SR** curves of the decryption process (using the inverse S-Boxes) indicate the recovery of more than 90% of the secret key while its counterpart, the original S-Box optimized w.r.t the confusion coefficient variance, still show some level of resistance towards the power analysis. We like to remark the case of the S-Box from Díaz (2019) (Figure 1 **(b)**) where the original S-Box with confusion coefficient variance value of 6.649 is practically unbreakable by the CPA attack on the encryption process as **SR** does not go above 20%; however, as we expect, its inverse substitution leak information that can be used to fully recover the secret key. Furthermore, this can be extended to all the inverse S-Boxes of the presented in Table 1. Hence, we can conclude that both the S-Box and its inverse should be optimized in order to resist a side-channel analysis. In the remaining of this paper we task ourselves to the search of such S-Boxes.

3 New methods for generating S-boxes with theoretical resistance against CPA

In all the papers referred in Table 1 the heuristic approach is taken to search for S-Boxes having good values of confusion coefficient variance. Following this line of research we introduce in this section two simple heuristic methods to obtain S-Boxes whose inverse are also resistant to a power side-channel analysis. The first of these methods is designed to optimize, at the same time, the S-Boxes and their respective inverses, while the second is conceived to search within the space of involutive 8-bit permutations.

When working with heuristic algorithms to generate S-Boxes satisfying a desired set of criteria it becomes necessary to take into account the fitness function that will be used to move through the S-Box space, since heuristic algorithms are sensitive to the selection of the initial pool of solutions (pseudo-random generated S-Boxes in our case of study) as well as the aforementioned fitness function. Our goal is to produce S-Boxes with the best possible value of nonlinearity and differential uniformity which also present a good resistance to power side-channel analysis. Thus, we propose to adapt the fitness function from Freyre-Echevarría et al. (2020) including the value of the confusion coefficient variance of the inverse S-Box into the calculation.

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

Input: A bijective substitution box $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$
Input: The number of evaluations to make: *evals*

Output: A high nonlinear substitution box with built-in theoretical resistance to CPA as well as its inverse.

Calculate the inverse of S, i.e. S^{-1}
Calculate the best fitness function f_{best} according to equation 6.

while $evals > 0$ **do**
  Select at random $a, b \in \mathbb{F}_2^n$
  $S_c \leftarrow swap(S, a, b)$
  $S_c^{-1} \leftarrow swap(S^{-1}, S_c(a), S_c(b))$
  Calculate the fitness function f_{curr} according to equation 6 using S_c, S_c^{-1}.

  if $f_{curr} \geq f_{best}$ **then**
    $f_{best} \leftarrow f_{curr}$
    $S \leftarrow S_c$
    $S^{-1} \leftarrow S_c^{-1}$
  end
  $evals \leftarrow evals - 1$
end

return S

Algorithm 1: Two-Way Hill Climbing

Then, for one S-Box S and its inverse S^{-1}, the adaptation of the fitness function is expressed as follows:

$$fitness_{S,\,S^{-1}} = 2^{2n}(\mathscr{N}_S - \delta_S) + 2^{n-1}(\kappa(S) + \kappa(S^{-1})) - \mathsf{CF}(S) \tag{6}$$

where the function $\mathsf{CF}(S)$ denotes the cost function related to nonlinearity presented by Picek et al. (2016). The analysis of the possible output values for nonlinearity, differential uniformity and confusion coefficient variance for different selection of the weights associated to each term of the function is carried by Freyre-Echevarría et al. (2020) and therefore it is not in the scope of our paper.

We follow a hill climbing approach to board the problem of optimizing one S-Box and its inverse at the same time. On each iteration of the main cycle of the algorithm we perform two swap operations, the first modify the structure of the S-Box in the search for a new candidate solution while the second is made to the structure of the inverse S-Box to obtain the inverse of the S-Box resulting from the first swap mutation. Then, we calculate the fitness function of the new candidate S-Box and its inverse. If the new candidates are better

Table 2 - Statistical analysis of the cryptographic properties of S-Boxes generated by the proposed optimization method.

