

Multi-Objective Generation of S-Boxes Using Evolutionary Algorithms [†]

Enrique Dávalos , Adolfo Salas , Javier Benítez and Christian Von Lücken * 

Facultad Politécnica, Universidad Nacional de Asunción, San Lorenzo 111421, Paraguay; edavalos@pol.una.py (E.D.); adolfosalas1@gmail.com (A.S.); benitezbrachojavier@gmail.com (J.B.)

* Correspondence: clucken@pol.una.py

[†] Presented at the First Summer School on Artificial Intelligence in Cybersecurity, Cancun, Mexico, 3–7 November 2025.

Abstract

Substitution boxes, or S-boxes, are critical elements of symmetric block cipher algorithms—these being the ones that provide “confusion” (a concept defined by Claude Shannon). This work presents a method for generating 8×8 S-boxes using a multi-objective evolutionary algorithm, aiming to simultaneously optimize Nonlinearity (NL) and the Strict Avalanche Criterion (SAC), which are two important cryptographic properties of S-boxes. Chaotic maps were used to generate the initial population. Experimental executions were carried out, and the results were compared to evaluate the different Pareto fronts obtained. The results indicate that the proposed versions of our algorithm achieve good performance, comparable to the state of the art (with only 150 generations of execution), and it was also found that they continue to improve for runs of 5000 generations. This method can be used for the generation of S-boxes with specific properties.

Keywords: S-boxes; nonlinearity; strict avalanche criterion; evolutionary algorithms; multi-objective optimization

1. Introduction

Substitution boxes, or S-boxes $m \times n$, refer to a substitution (or mapping) of m -bit input vectors to n -bit output vectors. They are mainly used to hide the relationship between the input cleartext and the output ciphertext in block cipher algorithms [1]. The construction of these boxes and their cryptographic properties have been widely studied since the security of an encryption algorithm against analytical attacks, such as linear cryptanalysis, differential cryptanalysis and others, depends on these properties [1,2].

The most-cited metric in the scientific literature to define how strong a specific S-box can be against known analytical attacks is Nonlinearity (NL). Most works refer to this property as the only objective function in the proposed search algorithms. However, several other parameters seek to evaluate other important aspects of the strength of the S-boxes. One of those properties is the Strict Avalanche Criterion, or SAC. This parameter guarantees that a small change in the input will produce a significant change in the output [3].

It is evident that, therefore, the generation of S-boxes with good cryptographic properties must be treated as a multi-objective optimization problem. In this work, we present an approach for the generation of S-boxes of size 8×8 using multi-objective evolutionary algorithms for the simultaneous optimization of two strength metrics of S-boxes: (i) NL and the (ii) SAC. Furthermore, the algorithm also verifies compliance with the bijective property.



Academic Editors: Luis Javier García Villalba, Héctor Manuel Pérez Meana, Gabriel Sánchez Pérez and Ana Lucila Sandoval Orozco

Published: 30 January 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

In addition, chaotic maps [4] were used to generate the initial population of the evolutionary algorithm.

Most of the common techniques proposed in the state of the art for the construction or generation of S-boxes are the following: algebraic constructions, pseudo-random generation [5], heuristic approaches and metaheuristic approaches [6]. In the scientific literature, almost all previous works have been focused on the optimization of a single metric, which is, generally, NL. To the best of our knowledge, the only paper that presents a multi-objective approach is [7], and it performed a very large number of iterations (5000 generations) to achieve results similar to the state of the art.

2. Materials and Methods

2.1. Properties of Cryptographically Robust S-Boxes

Below, we present the three properties that were used in our work (based mainly on [4,8]): Bijection, Nonlinearity and SAC.

- **Bijjective Property.** A S-box $n \times n$ complies with the bijective property if it has all the output values being different in an interval of $[0, 2^n - 1]$, that is, if no output is repeated for more than one input.
- **Nonlinearity (NL).** Suppose $f(x) : F_2^n \rightarrow F_2$ is a Boolean function. Then, the Nonlinearity N_f of $f(x)$ is defined as follows:

$$N_f = \min_{l \in L_n} d_H(f, l), \quad (1)$$

where L_n is the set of affine functions, and $d_H(f, l)$ is the Hamming distance between f y l . Let there be a S-box where each possible output has 8 bits that consists of 8 Boolean functions f , one for each bit position. The NL of an 8×8 substitution box is, therefore, usually taken as the smallest value among the eight N_f .

