

# An In-Depth Analytical Cryptanalysis for Substitution Boxes: Odd Size Case Study <sup>†</sup>

Ismail El Gaabouri <sup>1,2,\*</sup> , Mostafa Belkasmi <sup>1</sup>, Mohamed Senhadji <sup>1</sup> and Brahim El Bhiri <sup>3</sup>

<sup>1</sup> ICES Team, École Nationale Supérieure d'Informatique et d'Analyse des Systèmes, Mohamed V University, Rabat 10000, Morocco; mostafa.belkasmi@ensias.um5.ac.ma (M.B.); mohamed.senhadji@ensias.um5.ac.ma (M.S.)

<sup>2</sup> Smartilab Laboratory, École Marocaine des Sciences de l'Ingénieur (EMSI), Honoris United Universities, Rabat 10000, Morocco

<sup>3</sup> Harmony Technology, Rabat 10100, Morocco; b.elbhiri@ieee.org

\* Correspondence: ismail\_elgaabouri@um5.ac.ma

<sup>†</sup> Presented at the 7th edition of the International Conference on Advanced Technologies for Humanity (ICATH 2025), Kenitra, Morocco, 9–11 July 2025.

## Abstract

From hieroglyphic writing in ancient Egypt to the post-quantum edge, cryptology is usually seen as an immortal concept that evolves within the enhancement of human civilization. However, modern cryptography primitives try to make revealing ciphered information as tough as possible for attackers. As a sort of enhancement, substitution boxes play an important role in leveraging security, especially for symmetric-based algorithms. The S-box concept is integrated internally into the encryption process for block ciphers and added as a strengthened layer for stream ciphers. Consequently, in-depth analytical considerations are always needed to gather the required information if any S-box wants to be integrated. For this reason, this paper is about providing a scrutiny cryptanalysis for these S-boxes and, more precisely, size ones, since they are not widely investigated.

**Keywords:** substitution box; cryptanalysis; security



Academic Editor: Ayman S. Mosallam

Published: 15 October 2025

**Citation:** El Gaabouri, I.; Belkasmi, M.; Senhadji, M.; El Bhiri, B. An In-Depth Analytical Cryptanalysis for Substitution Boxes: Odd Size Case Study. *Eng. Proc.* **2025**, *112*, 38. <https://doi.org/10.3390/engproc2025112038>

**Copyright:** © 2025 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) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Cryptography is derived from two words from the ancient greek language, ‘Krypto’, meaning secret, and ‘graphein’, meaning drafting or writing. Cryptography at first sight comes as a technique to cover up the information and make it secretly transmitted between different instances (humans, servers, wall writes) [1]. It tries to transform a human-comprehensible message into an obscure text called a ciphertext (incomprehensible). This process is called encryption, and to obtain the original message, reversing the procedure is sufficient to recover its value. The ciphering and deciphering approach plays a paramount role in safeguarding communications. Nevertheless, cryptology is considered a timeless science that has been in progress since its early appearance. The first exemplars of cryptography were seen in Ancient Egypt (4000 BC) with the pharaohs, while its edge today is the post-quantum era, where the National Institute of Technology (NIST) tries to prepare some cryptosystems immune to quantum computer attacks. In general, cryptography provides some necessary security properties that guarantee the trustworthiness of the information flow. This illustrates its importance to always be in the enhancement process. One of its main objectives is to ensure the confidentiality of any system’s users by hiding the real value of the information that typically crosses the Internet [2]. Thus, cryptography

primitives are categorized into two main sorts: symmetric and asymmetric algorithms. The first ones are set to use the same key for both the encryption and decryption processes. Meanwhile the second ones apply two different keys referred to as the public key and private key for encrypting and deciphering, respectively [3]. Since asymmetric algorithms are not resource-friendly in operational use, symmetrical ones are widely preferred due to their simplicity of usage (only one key is needed). One of the main components of the symmetric primitives is the substitution boxes, since they are the only part of the ciphering process that offers nonlinearity between the input and the output. Therefore, this essential component requires in-depth consideration due to its significant impact on the cryptosystem's security strength. As a result, this paper provides an analytical cryptanalysis from several standpoints. This paper is structured as follows: Section 2 highlights the article topic's state of the art. Section 3 illustrates several cryptanalysis properties that an S-box must consider to level up its resistance to cryptanalysis-based attacks. Section 4 uncovers some of the well-known odd S-box cryptographic measurements in the literature. At the other end, Section 5 calls attention to further consideration that must be taken into action by researchers to enhance the S-boxes' resilience to several cryptanalysis-related attacks. To summarize, Section 6 synthesizes this article and open pathways for future perspectives on the topic.