Criteria	Minimum value	Maximum value	Average value
$\mathcal{N}_S$	98	100	99.24
δ_S	8	8	8
$\kappa(S)$	2.539	4.609	4.022
$\kappa(S^{-1})$	2.43	4.675	4.107

than the best solution found by the algorithm according to the fitness conditions imposed by equation 6 then one substitute the best solutions by the new candidates. The pseudo-code of the optimization mechanism is presented in Algorithm 1. An additional remark on the above procedure is that mutations made guarantee that S_c^{-1} is the inverse of S_c which avoid the unnecessary calculation of the inverse of S_c by iterating for each one of the 2^n input values.

We create a test benchmark for Algorithm 1 consisting in 50 experiments with input number of evaluations equal to 100000. As we aforementioned the initial S-Boxes supplied to the optimization procedure were pseudo-randomly generated. Once all experiments conclude, we conduct an statistical analysis of the properties taken into account in our paper attending to the following criteria: maximum, minimum and average values of the properties as shown in Table 2.

As one may see in the above table we manage to find S-Boxes whose values of nonlinearity and differential uniformity reach the reported in Freyre-Echevarría (2020); Freyre-Echevarría et al. (2020) and surpass the best results presented in Picek et al. (2014); Díaz (2019) w.r.t these properties starting from pseudo random candidates. Furthermore, the average confusion coefficient variance value of both the S-Boxes and their inverses go above 4, which is an indicative of the quality of the results obtained. However, we consider that the minimum values of confusion coefficient variance obtained still need to be improved. This can be achieved by extending the number of solutions to be evaluated or working with the fitness function from equation 6 as done by Freyre-Echevarría et al. (2020).

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

Input: A bijective substitution box $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$

Output: An involutive substitution box.

```
// Initialize a list of 2^n elements filled with 0
```
$I \leftarrow \{0\}^{2^n}$

$x \leftarrow 0$
while $x < 2^n$ **do**
  $I(S(x)) \leftarrow S(x+1)$
  $I(S(x+1)) \leftarrow S(x)$
  $x \leftarrow x+2$
end

return I

Algorithm 2: Generation of an involutive S-Box.

3.1 A two in one solution: Involutive S-Boxes with theoretical resistance against CPA

As stated in Lerman et al. (2017) one of the future directions of research w.r.t side-channel attack resistant S-Boxes is the study of involutive substitutions. In their words: *"...ciphers with involutive S-boxes have smaller area cost than those having separate S-Boxes for encryption and decryption. The main difficulty of this future work lies in the definition of a new search strategy in order to stay only in the involutive S-Boxes search space"*. In this section we board such study with a very simple strategy to obtain high nonlinear 8-bit involutions with built-in resistance to side-channel attacks.

Let begin introducing the base mechanism for the optimization procedure we carry later to improve the cryptographic properties of involutive S-Boxes. Algorithm 2 present a simple startegy to obtain an involutive S-Box using a permutation in $\mathbb{F}_2^n$. It is straightforward to notice that relating two consecutive values of the input permutation S as described in Algorithm 2 we can easily obtain an involutive subtitution.

The extension of this mechanism to an heuristic method to improve the cryptographic properties of the resulting involution is quite simple as well. The main idea is to make the changes on the structure of permutation S since after we apply Algorithm 2 the resulting permutation is ensured to be an involution. We show the pseudo-code of the proposed optimization scheme in Algorithm 3.

Algorithm 3 have similar procedure to Algorithm 1 with the particular change of the candidate S-Box gen-

eration procedure to adapt it to work with involutive substitutions. In addition, when calculating the fitness conditions of the problem we still use the function from equation 6 by using the candidate involution as the original S-Box and its inverse; hence the term associated to confusion coefficient variance calculation within equation 6 can be expressed as $2^{n-1}(\kappa(I)+\kappa(I^{-1}))=2^{n}\kappa(I)$.

As done for Algorithm 1 we create a test benchmark with identical number of experiments (50) and input number of evaluations (100000) while the initial S-Boxes remain pseudo-randomly generated. Furthermore, we conduct the same statistical analysis presented earlier on the obtained involutions. Table 3 summarizes these results taking into account the three properties boarded in this paper.