- **Strict Avalanche Criteria (SAC).** For a function to satisfy the SAC, each of its output bits should change with a probability of one half whenever a single input bit is complemented. A dependency matrix is used to test the Strict Avalanche Criterion of a substitution box [3]. If each element of the matrix $P_{i,j}$ approaches the ideal value of 0.5, then the S-box can be considered to almost satisfy the SAC criterion.

$$P_{ij}(f) = 2^{-n} \sum_{x \in GF(2^n)} f_j(x) \oplus f_j(x \oplus e_i). \quad (2)$$

To estimate a score, the offset or deviation of the dependency matrix from the ideal value of 0.5 is used.

2.2. Proposed Method

Next, we present our proposal, an evolutionary multi-objective algorithm that we call SBMO (S-Boxes Multi-Objective).

- **Initial Population Generation.** Each individual or *chromosome* is a binary matrix of size 256×8 that represents an 8×8 S-box, where each row corresponds to a value between 0 and 255.
The individuals of the initial population are generated by iterating two chaotic maps—the Logistic Map and the Tent Map [4,9].
- **Selection operator.** This consists of choosing individuals that will undergo the evolutionary operation of crossover.
Two variants are proposed:

- **NL Based:** Two individuals are chosen from the current population. The first is the one with the greatest NL in the entire population, which is marked as selected and removed from further selection in the current generation. The second is chosen using a binary tournament, and it is marked. The process is then repeated to choose the next pair among the unmarked individuals.
- **PF Based:** Two individuals are chosen. The first is a non-dominated individual, which is marked as selected and excluded from further selection in the current generation. The second is chosen, as in the previous variant, using a binary tournament.
- **Crossover.** Two columns, each representing one of the eight Boolean functions, are randomly chosen and swapped between the parent chromosomes, producing two offspring that are added to the population of the next generation of individuals.
- **Mutation.** Two elements of the matrix are randomly swapped; this procedure can also be viewed as flipping a bit in the 256×8 matrix and, subsequently, correcting the duplicated value.
- **Individual repair.** A repair procedure was designed to identify the duplicate elements in the S-box and to replace them, in descending sequential order, with the first missing value within the range $[0, 255]$.

3. Results

We performed a series of experiments on three proposed versions, as shown in Table 1, each of which were initialized with the following configuration:

$N = 100$ individuals; crossover probability $P_c = 0.7$; mutation probability $P_m = 1 - P_c$; stop criteria = 150; and 5000 generations.

We took the scores of one representative execution.

Table 1. Variants of our proposed algorithm.

Algorithm	Generations	Selection Operator
SBMO-NL-150	150	NL-Based
SBMO-PF-150	150	PF-Based
SBMO-5000	5000	NL/PF (alternatively)

The results (Pareto fronts) are shown in Figure 1.

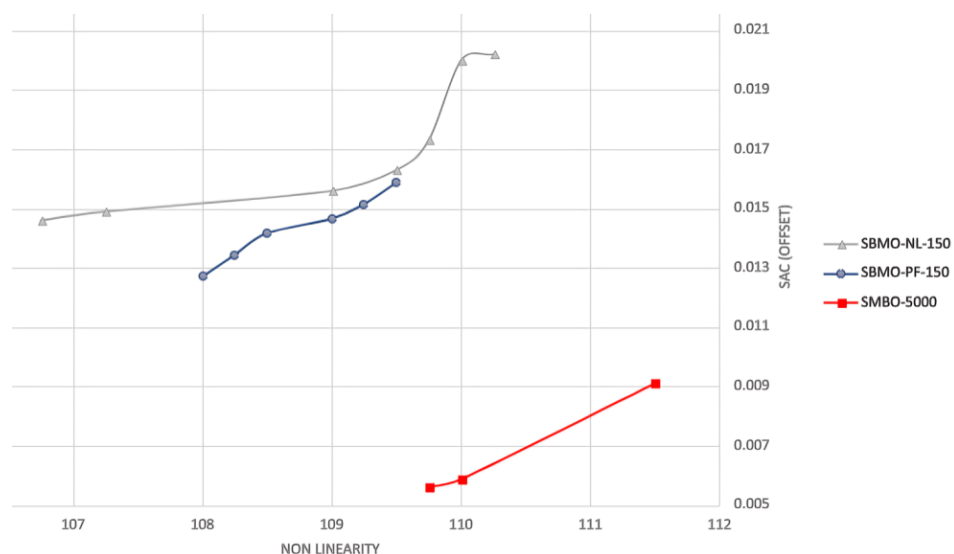


Figure 1. Comparison of Pareto fronts of SBMO-NL, SBMO-PF and SMBO-5000.