## 2. State of the Art

Substitution box (S-box) designs are frequently used to enhance cryptographic primitives' security, more precisely, the relation between the input and the output for the attackers to counterfeit. In cryptography, Boolean functions are used as a source of nonlinearity to build this sort of S-box, making it the only part of the cryptosystem that offers this crucial attribute [4,5]. S-boxes are considered transform Boolean functions that generally take  $n$  input bits and generate  $m$  output bits. The generated S-box can be represented mathematically as the following function:

$$S : F_2^n \rightarrow F_2^m, \quad x \rightarrow S(x)$$

Based on the published works in the literature, there are three types of S-boxes based on their input/output sizes. They can be presented as follows in Table 1.

**Table 1.** S-box types in the literature [4].

| S-Box Type       | Description                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------|
| Straight S-box   | Refers to the S-box design whose input and output have selfsame length                        |
| Compressed S-box | Highlights the S-box architecture in which its input length is greater than the output length |
| Expanded S-box   | Contrary to compressed S-box designs, the input is shorter than the output in length.         |

Also referring to the literature, the S-box size does not exceed 9 bits in size and remains at a 3-bit size as the lowest possible. Passing from the example of the *Pyjmask*<sub>3</sub> integrated S-box to the DryGASCON256 one, even S-box sizes are widely adopted due to their ease of use for block ciphers, since block sizes are also even (32-bit, 64-bit, 92-bit, 128-bit, 192-bit, 256-bit). For example, the widely employed AES cipher integrates a straight 8-bit S-box, and DES incorporates a compressed 6-bit-to-4-bit S-box. Hence, odd-sized ones are ordinarily neglected or rarely utilized. For this reason, we will try to focus on some of the efforts made by researchers to mainstream the latter, along with providing an overarching idea

about their security strength based on some of the well-known cryptographic measurements that exemplify these S-boxes' resistance to the following cryptanalysis attacks [6]. We can mention bijectivity, nonlinearity, linearity, differential attack resistance, the avalanche effect, and the immunity to algebraic attacks. Consequently, odd-sized S-boxes require specialized cryptanalysis because they do not fit neatly into classical binary cryptographic frameworks. Their mathematical properties, attack surfaces, and implementation quirks make them both interesting and challenging to analyze. Hence, cryptologists must adapt standard techniques (linear/differential cryptanalysis) or develop new ones to evaluate their security.

### 3. Cryptographic Measurements for S-Box Security Assessment

In this section, we try to point out the widely used cryptographic measurement by researchers to assess the substitution boxes' security strength. Hence, the security evaluation differs between even and odd S-box sizes. In our work, we are concerned only with measurements related to odd sizes as follows.

#### 3.1. Bijectivity

Since S-boxes are considered a Boolean function, one of their main properties is that an input must have only one output. For this reason, the bijectivity property carries this out, where hamming weight is used for this matter.

$$H_{wt}(\sum_{i=1}^n b_{if_i}) = 2^{m-1} \quad (1)$$

In this article, all the involved S-boxes meet the bijectivity property.

#### 3.2. Nonlinearity

The major idea of this cryptography property is to make solving a set of equations to obtain the initial input a hard task for the attacker to accomplish. Thus, the average hamming distance is used for odd-size S-boxes.

#### 3.3. Linearity Property

This property refers to a type of statistical attack that seeks the highest value of the input–output factor disproportion, where the Linear Approximation Table is set to be constituted as a fact of fact. We will consider the linear uniformity (LU) measure, which indicates the highest value in the Linear Approximation Table [4,7].