As one may see in Table 3 the resulting involutions have nonlinearity value at least 100 which compared to our earlier results represent an improvement on the overall performance of the obtained substitutions w.r.t this property. In addition, we were able to repeatedly produce substitutions having differential uniformity value equal to 8 maintaining the results of the experiment conducted early in this section towards the differential uniformity parameter. Finally, we obtain values of confusion coefficient variance which surpass the presented in the referred literature. Moreover, for the case of nonlinearity equal 102, we find an involution whose confusion coefficient variance is above 3 more than 1 point compared to the best result presented by Freyre-Echevarría et al. (2020) for the same nonlinearity value.

3.2 Power analysis of new S-Boxes

In order to complete the evaluation of our results we conducted the correlation power analysis of four of the obtained S-Boxes, two from Algorithm 1 and two from Algorithm 3 which are presented in Appendices A and B respectively. The experimental benchmark for correlation power analysis is the same as the presented in Section 2:

- Key: `0x8091a2b3c4d5e6f708192a3b4c5d6e7f`.
- Instruction overlapping: 0.
- Leakage points per instruction: 1.
- Leakage distribution function: $\frac{l \cdot sin(t)}{2}$, where l denotes the leakage at instant t of time.
- Noise variance of the system: 3.
- Simulated power traces collected: 250.
- Number of experiments per S-Box: 50.

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

Input: A bijective substitution box $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$
Input: The number of evaluations to make: *evals*

Output: A high nonlinear involutive substitution box with built-in theoretical resistance to CPA.

```
// Construct the involution corresponding to permutation S using
   Algorithm 2
```
$I \leftarrow \mathsf{ALG}_2(S)$

Calculate the best fitness function f_{best} according to equation 6.

while $evals > 0$ **do**
  Select at random $a, b \in \mathbb{F}_2^n$
  $S' \leftarrow swap(S, a, b)$
  $I' \leftarrow \mathsf{ALG}_2(S')$
  Calculate the fitness function f_{curr} according to equation 6 using I'
  if $f_{curr} \geq f_{best}$ **then**
    $f_{best} \leftarrow f_{curr}$
    $S \leftarrow S'$
    $I \leftarrow I'$
  end
  $evals \leftarrow evals - 1$
end
return I

Algorithm 3: Involutive S-Box Hill Climbing

For the better comprehension of the reader we present in Table 4 the cryptographic properties of the S-Boxes selected to conduct our practical analysis. We select such S-Boxes to comprise all obtained values of nonlinearity and to evaluate two different values of nonlinearity for the same type of S-Box.

From the data in Table 4 one may expect that involution I_1 present the lower resistance against the correlation power analysis since its confusion coefficient variance is the lowest among all candidates. The plots of the first order success rate of correlation power analysis on the selected S-Boxes is shown in Figure 2.

As we already mentioned the S-Box I_1 present the more discrete results of the tested candidates, however it shows a slightly better performance in the decryption process that it does in encryption since the attack does not reach the 90% success rate on fully recover the key. Still the resistance shown by S-Box I_1 in the decryption process is better than all the inverse S-Boxes of the presented in Figure 1. With respect to the remaining S-Boxes we analyze, the experimental results confirm our assumptions that a good coefficient variance value in the inverse S-Box (the same original S-Box in the case of involutive S-Boxes), lead to a

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

Table 3 - Statistical analysis of the cryptographic properties of the involutive S-Boxes generated by the proposed optimization method.

Criteria	Minimum value	Maximum value	Average value
$\mathcal{N}_S$	100	102	100.48
δ_S	8	8	8
$\kappa(S)$	1.778	4.269	3.704

Table 4 - Cryptographic properties of the S-Boxes tested for correlation power analysis.

S-Box	$\mathcal{N}_S$	δ_S	$\kappa(S)$	$\kappa(S^{-1})$
S_1 (Appendix A)	98	8	4.609	4.554
S_2 (Appendix A)	100	8	4.055	3.99
I_1 (Appendix B)	102	8	3.205	-
I_2 (Appendix B)	100	8	4.269	-

better practical resistance against the correlation power analysis measured through the lower value of success rate to fully recover the key in the decryption process.

