



Research paper

Construction of Side Channel Attack Resistant S-Boxes Using Genetic Algorithms Based on Coordinate Functions

B. Khadem^{1,*}, S. Rajav zade²

¹Faculty of Computer Engineering, Imam Hossein Comprehensive University, Tehran, Iran.

²Faculty of Mathematics, Payam-e-Noor University (PNU) Graduate Center, Tehran, Iran.

Paper Info

Paper History:

Received 18 March 2021

Reviewed 25 April 2021

Revised 17 July 2021

Accepted 26 July 2021

Keywords:

Substitution Box (S-Box)

Side Channel Attack (SCA)

Coordinate functions

Security properties

Abstract

Background and Objectives: Substitution-Box (S-Box) is one of the essential components creating confusion and nonlinear properties in cryptography. To strengthen a cipher against various attacks, including side channel attacks, these boxes need to have numerous security properties. In this paper, a novel S-Box construction method is introduced aimed at improving the resistance of S-Boxes against power analysis attacks.

Methods: In the preprocessing phase of this approach, a suitable initial S-Box with some basic security properties was generated by adopting a fast algorithm. Then, in the main stage, using the initial S-Box, we generate new S-Boxes which not only have the properties of the initial S-Box but also have significantly improved under another set of security properties. To do this, new S-Boxes were generated using a genetic algorithm on a particular subset of the linear combination set of coordinate functions of the initial S-Box.

Results: The performed experiments demonstrated that the values of all security properties of these new S-Boxes, especially the measures of transparency order, signal-to-noise ratio, confusion coefficient, bijection property, fixed point, and opposite fixed points, have been substantially improved. For example, our experiments indicate that 70, 220, 2071, 43, and 406 S-Boxes are found better than the initial S-Box, respectively, in the dimensions of 4×4 through 8×8

Conclusion: In this paper, a new S-Box construction method is introduced where the properties related to side channel attacks are improved, without destroying other security features. Besides, some results obtained from generated S-Boxes in the dimensions of 4×4 through 8×8 demonstrated that the generated S-Boxes are not only improved relative to the initial S-Box, but also in certain cases, considerably better than some well-known S-Boxes.

*Corresponding Author's Email Address:

Bkhadem@ihu.ac.ir

©2022 JECEI. All rights reserved.

Introduction

S-Boxes are the main components of security in the nonlinear part of many cryptosystems, which are responsible for creating confusion property. One of the major cryptosystem challenges is dealing with various security attacks. For example, the new generation of mobile phones (including the Kasumi block cipher) or the Wi-Fi protocol (including the WPA protocol along with AES block cipher) or RFID protocol has been the subject

of various attacks [1]-[3], [27], [28]. In these attacks, S-Boxes are usually the first components to be threatened. For this reason, special attention has been paid to the S-Box security and new methods of S-Box construction are proposed to make block ciphers resistant to various types of attacks.

Thus, the resistant S-Box construction methods are among the topics of interest for cryptography

researchers in the world. An S-Box (as a vector Boolean function) is a main source of confusion that should be resistant to various attacks. Therefore, it should have certain necessary properties such as nonlinear degree (NL), correlation immunity (CI), algebraic degree (AD), transparency order (TO) and algebraic immunity (AI). Each of S-Box properties represents different security measures against different attacks. For example, nonlinear property indicates the magnitude of the resistance against linear approximation attack, CI measures security against correlation attack, AD shows the strength of S-Box against algebraic attacks, avalanche property presents diffusion criterion and TO demonstrates resistance against differential power attack (DPA) [4]. The main challenge in this situation is that, most of these properties are not independent of each other and even there is some trade-off between them. It is clear that there is a subset of such properties interacting directly or inversely in pairs [5], [29]. For example, due to the inverse relationship between the balanced-ness property and NL of a Boolean function, it is not possible to meet mutual ideal properties such that for balanced Boolean functions, the NL criterion is deducted from the maximum possible value [23]. In particular due to the conflicting nonlinearity and TO [30], finding the S-Boxes with the high nonlinearity and low TO is difficult. Carlet [31] also has been shown that certain S-Boxes with high nonlinearity have very bad TOs.

A. Related Works

In the last decade, numerous studies have been carried out on how to generate an appropriate S-Box. Overall, these construction methods can be divided into three categories, called random methods, algebraic methods, and heuristic methods.

A comprehensive search in the set of S-Boxes [6], use of permutation algorithms [24], pseudo-random generators [7], key-dependent permutations [8], and pseudo-random generators with chaotic cores [7] are some typical methods in the random category. The advantages of random methods include high-speed searches, and their disadvantages include blind and even failed searches. Using the Bent functions [32] in order to withstand differential attacks and using the power mappings such as the use of reverse power mapping in the AES-like the S-Box construction methods [25] are among the algebraic category. Algebraic methods are deterministic algorithms that can generate an S-Box under certain fixed conditions in a short time, but usually their generated S-Boxes have ideal values only in terms of certain properties such as NL or AD and cannot guarantee other properties and therefore are not suitable at all [9]. Finding an algebraic approach that would undoubtedly lead to finding the ideal S-Boxes yet

remains an open problem. However, to find an appropriate method that can generate acceptable S-Boxes with reasonable time and memory complexity, some researchers suggest hybrid, heuristic methods. Therefore, some methods such as the hybrid use of chaotic mapping and genetic algorithms [10] are proposed which can yield suitable S-Boxes. Some of these methods, include [11], employing one or more appropriate initial S-Boxes in a random search. Other methods, generate a set of equivalent S-Boxes with a suitable generated S-Box in a fast random construction method [12]. Among the known equivalences in Boolean vector functions, we can mention Carlet-Charpin-Zinoviev equivalence [13] and Extended Affine Equivalence [14], which are based on the transposition of coordinate functions of an initial S-Box [6]. Picek, S., et al. [33] showed that the extended affine equivalence can be exploited to generate S-Boxes with different TO.