#### 3.4. Differential Property

This property refers to a type of statistical attack that utilizes the S-box Differential Distribution Table (DDT) attributes to harvest information about the previous input/output values. We will consider the differential uniformity (DU) measure, which indicates the highest value on the DDT.

#### 3.5. Avalanche Effect

This is a metric that examines the extent to which a cryptographic function's output varies when its input is moderately altered [8]. To attain a good avalanche effect property, the Strict Avalanche Criterion (SAC) must have a change in the output greater than or equal to half (0.5 or 50%),

### 3.6. Algebraic Attack Resistance

This kind of cryptanalysis attack depends on the function's algebraic characteristics. The primary intention of an algebraic assault is to identify a polynomial with a certain quality related to the Boolean function [9]. We will consider the Algebraic Immunity measure, which indicates the maximum polynomial degree that is needed to break through the whole S-box.

## 4. S-Box Cryptanalysis

To draw attention to the different cryptographic characteristics of odd-sized substitution boxes in the literature, this section will attempt to highlight the commonly used ones together, highlighting their strengths and identifying the qualities that specifically require more examination, despite their infrequent incorporation. Thereby, some instances of each odd-size length will be taken into the evaluation process just to highlight how the values of the cryptographic measurements differ from one S-box size to another. Thus, for 3-bit S-boxes the choice is *Pyjmask*<sub>3</sub> [10] and PRINTcipher [11] S-box ciphers. For 5-bit S-boxes, Ascon's [12], *Fides*<sub>5</sub> [13] and Shamash [14] are considered. For 7-bit S-boxes, Wage [15] is selected, and for 9-bit the DryGASCON256 [16] integrated S-box will be also involved (Figures 1–6).

It is known that a cryptosystem's strength is directly related to its S-box resilience. However, an S-box's strength always depends on the construction methods used. To the best of our knowledge, there are three widely used methods: random search, metaheuristic, and mathematical. As an example, random search could find acceptable S-boxes with ease of implementation. Metaheuristics need more thoughtfulness but offer near-to-optimal dynamic patterns. Lastly, mathematical methods offer robust solutions that suffer from being statistical [4]. In this work, we are focusing on providing a thorough cryptanalysis to spotlight some of the S-box sizes that require more exploration by cryptographers. Based on Table 2, we can notice the following:

- The sophisticated small-size S-boxes highlight satisfactory cryptanalysis values, where *Pyjmask*<sub>3</sub> and PRINTcipher have similar results, where the nonlinearity equals 1.7142, which is extremely good for a 3-bit S-box. For linear uniformity and differential uniformity, the outcomes are tolerable due to the small number of possibilities. The avalanche effect is broadly met by both ciphers together with immunity to algebraic attacks.
- For 5-bit sboxes, thrice-evaluated S-boxes carry out flawlessly the cryptanalysis recommendations by NIST. However, Shamash exhibits the best upshots in comparison with both Ascon and *fides*<sub>5</sub>.
- Larger odd-size S-box cryptographic properties need to be more optimized, since for average hamming distance the values 3.156 and 3.75 for Wage and DRYGASCON256, respectively, are under what a good nonlinearity is expected to be.
- For linear and differential attack resistance, Wage provides an acceptable value when compared to DRYGASCON256 but needs more improvement in order to be categorized as a good S-box contender.
- SAC values are not as they are recommended to be, where both Wage and DRYGASCON values are under 50%, at 35% and 47.57% accordingly.
- For algebraic immunity, the value is always preferred to be at least half of the number of the used bits in the S-box. All the examined S-box examples need more consideration regarding this property. But, the 7-bit and 9-bit ones require some serious attention, especially DRYGASCON256, where an attacker can solve a polynomial of degree 3 to gain information about a 9-bit Boolean function.