Why do we emphasize the analysis on the decryption process is simple to understand. In the real world scenario an attacker often does not have access to plain texts supplied to the encryption algorithm but it can capture the cipher texts corresponding to such plain texts and capture the power consumption of the device decrypting the data. Hence he can conduct the correlation power analysis to recover the last round key of the algorithm (AES in our case of study) and revert the key schedule to obtain the encryption key of the same. Thus, it may be convinient to take into account the inverse S-Box when designing such component for block ciphers with built-in resistance to side-channel analysis. Furthermore it is desirable a key-schedule which guarantee that the complexity of find any of the round keys or the algorithm's encryption key from the prior knowledge of another round key is equal or greater than the complexity to recover the last.

Conclusions

In this paper we conduct an analysis of the built-in resistance of various 8-bit permutations towards side-channel attacks. We show that most S-Boxes optimized to resist a correlation power analysis does not have an inverse offering the same level of resistance. This can be a disadvantage because a weak inverse S-Box may

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

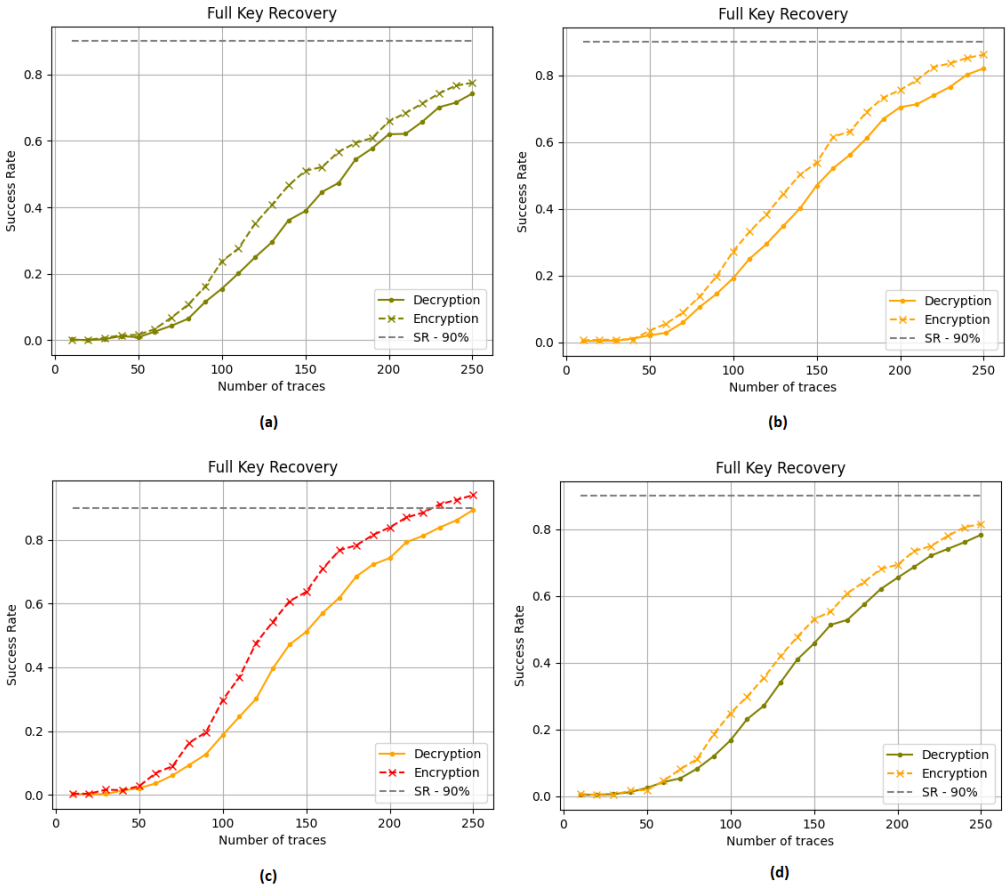

Fig. 2 - Comparison between the results of the correlation power analysis on the encryption and decryption process of AES-128 using the S-Boxes from Table 4: **(a)** S_1, **(b)** S_2, **(c)** I_1, **(d)** I_2.