B. Our Contribution

Our proposed hybrid construction method consists of two phases. In the innovative pre-processing phase, a suitable initial S-Box is generated [15] and the set of its component Boolean functions is considered. Then, a large set of all linear combinations of the previous set is generated and all their corresponding S-Boxes are considered but not generated. In the main phase, we employed a genetic smart algorithm to select special S-Boxes from the above considered set, which have significantly better properties in terms of signal to noise rate (SNR), TO, and confusion coefficient properties. We show that these S-Boxes are more resistant to side channel attacks (SCAs) particularly power attacks.

Subsequently, in the second Section, we will introduce the basic properties and concepts required for an S-Box. In Section 3, we will propose the method for the construction of S-Boxes resistant to SCAs so that it improves some properties without destroying other security features. Section 4 expresses the experimental results of the tests performed in both theoretical and practical forms presents some S-Boxes generated by this method in the sizes of 4×4 to 8×8 and compares them with other known S-Boxes. Eventually, in Section 5, we will present a general conclusion and some future suggestions.

Preliminary Definitions

In this section, some of the properties and concepts and required definitions to study the rest of the paper are provided. A vectorial Boolean function is a mapping in the form of $S: F_2^n \rightarrow F_2^m$, with $m > 1$ as follows:

$$S(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) \quad (1)$$

It is usually called an S-Box and sometimes a (n, m) -function. In case $m=1$, S is a simple n -variable Boolean function [16].

Functions $f_i: \{0,1\}^n \rightarrow \{0,1\}$ for $i = 1, \dots, m$ are Boolean n -variable functions called coordinate functions. The Walsh transform of S is represented by W_S , which is defined on the field $F_2^n \times F_2^m$ as follows [34]:

$$W_S(w \cdot u) = \sum_{0 \neq u \in F_2^m, w \in F_2^n} (-1)^{u \cdot S(x) \oplus w \cdot x} \quad (2)$$

where $u \cdot x = u_1 \cdot x_1 \oplus \dots \oplus u_n \cdot x_n$ is the inner product on the specified finite. We represent all linear combinations of coordinate functions of S , with the set as shown below:

$$G = \{g_j; g_j = a \cdot S \cdot a \in F_2^n\} \quad (3)$$

In this paper bijection, fixed points, and opposite fixed points are called primary properties for simplicity. Nonlinearity degree, algebraic degree, CI, differential uniformity, Robustness to differential cryptanalysis, AI, Absolute indicator and sum-of-squares indicators are also called secondary properties. We also call the TO, SNR, and CC the properties for resistance to SCAs.

A. Security Properties for the Evaluation of an S-Box

The security properties of an S-Box are indicators to represent their resistance against various attacks. For example, the properties of NL and CI indicate the resistance to linear attacks. The properties of RDC and DU show resistance to differential attacks, and the properties of FP and OFP represent resistance to algebraic attacks. Improving properties such as TO, SNR, and CC also cause the resistance to SCAs. Then, some of the most important of these properties will be introduced. $u \in F_2^n$, $v \in F_2^m$, and i are an n -bit strings. Multiplication and addition operations are also defined on the field.

B. Balanced-ness (BC)

We consider S as balanced if $W_S(0 \cdot u) = 0$ [11]. The higher the magnitude of S-Box imbalance, the higher the probability of linear approximation is obtained.

C. Nonlinearity Degree (NL)

NL is defined as follows [17]:

$$NL(S) = 2^{n-1} - \frac{1}{2} \max_{0 \neq v \in F_2^m, w \in F_2^n} \left| \sum_{x \in F_2^n} (-1)^{v \cdot F(x) \oplus w \cdot x} \right| \quad (4)$$

The high nonlinearity degree of an S-Box increases the resistance to linear cryptanalysis.

C. Algebraic Degree (AD)

S can be uniquely expressed by the following polynomial:

$$S(x_1, \dots, x_n) = \sum_{I \subseteq \{1, \dots, n\}, a_I \in F_2^q} x^I a_I \quad (5)$$

where $x^I = \prod_{i \in I} x_i$. As a result, the AD of S represented by $\deg(S)$ is defined as follows [8]:

$$\deg(S) = \max\{\#I | a_I \neq 0\} \quad (6)$$

The low degree of an S-Box decreases the resistance against cryptanalytic attacks, namely algebraic attack, higher-order differential, interpolation, cube attacks.

D. Correlation Immunity (CI)

S is immune from the correlation of degree t if we have $W_S(w \cdot u) = 0$ for every u, w that $0 \leq hw(w) \leq t$ [35]. An S-Box is both balanced and correlation immune of t^{th} -order is known as t -resilient. The high order resilient S-Boxes are useful against the correlation attack.

E. Differential Uniformity (DU)

S is called δ -uniform if and only if we have for each the following:

$$0 \neq a \in F_2^n, z \in F_2^m \quad |\{x \in F_2^n; S(x) \oplus S(x \oplus a) = z\}| \in \{0, 2, 4, \dots, \delta\} \quad (7)$$

Smaller values of δ are more appropriate [19]. The smaller value of differential uniformity increases the S-Box resistance to differential cryptanalysis.