|   |   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7 |
|---|---|----|----|----|----|----|----|----|---|
| 0 | 4 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 |
| 1 | 0 | 0  | -2 | -2 | 0  | 0  | 2  | -2 |   |
| 2 | 0 | 0  | 0  | 0  | 2  | -2 | -2 | -2 |   |
| 3 | 0 | 0  | 2  | -2 | 2  | 2  | 0  | 0  |   |
| 4 | 0 | -2 | 0  | -2 | 0  | -2 | 0  | 2  |   |
| 5 | 0 | 2  | 2  | 0  | 0  | -2 | 2  | 0  |   |
| 6 | 0 | -2 | 0  | 2  | 2  | 0  | 2  | 0  |   |
| 7 | 0 | -2 | 2  | 0  | -2 | 0  | 0  | -2 |   |

Figure 1. Pyjmask3 3-bit S-box Linear Approximation Table.

|    | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | a  | b  | c  | d  | e  | f  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1a | 1b | 1c | 1d | 1e | 1f |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0  | 16 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |    |
| 1  | 0  | 0  | 0  | -4 | -4 | -4 | 4  | 0  | 0  | 4  | 4  | -4 | 0  | -4 | -4 | -4 | 0  | 0  | -4 | 0  | 0  | 0  | -4 | 0  | 0  | 4  | 0  | 0  | 4  | 0  | 4  | -4 |    |
| 2  | 0  | 0  | 4  | -4 | -4 | 0  | 4  | 0  | 0  | 0  | 0  | 0  | 4  | 0  | 0  | -4 | 4  | -4 | 4  | 4  | 0  | 4  | 4  | 0  | -4 | -4 | 0  | 0  | 0  | 4  | 0  | 4  |    |
| 3  | 0  | 0  | -4 | 0  | 0  | -4 | 0  | 0  | 0  | -4 | 4  | 4  | 4  | -4 | 4  | 0  | -4 | -4 | 0  | -4 | 0  | 4  | 0  | 0  | -4 | 0  | 0  | 0  | 4  | -4 | -4 | 0  |    |
| 4  | 0  | 0  | 0  | 0  | 0  | 0  | 4  | -4 | 0  | 0  | 4  | 4  | -4 | -4 | -4 | 4  | 4  | 0  | 4  | 0  | 4  | 0  | 0  | 4  | 4  | 0  | 0  | -4 | 0  | -4 | 0  | 4  |    |
| 5  | 0  | 0  | 0  | 4  | -4 | -4 | 0  | -4 | 0  | 4  | 0  | 0  | 4  | 0  | 0  | 0  | -4 | 0  | 0  | 0  | -4 | 0  | 4  | -4 | 4  | -4 | 4  | -4 | 0  | -4 | -4 | 4  | 0  |
| 6  | 0  | 0  | 4  | 4  | 4  | 0  | 0  | 4  | 0  | 0  | 4  | -4 | 0  | 4  | -4 | 0  | 0  | -4 | 0  | -4 | 4  | 4  | 4  | -4 | 0  | 4  | 0  | -4 | 0  | 0  | 0  | 0  |    |
| 7  | 0  | 0  | -4 | 0  | 0  | 4  | -4 | -4 | 0  | -4 | 0  | 0  | 0  | 0  | 0  | -4 | 0  | -4 | -4 | 4  | 4  | -4 | 0  | -4 | 0  | 0  | 0  | -4 | 4  | 0  | 4  | 4  |    |
| 8  | 0  | -4 | 4  | 0  | 4  | 4  | 4  | 4  | 0  | 0  | 0  | 0  | 0  | -4 | 4  | 0  | 0  | 0  | -4 | 4  | -4 | 0  | 4  | 0  | 4  | 0  | -4 | 0  | 4  | -4 | 0  | 0  |    |
| 9  | 0  | -4 | 4  | -4 | 0  | 0  | 0  | -4 | 0  | -4 | -4 | -4 | 0  | 0  | 0  | 4  | 0  | 0  | 0  | -4 | -4 | 0  | 0  | 0  | -4 | 4  | 4  | 0  | 0  | -4 | 4  | 4  |    |