leak information about the secret key. To counteract this fact we propose two simple optimization mechanisms which allow the designer to obtain S-Boxes with some level of resistance to side-channel analysis. In the first proposed method, one S-Box and its inverse are optimized at the same time to have good values of the theoretical properties measured in this paper, while in the second we board the optimization of involutive S-Boxes with built-in resistance to side-channel analysis which eliminate the necessity of having two S-Boxes, one for encryption and one for decryption. Finally, we show that our results improve the presented in the referred literature in both, theoretical and practical approaches.

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

References

Frederik Armknecht. Improving fast algebraic attacks. In *International Workshop on Fast Software Encryption*, pages 65–82. Springer, 2004.

Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. *Journal of CRYPTOLOGY*, 4(1):3–72, 1991.

Begül Bilgin, Lauren De Meyer, Sébastien Duval, Itamar Levi, and François-Xavier Standaert. Low and depth and efficient inverses: a guide on s-boxes for low-latency masking. *IACR Transactions on Symmetric Cryptology*, 2020(1):144–184, 2020.

Claude Carlet, Yves Crama, and Peter L Hammer. Vectorial boolean functions for cryptography., 2010.

Claude Carlet, Annelie Heuser, and Stjepan Picek. Trade-offs for s-boxes: Cryptographic properties and side-channel resilience. In *International conference on applied cryptography and network security*, pages 393–414. Springer, 2017.

Claude Carlet, Eloi de Chérisey, Sylvain Guilley, Selçuk Kavut, and Deng Tang. Intrinsic resiliency of s-boxes against side-channel attacks–best and worst scenarios. *IEEE Transactions on Information Forensics and Security*, 16:203–218, 2020.

Kaushik Chakraborty, Sumanta Sarkar, Subhamoy Maitra, Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Emmanuel Prouff. Redefining the transparency order. *Designs, codes and cryptography*, 82(1):95–115, 2017.

Joan Daemen and Vincent Rijmen. *The design of Rijndael, 2nd Ed.*, volume 2. Springer, 2020.

Ismel Martínez Díaz. *Búsqueda local de S-cajas con alta varianza del coeficiente de confusión*. Master thesis, Universidad de la Habana, Cuba, 2019.

Yunsi Fei, Qiasi Luo, and A Adam Ding. A statistical model for dpa with novel algorithmic confusion analysis. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 233–250. Springer, 2012.

Yunsi Fei, A Adam Ding, Jian Lao, and Liwei Zhang. A statistics-based fundamental model for side-channel attack analysis. *Cryptology ePrint Archive*, 2014.

Alejandro Freyre-Echevarría. *Evolución híbrida de S-cajas no lineales resistentes a ataques de potencia*. Bsc. thesis, Universidad de La Habana, Cuba, 2020.

Alejandro Freyre-Echevarría, Ismel Martínez-Díaz, Carlos Miguel Legón Pérez, Guillermo Sosa-Gómez, and Omar Rojas. Evolving nonlinear s-boxes with improved theoretical resilience to power attacks. *IEEE Access*, 8:202728–202737, 2020.

Jovan D Golić and Christophe Tymen. Multiplicative masking and power analysis of aes. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 198–212. Springer, 2002.

Sylvain Guilley, Philippe Hoogvorst, and Renaud Pacalet. Differential power analysis model and some results. In *Smart card research and advanced applications VI*, pages 127–142. Springer, 2004.

Liran Lerman, Olivier Markowitch, and Nikita Veshchikov. Comparing sboxes of ciphers from the perspective of side-channel attacks. In *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, pages 1–6. IEEE, 2016.

Liran Lerman, Nikita Veshchikov, Stjepan Picek, and Olivier Markowitch. On the construction of side-channel attack resilient s-boxes. In *International Workshop on Constructive Side-Channel Analysis and Secure Design*, pages 102–119. Springer, 2017.