Three representative S-boxes, taken from Figure 1, were compared (as shown in Table 2) with other state-of-the-art works. Note that this comparison is not entirely fair since only [7] is multi-objective (like ours).

Table 2. Comparison of the S-boxes.

S-Box	NL (Avg)	SAC (Avg)	SAC (Offset)
SBMO-NL	110.25	0.5041	0.0198
SBMO-PF	108.00	0.5098	0.0122
Ref. [10]	106.25	0.5002	0.0324
Ref. [5]	106.25	0.5029	0.0332
Ref. [8]	109.00	0.4936	0.0331
SBMO-5000	111.50	0.5012	0.0090
Ref. [7]	110.50	0.4929	0.0344

4. Discussion

These results show that our algorithm converges rapidly and yields results comparable to, and even surpassing, many of the state-of-the-art algorithms for 150 generations.

For runs of 5000 generations, SBMO-5000 generates results reaching 111.5 for the NL, which is very close to 112 (i.e., the maximum experimental value achieved). It also generates excellent results for the SAC.

Our proposal, with its high convergence and multi-objective properties, can be very useful in situations requiring the rapid, simultaneous generation of substitution boxes with good cryptographic values and specific properties.

Author Contributions: Conceptualization, E.D.; methodology, C.V.L.; software, A.S. and J.B.; validation, E.D. and C.V.L.; formal analysis, A.S.; investigation, A.S. and J.B.; resources, A.S. and J.B.; data curation, E.D.; writing—original draft preparation, E.D. and A.S.; writing—review and editing, C.V.L.; visualization, E.D.; supervision, E.D.; project administration, A.S. and J.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original data presented in the study are openly available in: <https://gitlab.com/adolfosalas1/nsga-v2>, accessed on 26 January 2026.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Adams, C.; Tavares, S. The structured design of cryptographically good S-boxes. *J. Cryptol.* **1990**, *3*, 27–41. [\[CrossRef\]](#)
2. Branstad, D.; Gait, J.; Katzke, S. *Report of the Workshop on Cryptography in Support of Computer Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 1977. [\[CrossRef\]](#)
3. Webster, A.F.; Tavares, S.E. On the design of S-boxes. In *Advances in Cryptology, Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 18–22 August 1985*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 523–534.
4. Lambić, D. A novel method of S-box design based on discrete chaotic map. *Nonlinear Dyn.* **2017**, *87*, 2407–2413. [\[CrossRef\]](#)
5. Lu, Q.; Zhu, C.; Deng, X. An efficient image encryption scheme based on the LSS chaotic map and single S-box. *IEEE Access* **2020**, *8*, 25664–25678. [\[CrossRef\]](#)
6. Ivanov, G.; Nikolov, N.; Nikova, S. Reversed genetic algorithms for generation of bijective S-boxes with good cryptographic properties. *Cryptogr. Commun.* **2016**, *8*, 247–276. [\[CrossRef\]](#)
7. Ahmad, M.; Alkanhel, R.; El-Shafai, W.; Algarni, A.D.; Abd El-Samie, F.E.; Soliman, N.F. Multi-objective evolution of strong S-boxes using non-dominated sorting genetic algorithm-II and chaos for secure telemedicine. *IEEE Access* **2022**, *10*, 112757–112775. [\[CrossRef\]](#)

8. Lawah, A.I.; Ibrahim, A.A.; Salih, S.Q.; Alhadawi, H.S.; JosephNg, P.S. Grey Wolf Optimizer and Discrete Chaotic Map for Substitution Boxes Design and Optimization. *IEEE Access* **2023**, *11*, 42416–42430. [[CrossRef](#)]
9. Tang, G.; Liao, X.; Chen, Y. A novel method for designing S-boxes based on chaotic maps. *Chaos Solitons Fractals* **2005**, *23*, 413–419. [[CrossRef](#)]
10. Ben Farah, M.A.; Farah, A.; Farah, T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dyn.* **2020**, *99*, 3041–3064. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.