| a  | 0  | -4 | 0  | 4  | 0  | 4  | 0  | -4 | 0  | 0  | 0  | 0  | 4  | -4 | 4  | -4 | 4  | 4  | 0  | 0  | 4  | 4  | 0  | 0  | 4  | 4  | 0  | -4 | 0  | 0  | -4 |    |    |
| b  | 0  | -4 | 0  | 0  | 4  | 0  | -4 | -4 | 0  | 4  | 4  | -4 | 4  | 0  | 0  | 0  | 4  | -4 | 4  | 0  | -4 | -4 | -4 | 0  | 0  | 0  | -4 | 0  | 0  | 0  | -4 | 0  |    |
| c  | 0  | 4  | -4 | 0  | 4  | -4 | 0  | 0  | 0  | -4 | -4 | 4  | 0  | 0  | 4  | 4  | 0  | 0  | 4  | 0  | 0  | 4  | 4  | 0  | 0  | 4  | -4 | 4  | 0  | 0  | -4 |    |    |
| d  | 0  | -4 | -4 | -4 | 0  | 0  | 4  | 0  | 0  | 4  | 0  | 0  | -4 | 4  | 4  | 0  | 4  | 0  | -4 | -4 | 0  | 0  | 0  | -4 | 0  | -4 | 4  | -4 | 0  | 0  | -4 | 0  |    |
| e  | 0  | 4  | 0  | 4  | 0  | 4  | 4  | 0  | 0  | 0  | 4  | -4 | 0  | 0  | 0  | 0  | 4  | 4  | 0  | 0  | -4 | 0  | -4 | -4 | -4 | 4  | 4  | 4  | -4 | 0  | 0  |    |    |
| f  | 0  | -4 | 0  | 0  | -4 | 0  | 0  | 0  | -4 | 0  | 0  | 0  | -4 | -4 | 4  | 0  | -4 | 0  | 0  | 0  | 0  | -4 | 4  | -4 | 4  | 0  | 4  | 4  | 0  | 4  | -4 | -4 |    |
| 10 | 0  | 0  | 4  | -4 | 0  | 0  | -4 | -4 | 4  | 0  | 4  | 0  | 0  | 4  | 0  | -4 | -4 | 4  | 0  | 0  | 0  | 0  | 4  | 4  | 4  | 0  | 4  | 0  | 4  | 0  | -4 | 0  |    |
| 11 | 0  | 0  | 4  | 0  | 4  | -4 | 0  | -4 | 4  | -4 | 0  | 4  | 0  | 0  | -4 | 0  | 4  | 4  | -4 | 0  | 0  | 0  | 0  | -4 | -4 | -4 | -4 | 0  | 0  | 0  | 0  | -4 |    |
| 12 | 0  | 0  | 0  | 0  | 4  | 0  | 0  | 4  | 4  | 0  | 4  | 0  | 4  | -4 | 0  | 0  | 0  | 0  | -4 | -4 | 0  | -4 | 0  | 4  | 0  | -4 | 4  | 0  | -4 | 4  | 4  | 4  |    |
| 13 | 0  | 0  | 0  | 4  | 0  | -4 | 4  | -4 | -4 | 0  | -4 | -4 | 0  | 4  | -4 | 0  | 0  | 0  | -4 | 0  | -4 | 0  | -4 | 4  | 4  | 0  | 0  | -4 | 0  | 4  | 0  | 0  |    |
| 14 | 0  | 0  | 4  | 4  | 0  | 0  | 0  | 0  | 4  | 0  | 0  | 4  | -4 | 0  | 4  | 0  | 0  | -4 | 4  | 0  | -4 | 0  | -4 | 0  | 0  | 0  | 4  | -4 | 4  | 4  | 4  | -4 |    |
| 15 | 0  | 0  | 4  | 0  | 4  | -4 | -4 | 0  | -4 | 4  | -4 | 0  | -4 | -4 | 0  | -4 | 0  | -4 | 0  | 0  | 4  | 0  | 0  | 0  | 0  | -4 | 4  | 4  | 0  | -4 | 0  | 0  |    |
| 16 | 0  | 0  | 0  | 0  | -4 | 0  | -4 | 0  | 4  | 0  | 0  | -4 | 0  | 0  | 4  | 4  | 4  | 0  | 0  | -4 | 4  | 4  | 0  | 0  | 4  | -4 | -4 | 4  | 4  | 0  | 4  | 0  |    |
| 17 | 0  | 0  | 0  | -4 | 0  | 4  | 0  | 0  | 4  | 4  | -4 | 0  | 0  | -4 | 0  | 0  | -4 | 0  | 4  | -4 | 4  | -4 | 4  | 0  | -4 | 0  | -4 | -4 | 0  | 0  | 0  | -4 |    |