Huizhong Li, Yongbin Zhou, Jingdian Ming, Guang Yang, and Chengbin Jin. The notion of transparency order, revisited. *The Computer Journal*, 63(12):1915–1938, 2020.

Huizhong Li, Guang Yang, Jingdian Ming, Yongbin Zhou, and Chengbin Jin. Transparency order versus confusion coefficient: a case study of nist lightweight cryptography s-boxes. *Cybersecurity*, 4(1):1–20, 2021.

Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 386–397. Springer, 1993.

Kaisa Nyberg. Perfect nonlinear s-boxes. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 378–386. Springer, 1991.

Stjepan Picek, Kostas Papagiannopoulos, Barış Ege, Lejla Batina, and Domagoj Jakobovic. Confused by confusion: Systematic evaluation of dpa resistance of various s-boxes. In *International Conference on Cryptology in India*, pages 374–390. Springer, 2014.

Stjepan Picek, Marko Cupic, and Leon Rotim. A new cost function for evolution of s-boxes. *Evolutionary computation*, 24(4):695–718, 2016.

Stjepan Picek, Guilherme Perin, Luca Mariot, Lichao Wu, and Lejla Batina. Sok: Deep learning-based physical side-channel analysis. *ACM Computing Surveys*, 2021.

Paolo Ernesto Prinetto and Samuele Yves Cerini. Empirical evaluation of the resilience of novel s-box implementations against power side-channel attacks. 2021.

Emmanuel Prouff. Dpa attacks and s-boxes. In *International Workshop on Fast Software Encryption*, pages 424–441. Springer, 2005.

Mark Randolph and William Diehl. Power side-channel attack analysis: A review of 20 years of study for the layman. *Cryptography*, 4(2):15, 2020.

Jorai Rijsdijk, Lichao Wu, Guilherme Perin, and Stjepan Picek. Reinforcement learning for hyperparameter tuning in deep learning-based side-channel analysis. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 677–707, 2021.

Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digital Investigation*, 29:43–54, 2019.

François-Xavier Standaert, Tal G Malkin, and Moti Yung. A unified framework for the analysis of side-channel key recovery attacks. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 443–461. Springer, 2009.

Nikita Veshchikov. Silk: high level of abstraction leakage simulator for side channel analysis. In *Proceedings of the 4th program protection and reverse engineering workshop*, pages 1–11, 2014.

Antoine Wurcker. Ease of side-channel attacks on aes-192/256 by targeting extreme keys. *Cryptology ePrint Archive*, 2019.

Gabriel Zaid, Lilian Bossuet, François Dassance, Amaury Habrard, and Alexandre Venelli. Ranking loss: Maximizing the success rate in deep learning side-channel analysis. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 25–55, 2021.

Conflicto de interés

Los autores autorizan la distribución y uso de su artículo.

Contribuciones de los autores

1. Conceptualización: Todos los autores contribuyeron de igual forma a la realización de este artículo.
2. Curación de datos: Todos los autores contribuyeron de igual forma a la realización de este artículo.
3. Análisis formal: Todos los autores contribuyeron de igual forma a la realización de este artículo.
4. Adquisición de fondos: Todos los autores contribuyeron de igual forma a la realización de este artículo.
5. Investigación: Todos los autores contribuyeron de igual forma a la realización de este artículo.
6. Metodología: Todos los autores contribuyeron de igual forma a la realización de este artículo.
7. Administración del proyecto: Todos los autores contribuyeron de igual forma a la realización de este artículo.
8. Recursos: Todos los autores contribuyeron de igual forma a la realización de este artículo.
9. Software: Todos los autores contribuyeron de igual forma a la realización de este artículo.
10. Supervisión: Todos los autores contribuyeron de igual forma a la realización de este artículo.
11. Validación: Todos los autores contribuyeron de igual forma a la realización de este artículo.
12. Visualización: Todos los autores contribuyeron de igual forma a la realización de este artículo.
13. Redacción - borrador original: Todos los autores contribuyeron de igual forma a la realización de este artículo.
14. Redacción - revisión y edición: Todos los autores contribuyeron de igual forma a la realización de este artículo.