F. Fixed Point and Opposite Fixed Point (FP, OFP)

x is a fixed-point of S if $S(x) = x$, and x is an opposite fixed-point of S if $S(x) = x + 1$ [36]. We denote the number of fixed points of S and opposite fixed points by $FP(S)$ and $OFP(S)$, respectively. The number of FP and OFP should be kept as low as possible to avoid leakage in any statistical cryptanalysis.

G. Robustness against Differential Cryptanalysis (RDC)

If L is the largest value of the differential characteristic table of S and R is the number of non-zero values of its first column (the value of 2^n is not calculated in the first row), then S is called ε -resistant to differential cryptanalysis and the value of ε is expressed as follows [20]:

$$\varepsilon = \left(1 - \frac{R}{2^n}\right) \left(1 - \frac{L}{2^n}\right) \quad (8)$$

H. Sum-of-Square Indicator (SSI)

If σ is the symbol of the absolute indicator or the maximum value of absolute autocorrelation of S , which is derived from the autocorrelation function $\hat{r}_S$ then [26]:

$$\sigma = \max_{0 \neq v \in F_2^m} \sum_x \hat{r}_{v \cdot S}^2(\alpha) \quad (9)$$

I. Absolute Indicator (AbI)

If $|AC(S)|_{\max}$ is the symbol of the absolute indicator or the maximum value of absolute autocorrelation of S , which is derived from the autocorrelation function [26] being as follows:

$$\hat{r}_S(\alpha \cdot v) = \hat{r}_{v \cdot S}(\alpha) = \sum_x (-1)^{v \cdot S(x) \oplus v \cdot S(x \oplus \alpha)} \quad (10)$$

then

$$|AC(S)| = \max_{0 \neq v \in F_2^m, \alpha \in F_2^n} |\hat{f}_{v,S}(\alpha)|_{\max} \quad (11)$$

with the low AC and σ , it is harder to perform an analysis of cipher text, when trying to come up with an attack [20].

J. Algebraic Immunity (AI)

If B_n is a set of n -variable Boolean functions, then the AI of S is equal to [37]:

$$AI_S = \min\{deg(g): 0 \neq g \in B_n, \exists b \in F_2^m \text{ s.t. } g|_{S^{-1}(b)} = 0\} \quad (12)$$

The large AI increases the resistance to algebraic attacks.

K. Signal to Noise Ratio (SNR)

The SNR is defined as follows:

$$SNR(DPA)(S) = m 2^{2n} (\sum_k (\sum_{i=0}^{n-1} (-1)^{S_i}(k))^4)^{-1/2} \quad (13)$$

where $\hat{f}(k) = \sum_x (-1)^{x \cdot k} f(x)$ is the Walsh-Hadamard transform (WHT) of a Boolean function f . Increasing the SNR value of the S-Box enhances its robustness against differential cryptanalysis, and decreasing it, increases the robustness of the S-Box to PDA [21].

L. Transparency Order (TO)

The definition of TO represented as follows [34]:

$$TO_S = \max_{\beta \in F_2^n} \left(|m - 2hw(\beta)| - \frac{SS(a \cdot \beta \cdot v)}{2^{2n} - 2^n} \right) \quad (14)$$

where

$$SS(a \cdot \beta \cdot v) = \sum_{0 \neq a \in F_2^n} \left| \sum_{v \in F_2^m, hw(v)=1} (-1)^{v \cdot \beta} W_{DaS}(0 \cdot v) \right|$$

where W_{DaS} is the Walsh-Hadamard transform of derivative S related to the vector $a \in F_2^n$. By reducing the amount of TO, the resistance of the S-Box against DPA increases [20].

M. Confusion Coefficient (CC)

Suppose the selected function for DPA is a bit in the last round of encryption ψ that depends on the encrypted ciphertext bits, the subkey, and the S-Box response. Therefore, if $(\psi|k_i)$ and $(\psi|k_j)$ are related to the assumed keys ψ and k_j , we define the CC κ on the two keys (k_i, k_j) as follows [38]:

$$\kappa = \kappa(k_i, k_j) = Pr[(\psi|k_i) \neq (\psi|k_j)] = \frac{N_{(\psi|k_i) \neq (\psi|k_j)}}{N_t} \quad (15)$$

where N_t is the total number of values of the corresponding encrypted bits, and $N_{(\psi|k_i) \neq (\psi|k_j)}$ is the number of iterations that the keys k_i and k_j in different values ψ generate different responses. Decreasing the value of CC increases the resistance to SCAs [26].

The Proposed S-Box Construction Method

SCAs are among the most critical attacks on S-Boxes,

and decreasing the values of properties such as TO, SNR, and CC will increase the resistance to these attacks [20], [26], [21]. In this paper, a proposed method is designed, intending to improve the resistance of generated S-Boxes to SCAs. This approach enhances this resistance by using a genetic algorithm on linear combinations of coordinate functions. Usually, S-Boxes are evaluated from two perspectives of security and performance efficiency. The time and memory complexity required by the algorithm are called performance properties. The security properties of the S-Box represent the degree of robustness to various attacks.

It should be noted that some security properties have an inverse relationship with each other, meaning that improving one weakens the other. For example, AD and CI are in this way [22].

The main question of this study is whether it is possible to generate a new S-Box by selecting and replacing some Boolean functions from the linear combinations of coordinate functions of an initial S-Box, which, while maintaining the primary and secondary properties, improves the properties of robustness to SCAs.