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

A Some S-Boxes found

$S_1 = \{150, 166, 240, 120, 138, 96, 7, 32, 233, 236, 54, 27, 124, 167, 157, 239, 72, 84, 6, 140, 197, 177, 176, 102, 31, 235, 214, 123, 106, 86, 145, 90, 50, 121, 220, 142, 100, 3, 73, 48, 151, 169, 46, 156, 245, 173, 222, 182, 2, 128, 80, 20, 147, 29, 199, 23, 251, 215, 119, 219, 227, 122, 172, 201, 237, 125, 191, 189, 81, 162, 232, 206, 192, 9, 36, 33, 101, 165, 91, 59, 77, 30, 85, 202, 95, 238, 255, 247, 76, 56, 82, 89, 49, 5, 144, 65, 221, 187, 241, 188, 139, 60, 185, 109, 193, 152, 160, 11, 57, 99, 200, 174, 41, 141, 110, 208, 79, 252, 62, 253, 133, 87, 45, 158, 224, 88, 35, 130, 51, 244, 47, 107, 190, 231, 250, 254, 43, 26, 37, 70, 132, 4, 52, 136, 217, 186, 143, 230, 203, 61, 180, 155, 12, 40, 44, 24, 243, 154, 78, 209, 146, 163, 55, 75, 94, 234, 111, 171, 198, 184, 83, 15, 25, 17, 64, 18, 246, 242, 207, 127, 115, 195, 113, 105, 16, 10, 161, 8, 38, 131, 134, 213, 42, 66, 196, 28, 216, 74, 137, 225, 181, 118, 126, 63, 218, 67, 71, 14, 97, 114, 98, 108, 0, 129, 1, 22, 53, 149, 210, 92, 223, 183, 93, 249, 194, 164, 148, 69, 153, 170, 226, 58, 211, 159, 103, 248, 212, 112, 39, 204, 168, 21, 228, 13, 19, 34, 68, 104, 116, 135, 178, 179, 205, 175, 117, 229\}$

$S_2 = \{172, 89, 14, 236, 74, 63, 51, 232, 158, 100, 198, 27, 197, 179, 187, 138, 146, 150, 191, 96, 239, 40, 174, 201, 32, 190, 148, 54, 157, 147, 76, 231, 30, 210, 145, 117, 73, 250, 134, 43, 55, 33, 135, 206, 137, 12, 151, 56, 13, 99, 31, 49, 115, 17, 50, 167, 10, 238, 124, 155, 185, 141, 131, 220, 36, 251, 184, 15, 78, 92, 133, 237, 194, 209, 103, 34, 214, 37, 205, 181, 252, 128, 168, 70, 98, 154, 107, 8, 21, 196, 24, 207, 65, 217, 199, 109, 26, 243, 90, 104, 35, 153, 66, 182, 102, 75, 234, 164, 95, 4, 166, 152, 93, 82, 200, 216, 44, 108, 215, 132, 142, 120, 160, 143, 19, 125, 203, 106, 39, 77, 9, 171, 130, 255, 11, 28, 175, 193, 86, 18, 213, 169, 254, 224, 116, 212, 248, 192, 183, 112, 69, 242, 1, 127, 113, 53, 60, 123, 162, 126, 94, 29, 48, 111, 25, 59, 47, 67, 119, 208, 247, 57, 91, 180, 253, 140, 173, 101, 244, 84, 211, 5, 41, 110, 6, 230, 228, 178, 114, 122, 3, 246, 52, 235, 195, 22, 170, 88, 2, 241, 149, 227, 218, 81, 233, 144, 240, 58, 188, 72, 202, 105, 186, 71, 221, 80, 85, 165, 68, 245, 136, 249, 204, 46, 129, 118, 79, 156, 176, 83, 64, 121, 163, 97, 222, 0, 223, 20, 226, 139, 189, 7, 38, 229, 177, 225, 219, 16, 87, 161, 23, 61, 42, 159, 45, 62\}$