Following the answer to the research question, it was initially found by theoretical investigations that there was no change in the set G by substituting g_j instead of f_i in S , and therefore the secondary properties would remain unchanged. On the other hand, because the truth table of the coordinate functions changes, there will be a possibility of changing the primary properties and the properties for resistance to SCAs. Besides, in the preprocessing stage of the proposed method, evaluation and comparison have been done to select the appropriate S-Box, sometimes with the production of 2 million S-Boxes by random methods, methods of producing S-Boxes in the Sage tool, and some other novel methods.

This scheme consists of two stages. The first stage is pre-processing, and the second stage is the main section. In the preprocessing stage, a suitable S-Box is generated using a fast heuristic algorithm [15]. The basic properties of this S-Box are compared with the basic properties of known S-Boxes.

If their values are better or equal, the generated S-Box is selected.

This S-Box is called S , and we employ it as the initial S-Box in the main section.

The main section can be implemented as a genetic algorithm with the input of the S-Box S from the preprocessing stage (see Algorithm 1). The details of the algorithm are as follows:

Stage 1. Extraction of coordinate functions of the S-Box $S_{n \times n}$, i.e., f_i :

$$S(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)) \quad (16)$$

Stage 2. Generation of a set of all linear combinations of the coordinate functions S with the name G in expression (3), i.e., each of g_j is being as follows:

$$g_j = \sum_{i=0}^{n-1} a_i \cdot f_i, a_i \in F_2 \quad (17)$$

Thus, we will have $\#G = 2^n$.

Stage 3. n -random selection of g_j and placing them as coordinate functions in a new S-Box named S_i .

$$S_i = (g_0(x), \dots, g_{n-1}(x)) \quad (18)$$

The order does not matter in this selection. On the basis of the observations made, the values of the S-Box properties resulting from the displacement of the coordinate functions of an initial S-Box are equal to the initial S-Box in all properties except possibly fixed points and opposite fixed points.

After generating the S-Boxes, there will be the possibility of changing the order of their coordinate functions.

Stage 4. Repetition of step 3 and generation of set C (number of members of set C is optional):

$$C = \{S_i: S_i(x) = (g_0(x), \dots, g_{n-1}(x)), g_j \in G, x \in F_2^n\} \quad (19)$$

Therefore, we will have $\#C = \binom{2^n}{n}$.

Stage 5. Running of the bijective evaluation function on the members of set C and production of set B :

$$B = \{S_i: S_i \text{ is bijective}\} \quad (20)$$

At this stage, non-bijective S-Boxes are removed.

Stage 6. Running of the function of fixed points and opposite fixed points on the members of set B and production of set F :

$$F = \{S_i: S_i \in B, FP(S_i) = 0, OFP(S_i) = 0\}. \quad (21)$$

At this point, S-Boxes with fixed points or opposite fixed points are deleted.

Stage 7. Running of TO evaluation function on members of set F and production of set T :

$$T = \{S_i: S_i \in F, TO_{S_i} \geq TO_S\} \quad (22)$$

Therefore, the condition for the non-empty set of T is to find at least one S-Box generated from the S-Boxes, which is not firstly an initial S-Box, secondly, it is bijective, has no fixed points, and TO is less than or equal to TO_S .

The above steps can be briefly illustrated in Algorithm 1.

Algorithm 1: Proposed Method Algorithm

Input: The initial S-Box $S_{n \times n}$.

Output: The improved S-Boxes set T .

1. Compute the set
 2. $g = \{g_j: g_j = a \cdot S, 0 \neq a \in F_2^n\}$.
 3. **for** $i = 0$ to $\binom{2^n - 1}{n} - 1$ **do**
 4. $S_i = (g_{j_0}, \dots, g_{j_{n-1}}), j_k \in I$
 5. **if** $FP(S_i) + OFP(S_i) + TO(S_i) = TO(S_i) \leq TO(S)$ **then**
 6. Insert S_i into the set T
 7. **else**
 8. break
 9. **end for**
 10. **until** reaching to maximum iteration allowed
 11. **return** T
-

Results and Discussion

Although, the proposed S-Boxes (Tables 7 to 15) are presented in lookup table form which is used in software templates, but in order to ensure that these proposed S-Boxes are really improved in terms of SNR, TO and CC, we performed both theoretical and practical experiments.

A. Theoretical

In this experiment, some generated S-Boxes with dimensions of 4x4, 5x5, 6x6, 7x7, and 8x8 indicated in Tables 7 to 15, evaluated by an improved version of SET [39] tool as well as the values of the main properties gained from them are shown in Tables 2,3,4,5 and 6. These S-Boxes are compared with the appropriate S-Box and two other well-known S-Boxes. These tables show that the resulting S-Boxes have been improved in terms of SNR, TO and CC without destroying other security features. Therefore, the generated S-Boxes are more resistant to power attacks than the original S-Boxes.

B. Practical

To ensure the results are accurate in practice, we implemented two sample generated 8x8 S-Boxes along with AES S-Box on ATXMEGA and compared their resistance to correlation power attacks (CPAs) in terms of power leakage in a real situation (Fig. 1 and 2). In this experiment, we programmed the AES and two generated S-Boxes (called S1 and S2) on the ATXMEGA chip of the power analysis board. The ATXMEGA chip received a 3MHz clock from the crystal. Also the oscilloscope sampling rate is set to 400 M Sample / s. The attack was carried out for 3 S-Boxes separately and in four stages called as (a) determining the average amount of power consumption and (b) recording them, creating intermediate values and simulating power consumption and, (c) performing correlation power analysis and finally (d) recording the results.