Revista Cubana de Ciencias Informáticas
Vol. 17, No. 1, Mes Enero-Marzo, 2023
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 94-114

B Some involutions found

$I_1 = \{1, 0, 186, 107, 21, 196, 112, 59, 235, 176, 143, 232, 27, 240, 20, 131, 149, 106, 159, 213, 14, 4, 99, 208, 31, 79, 242, 12, 122, 141, 76, 24, 160, 68, 78, 161, 142, 74, 127, 239, 212, 70, 132, 65, 123, 151, 154, 124, 69, 168, 184, 121, 92, 87, 63, 254, 155, 245, 98, 7, 215, 219, 102, 54, 225, 43, 207, 223, 33, 48, 41, 255, 222, 115, 37, 145, 30, 209, 34, 25, 197, 156, 111, 221, 140, 144, 104, 53, 94, 229, 120, 170, 52, 117, 88, 137, 133, 128, 58, 22, 134, 180, 62, 236, 86, 164, 17, 3, 248, 243, 226, 82, 6, 129, 139, 73, 169, 93, 190, 182, 90, 51, 28, 44, 47, 247, 216, 38, 97, 113, 206, 15, 42, 96, 100, 198, 241, 95, 150, 114, 84, 29, 36, 10, 85, 75, 171, 199, 224, 16, 138, 45, 158, 175, 46, 56, 81, 167, 152, 18, 32, 35, 177, 228, 105, 178, 250, 157, 49, 116, 91, 146, 205, 231, 204, 153, 9, 162, 165, 188, 101, 244, 119, 237, 50, 203, 2, 192, 179, 217, 118, 252, 187, 234, 251, 227, 5, 80, 135, 147, 233, 249, 220, 185, 174, 172, 130, 66, 23, 77, 238, 218, 40, 19, 230, 60, 126, 189, 211, 61, 202, 83, 72, 67, 148, 64, 110, 195, 163, 89, 214, 173, 11, 200, 193, 8, 103, 183, 210, 39, 13, 136, 26, 109, 181, 57, 253, 125, 108, 201, 166, 194, 191, 246, 55, 71\}$

$I_2 = \{153, 26, 141, 215, 30, 130, 228, 191, 94, 240, 81, 14, 119, 69, 11, 91, 171, 164, 210, 63, 115, 22, 21, 121, 221, 157, 1, 188, 234, 172, 4, 139, 39, 250, 99, 146, 60, 127, 78, 32, 65, 55, 205, 163, 73, 47, 190, 45, 137, 103, 180, 168, 100, 109, 138, 41, 68, 248, 123, 242, 36, 86, 253, 19, 124, 40, 90, 235, 56, 13, 75, 107, 255, 44, 136, 70, 213, 105, 38, 162, 120, 10, 206, 95, 176, 112, 61, 245, 214, 202, 66, 15, 218, 135, 8, 83, 150, 229, 116, 34, 52, 238, 195, 49, 145, 77, 243, 71, 129, 53, 211, 203, 85, 252, 142, 20, 98, 219, 225, 12, 80, 23, 155, 58, 64, 166, 173, 37, 217, 108, 5, 201, 251, 151, 194, 93, 74, 48, 54, 31, 216, 2, 114, 254, 187, 104, 35, 209, 199, 200, 96, 133, 241, 0, 177, 122, 197, 25, 170, 223, 224, 244, 79, 43, 17, 232, 125, 222, 51, 247, 158, 16, 29, 126, 184, 196, 84, 154, 181, 212, 50, 178, 189, 226, 174, 246, 233, 144, 27, 182, 46, 7, 239, 198, 134, 102, 175, 156, 193, 148, 149, 131, 89, 111, 236, 42, 82, 230, 231, 147, 18, 110, 179, 76, 88, 3, 140, 128, 92, 117, 227, 24, 167, 159, 160, 118, 183, 220, 6, 97, 207, 208, 165, 186, 28, 67, 204, 249, 101, 192, 9, 152, 59, 106, 161, 87, 185, 169, 57, 237, 33, 132, 113, 62, 143, 72\}$