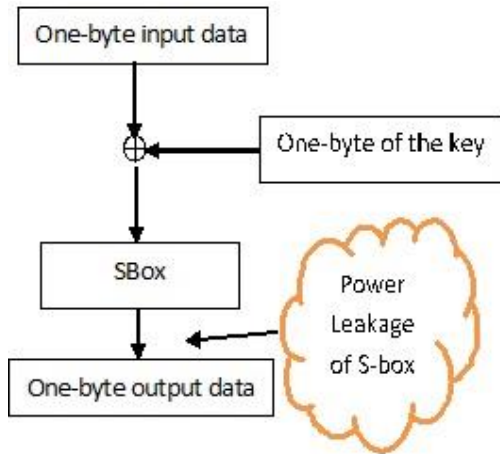


Fig. 1: Location of power leakage measurement.

Table 16 indicates these obtained results. This Table also shows that by comparing the number of required samples to obtain a correct key byte, we can conclude that S1 with 35 samples are the most resistant, followed by AES S-Box with 30 samples and finally S2 with 20 samples.

It should be noted that the experiment was repeated 256 times to ensure the correctness of the results for each sample.

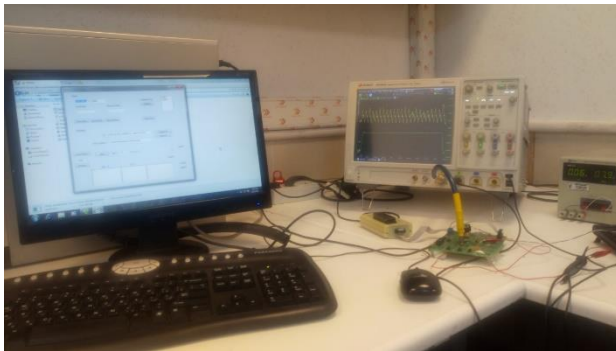


Fig. 2: Experiment environment.

Conclusion

In this paper, an approach is presented in which the properties related to SCAs such as SNR, TO, and CC are improved by using a suitable S-Box, without destroying other security features. Besides, some results obtained from examining S-Boxes in the dimensions of 4×4, 5×5, 6×6, 7×7, and 8×8 demonstrated that the generated S-Boxes have not only improved relative to the initial S-Box, but in some cases, considerably better than the well-known S-Boxes.

On the basis of the observations made, the properties of TO and CC have a direct relationship with each other, and both have an inverse relationship with SNR. This means that the SNR decreases by improving the properties of TO and CC and vice versa so that an S-Box

that was better than the initial S-Box in all three cases was not found. Along with related words, overall, the generated S-Boxes have improved in all properties or have exactly the same values as the initial S-Box properties.

Some of the achieved results can be seen briefly in Table 1. Subsequently, it is proposed that the parallelism in the genetic algorithm is employed to be taken into account so that S-Boxes with dimensions larger than 8 × 8 can also be generated.

In Table 1, the symbols $\#T_{total}$, $\#T_{bij}$, $\#T_{FP}$, $\#T_{OFP}$, $\#T_{SNR}$, $\#T_{TO}$ and $\#T_K$ show the number of total generated S_i , the number of bijective S_i , the number of S_i with $FP(S) = 0$, the number of S_i with $OFP(S) = 0$, the number of S_i with better SNR, the number of S_i with better TO, and the number of S_i with better κ , respectively.

Table 1: The number of generated S-Boxes in different sizes

Samples	4x4	5x5	6x6	7x7	8x8
$\#T_{total}$	1820	201376	10^5	10^5	10^4
$\#T_{bij}$	840	8332	40292	38185	4359
$\#T_{FP}$	356	29399	13709	12978	1399
$\#T_{OFP}$	339	36875	14934	16531	1207
$\#T_{SNR}$	0	60	6	23	2413
$\#T_{TO}$	355	310	9571	359	4273
$\#T_K$	835	83238	40286	38164	1905
$\#T_{better}$	70	220	2071	43	406

Table 2: Comparing the evaluation properties of 4×4 S-Boxes

Properties	4x4			initial	proposed	PRINCE	PRESENT
	min	avg	max				
B	√	√	√	√	√	√	√
NL	4	4	4	4	4	4	4
AD	3	3	3	3	3	3	3
CI	0	0	0	0	0	0	0
R	0.75	0.75	0.75	0.75	0.75	0.75	0.75
δ	4	4	4	4	4	4	4
AC	8	8	8	8	8	8	8
σ	640	640	640	640	640	640	640
AI	2	2	2	2	2	2	2
FP	0	0.889	5	0	0	0	0
OFP	0	0.894	5	0	0	0	0
SNR	1.612	3.466	3.108	1.612	1.663	2.128	2.128
TO	3.4	3.539	3.733	3.533	3.466	3.4	3.533
K	0.157	0.457	1.357	1.357	1.357	0.657	0.657

Table 3: Comparing the evaluation properties of 5x5 S-Boxes

Properties	5x5			initial	proposed	Keccak	Primate
	min	avg	max				
B	✓	✓	✓	✓	✓	✓	✓
NL	10	10	10	10	10	10	10
AD	4	4	4	4	4	4	4
CI	0	0	0	0	0	0	0
R	0.937	0.937	0.937	0.937	0.937	0.937	0.937
δ	2	2	2	2	2	8	2
AC	8	8	8	8	8	8	8
σ	2048	2048	2048	2048	2048	2048	2048
AI	3	3	3	3	3	3	3
FP	0	1.029	7	0	0	1	1
OFP	0	0.81	7	0	0	1	1
SNR	2.307	3.432	4.603	2.361	2.517	3.922	3.690
TO	4.596	4.658	4.758	4.612	4.596	4.516	4.661
K	0.096	0.356	1.003	0.949	0.81	0.211	0.265

Table 4: Comparing the evaluation properties of 6x6 S-Boxes

Properties	6x6			initial	proposed	CTTL	Fides
	min	avg	max				
B	✓	✓	✓	✓	✓	✓	✓
NL	24	24	24	24	24	20	24
AD	5	5	5	5	5	5	5
CI	0	0	0	0	0	0	0
R	0.937	0.937	0.937	0.937	0.937	0.937	0.968
δ	4	4	4	4	4	4	2
AC	16	16	16	16	16	32	64
σ	8704	8704	8704	8704	8704	14464	16384
AI	3	3	3	3	3	3	3
FP	0	1.09	7	0	0	2	0
OFP	0	1.008	7	0	0	2	1
SNR	3.360	4.978	5.994	3.451	3.904	5.026	4.879
TO	5.694	5.740	5.801	5.734	5.694	5.734	5.730
K	0.109	0.262	0.664	0.622	0.454	0.216	0.238

Table 5: Comparing the evaluation properties of 7x7 S-Boxes

Properties	7x7			initial	proposed	WAGE	Niho
	min	avg	max				
B	✓	✓	✓	✓	✓	✓	✓
NL	54	54	54	54	54	54	54
AD	6	6	6	6	6	6	4
CI	0	0	0	0	0	0	0
R	0.984	0.984	0.984	0.984	0.984	0.937	0.984
δ	2	2	2	2	2	8	2
AC	24	24	24	24	24	80	16
σ	32768	32768	32768	32768	32768	86528	32768
AI	4	4	4	4	4	3	3
FP	0	0	0	0	0	0	2
OFP	0	0	0	0	0	4	1
SNR	4.806	6.670	8.077	5.318	5.84	6.628	7.062
TO	6.792	6.813	6.837	6.802	6.8	6.74	6.838
K	0.092	0.182	0.437	0.339	0.264	0.183	0.15

Table 6: Comparing the evaluation properties of 8x8 S-Boxes

Properties	8x8			initial	proposed	Camellia	CLEFFIA
	min	avg	max				
B	✓	✓	✓	✓	✓	✓	✓
NL	112	112	112	112	112	112	112
AD	7	7	7	7	7	7	7
CI	0	0	0	0	0	0	0
R	0.984	0.984	0.984	0.984	0.984	0.984	0.984
δ	4	4	4	4	4	4	4
AC	32	32	32	32	32	32	32
σ	133120	133120	133120	133120	133120	133120	133120
AI	4	4	4	4	4	4	4
FP	0	1.062	6	0	0	0	0
OFP	0	1.192	6	0	0	0	0
SNR	8.253	9.541	10.76	9.599	8.758	9.694	9.323
TO	7.847	7.855	7.863	7.86	7.85	7.855	7.851
K	0.075	0.114	0.172	0.111	0.146	0.107	0.121

Table 7: Initial 4x4 S-Box

8	0	1	10	9	4	2	6
11	7	14	12	5	15	13	3

Table 8: Our best generated 4x4 S-Box

3	0	5	15	6	13	12	1
10	4	2	14	8	7	11	9

Table 9: Initial 5x5 S-Box

8	0	26	17	22	28	29	24
19	16	4	6	7	18	16	23
13	31	25	30	2	20	12	1
5	3	15	27	9	21	10	11

Table 10: Our best generated 5x5 S-Box

24	0	23	22	12	28	13	31
30	7	3	11	26	15	19	29
10	5	14	20	8	4	27	17
18	25	2	6	9	21	16	1

Table 11: Initial 6x6 S-Box

22	25	37	10	14	5	60	15
0	7	26	63	50	59	48	23
6	62	24	38	16	58	32	61
43	20	29	4	52	33	35	12
13	56	44	54	51	47	42	27
28	40	11	55	9	36	41	45
46	8	31	34	17	2	18	19
30	39	49	1	3	57	21	53

Table 12: Our best generated 6x6 S-Box

2	30	47	53	59	41	49	28
0	11	27	52	10	58	40	37
44	19	57	42	46	29	6	22
20	32	16	14	38	33	3	25
62	63	31	4	45	26	51	60
55	17	18	35	48	8	54	56
61	23	50	36	9	34	12	43
21	13	15	39	5	24	7	1

Table 13: Initial 7x7 S-Box

66	114	56	86	115	85	11	78
124	71	44	3	41	87	4	81
104	10	34	15	108	48	2	16
95	92	65	67	55	62	28	97
76	57	12	96	6	18	120	91
54	35	79	100	109	69	121	9
36	126	111	77	74	45	125	122
73	90	26	98	58	80	51	72
118	33	21	116	123	117	82	61
110	64	68	99	19	37	46	53
83	31	50	24	93	89	52	60
84	22	63	107	25	38	88	7
39	30	17	13	119	102	8	14
5	29	20	127	70	106	43	112
59	49	101	1	47	113	32	0
23	94	40	75	27	103	105	42

Table 14: Our best generated 7x7 S-Box

52	17	127	112	58	18	56	123
23	10	59	98	5	91	21	7
83	19	61	45	70	37	73	81
1	99	86	31	82	35	30	34
50	84	79	9	92	24	2	20
121	22	80	28	109	67	41	113
97	94	36	25	110	16	60	75
12	63	66	64	54	44	71	39
4	95	111	77	96	102	101	65
15	125	104	107	51	74	114	27
78	124	108	11	72	93	48	106
57	13	8	49	32	40	118	119
3	87	122	100	47	85	90	6
62	53	68	117	33	26	76	88
29	14	55	43	89	115	116	0
38	42	46	69	105	126	120	103

Table 15: Our best generated 8x8 S-Box

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

Table 16: Experimental results of CPA attack

Samples	AES		S1		S2	
	Obtained key bytes	Key correlation coefficient	Obtained key bytes	Key correlation coefficient	Obtained key bytes	Key correlation coefficient
10	97	0.961954780212747	118	0.956011704408103	227	0.960010242659831
15	97	0.885291320534845	6	0.910922032419744	112	0.886333099327659
20	3	0.842358907364451	38	0.826128138147242	110	0.828956410200449
25	6	0.756529730202484	19	0.748836484915596	110	0.812522873710724
30	110	0.730385064352021	89	0.675115536418951	110	0.790117523485932
35	110	0.719629435623104	110	0.667255880801344	110	0.803285875513011

Author Contributions

B. Khadem did the preprocessing phase, the simulations and carried out the S-Box evaluation results and edited the manuscript.

S. Rajav Zade did and implemented the main stage, carried out the suitable S-Boxes, wrote the manuscript.

Acknowledgment

This work is completely self-supporting, thereby no any financial agency's role is available.

Conflict of Interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Abbreviations

AD	Algebraic Degree
AI	Algebraic Immunity,
CC	Confusion Coefficient
CI	Correlation Immunity
DPA	Differential Power Attack
CPA	Correlation Power Attack
DU	Differential Uniformity
FP	Fixed Point
NL	Nonlinearity Degree
OPF	Opposite Fixed Point
RDC	Robustness to Differential Cryptanalysis
S-Box	Substitution Box
SCA	Side Channel Attack
SNR	Signal-to-Noise Ratio
TO	Transparency Order

References

- [1] C. Luo, et al., "Power analysis attack of an AES GPU implementation," *J. Hardware Syst. Secur.*, 2(1): 69-82, 2018.
- [2] H. Wang, T. Peyrin, "Boomerang switch in multiple rounds, Application to AES variants and deoxys," *IACR Trans. Symmetric Cryptology*, 2019(1): 142-169, 2019.
- [3] M. Safkhani, "Cryptanalysis of R2AP an ultralightweight authentication protocol for RFID," *J. Electr. Comput. Eng. Innovations*, 6(1): 111-118, 2017.
- [4] K. Chakraborty, et al, "Redefining the transparency order," *Des. Codes Cryptogr.*, 82(1-2): 95-115, 2017.
- [5] D. Tang, W. Zhang, X. Tang, "Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties," *Des. Codes Cryptogr.*, 67(1): 77-91, 2013.
- [6] A. Anees, Y.-P. Chen, "Designing secure substitution boxes based on permutation of symmetric group," *Neural Comput. Appl.*, 32: 7045-7056, 2019.
- [7] G. Tang, X. Liao, "A method for designing dynamical S-boxes based on discretized chaotic map," *Chaos, Solitons Fractals*, 23(5): 1901-1909, 2005.
- [8] R. Yin, et al, "Designing key-dependent chaotic S-box with larger key space," *Chaos, Solitons Fractals*, 42(4): 2582-2589, 2009.
- [9] L. Budaghyan, et al, "On upper bounds for algebraic degrees of APN functions," *IEEE Trans. Inf. Theory*, 64(6): 4399-4411, 2017.
- [10] Y. Wang, et al, "A novel method to design S-box based on chaotic map and genetic algorithm," *Phys. Lett. A*, 376(6-7): 827-833, 2012.
- [11] D. Lambić, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons Fractals*, 58: 16-21, 2014.
- [12] A. Razaq, et al, "A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups," *IEEE Access*, 8: 75473-75490, 2020.
- [13] L. Budaghyan, C. Carlet, "CCZ-equivalence of bent vectorial functions and related constructions," *Des. Codes Cryptogr.*, 59(1): 69-87, 2011.
- [14] A. Canteaut, L. Perrin, "On CCZ-equivalence, extended-affine equivalence, and function twisting," *Finite Fields Appl.*, 56: 209-246, 2019.
- [15] B. Khadem, R. Ghasemi, "Improved algorithms in parallel evaluation of large cryptographic S-boxes," *Int. J. Parallel Emergent Distrib. Syst.*, 35(4): 461-472, 2020.
- [16] Y. Xu, C. Wu, "On the primary constructions of vectorial Boolean bent functions," *Citeseer*: 1-43, 2015.
- [17] C. Carlet, C. Ding, "Nonlinearities of S-boxes," *Finite Fields Appl.*, 13(1): 121-135, 2007.
- [18] P. Mishra, S. Sarkar, I. Gupta, "Determining the minimum degree of an S-box," *IACR Cryptology ePrint Archive*: 376, 2017.

- [19] C. Carlet, "Characterizations of the differential uniformity of vectorial functions by the Walsh transform," *IEEE Trans. Inf. Theory*, 64(9): 6443-6453, 2017.
- [20] B. Mazumdar, D. Mukhopadhyay, I. Sengupta, "Constrained search for a class of good S-Boxes with improved DPA resistivity," *IEEE Trans. Inf. Forensics Secur.*, 8(12): 2154-2163, 2013.
- [21] S. Guilley, P. Hoogvorst, R. Pacalet, "Differential power analysis model and some results," in *Proc. Smart Card Research and Advanced Applications Vi*. Springer: 127-142, 2004.
- [22] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," (Corresp.). *IEEE Trans. Inf. Theory*, 30(5): 776-780, 1984.
- [23] C-K. Wu, D. Feng, "Boolean functions and their applications in cryptography," Springer, 2016.
- [24] D. E. Knuth, "The art of computer programming," Vol. 3. Pearson Education, 1997.
- [25] J. Daemen, V. Rijmen, "The design of Rijndael." *Information security and cryptography*, Springer Berlin, 2002.
- [26] S. Picek, "Applications of evolutionary computation to cryptography," [SI: sn, 2015.
- [27] L. Grassi, M. Schofnegger, "Mixture Integral Attacks on Reduced-Round AES with a Known/Secret S-Box," in *Proc. International Conference on Cryptology in India*, Springer: 312-331, 2020.
- [28] N. Sugio, Y. Igarashi, T. Kaneko, "Integral cryptanalysis of reduced-round KASUMI," in *Proc. 2018 International Symposium on Information Theory and Its Applications (ISITA)*, 2018.
- [29] Y. Zheng, X.M. Zhang, "On relationships among avalanche, nonlinearity, and correlation immunity," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2000.
- [30] S. Picek, et al, "On using genetic algorithms for intrinsic side-channel resistance: the case of AES S-box," in *Proc. The First Workshop on Cryptography and Security in Computing Systems*, ACM, 2014.
- [31] C. Carlet, "On highly nonlinear S-boxes and their inability to thwart DPA attacks," in *Proc. International Conference on Cryptology in India*, Springer, 2005.
- [32] J. Detombe, S. Tavares "Constructing large cryptographically strong S-boxes," in *Proc. International Workshop on the Theory and Application of Cryptographic Techniques*, Springer, 1992.
- [33] S. Picek, et al, "Confused by confusion: Systematic evaluation of DPA resistance of various s-boxes," in *Proc. International Conference in Cryptology in India*, Springer, 2014.
- [34] E. Prouff, "DPA attacks and S-boxes," in *Proc. International Workshop on Fast Software Encryption*, Springer, 2005.
- [35] C. Carlet, et al, "Generalized correlation analysis of vectorial Boolean functions," in *Proc. International Workshop on Fast Software Encryption*, Springer, 2007.
- [36] H. Isa, N. Jamil, M. R. Z'aba. "S-box construction from non-permutation power functions," In *Proceedings of the 6th International Conference on Security of Information and Networks*, ACM, 2013.
- [37] C. Carlet, K. Feng, "An infinite class of balanced vectorial Boolean functions with optimum algebraic immunity and good nonlinearity," in *Proc. International Conference on Coding and Cryptology*, Springer, 2009.
- [38] Y. Fei, Q. Luo, A.A. Ding, "A statistical model for DPA with novel algorithmic confusion analysis," in *Proc. International Workshop on Cryptographic Hardware and Embedded Systems*, Springer, 2012.
- [39] S. Picek, et al, "S-box, SET, match: a toolbox for S-box analysis," in *Proc. IFIP International Workshop on Information Security Theory and Practice*, Springer, 2014.

Biographies



Behrooz Khadem (8 Aug. 1963) received the B.S. degree in applied mathematics from Tehran University, Tehran, Iran, in 1991 and the M.S. degree in applied mathematics from Shahid Bahonar University, Kerman, Iran, in 1995 and received the Ph.D. degree from the Department of Mosahab Mathematics, Kharazmi University, Tehran, Iran, in the area of Chaos-based cryptography in 2015. From 2011 until now he has been a professor assistant at the Imam Hossein Comprehensive University, Tehran, Iran. His research interest includes data security and cryptography. He has published over 50 research papers in reputed refereed journals and conference proceedings. His areas of research interests include, but not limited to applied mathematics, algorithms and complexity, computer security, chaos-based cryptography, applied cryptanalysis, security of communication networks, artificial intelligence, machine learning for security, image processing, and optimization techniques. He has served as a reviewer and technical program committee member of many journals and conferences.



Saeed Rajavzade (14 April. 1989) is a Ph.D. student of the Payam-e-Noor university in Tehran. He has graduated with mechanical engineering B.Sc. from Islamic Azad University of Tehran Markazi (2014) and pure mathematics M.Sc. from Maragheh University (2017). His interests are dynamical systems, nonlinear analysis, lattice as well as mathematical aspects of cryptography, lattice-based cryptography, and Algorithms.

Copyrights

©2022 The author(s). This is an open access article distributed under the terms of the Creative Commons Attribution (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, as long as the original authors and source are cited. No permission is required from the authors or the publishers.



How to cite this paper:

B. Khadem, S. Rajavzade, "Construction of side channel attack resistant s-boxes using genetic algorithms based on coordinate functions," *J. Electr. Comput. Eng. Innovations*, 10(1): 143-152, 2022.

DOI: [10.22061/JECEI.2021.7801.436](https://doi.org/10.22061/JECEI.2021.7801.436)

URL: https://jecei.sru.ac.ir/article_1592.html