| 18 | 0  | -4 | 0  | -4 | 4  | -4 | 0  | 0  | -4 | 0  | 4  | 0  | 0  | 0  | 4  | 4  | -4 | 4  | 4  | 4  | 4  | 0  | 0  | -4 | 0  | 0  | 0  | 0  | 0  | 4  | 4  | 0  |    |
| 19 | 0  | -4 | 0  | 0  | 0  | 0  | 4  | 0  | 4  | -4 | 0  | -4 | 0  | 4  | 0  | 0  | -4 | -4 | 0  | 4  | 4  | 0  | -4 | 4  | 0  | -4 | 0  | 0  | -4 | -4 | 0  | -4 |    |
| 1a | 0  | 4  | 4  | 0  | 0  | -4 | 4  | 0  | 4  | 0  | -4 | 0  | 4  | 0  | 4  | 0  | 0  | 0  | 0  | 0  | 0  | 4  | -4 | -4 | -4 | 4  | 4  | 0  | 0  | 0  | 0  | -4 | 4  |
| 1b | 0  | 4  | -4 | -4 | 4  | 0  | 0  | 0  | 4  | -4 | 0  | -4 | -4 | -4 | 0  | -4 | 0  | 0  | 4  | 0  | -4 | 4  | 0  | -4 | 4  | 0  | 0  | 0  | -4 | 0  | 0  | 0  |    |
| 1c | 0  | 4  | 0  | -4 | 4  | 4  | 4  | -4 | -4 | 0  | 0  | 4  | 4  | 4  | 0  | 0  | -4 | 0  | -4 | 0  | 0  | 0  | 0  | 4  | 0  | 0  | 4  | 0  | 0  | 4  | -4 |    |    |
| 1d | 0  | -4 | 0  | 0  | 0  | 0  | 0  | 4  | -4 | -4 | -4 | 0  | 4  | 0  | -4 | -4 | 0  | 4  | 4  | -4 | 0  | 0  | -4 | 0  | 4  | -4 | 0  | -4 | 4  | 0  | 0  | 0  |    |
| 1e | 0  | -4 | -4 | 0  | 0  | -4 | 0  | 4  | 4  | 0  | 0  | 4  | 0  | 4  | 0  | -4 | 4  | 0  | 4  | 0  | 0  | -4 | 4  | 0  | 0  | 4  | 0  | 4  | 0  | -4 | 4  | 0  |    |
| 1f | 0  | 4  | 4  | -4 | -4 | 0  | -4 | 4  | -4 | -4 | 4  | 0  | 0  | 0  | 4  | 0  | 4  | 0  | 0  | 0  | 0  | -4 | 0  | 0  | 0  | 0  | 0  | 0  | -4 | -4 | -4 | 0  | -4 |

Figure 2. Fides5 5-bit S-box Linear Approximation Table.

|   | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 |
| 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 |
| 3 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 |
| 4 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 |
| 5 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 |
| 6 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 |
| 7 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 |

Figure 3. PRINTcipher 3-bit S-box Distributed Differential Table.

|    | 0  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1a | 1b | 1c | 1d | 1e | 1f |   |   |
|----|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|
| 0  | 32 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |   |   |
| 1  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 4  | 0  | 4  | 0  | 4  | 0  | 4  | 0 |   |
| 2  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4  | 0  | 4  | 0  | 4  | 0  | 4  | 0  | 4  | 0  | 4  | 0  | 4  | 0  | 4  | 0  | 4 |   |
| 3  | 0  | 4 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 4 | 0 | 0 | 4  | 0  | 0  | 0  | 4  | 0  | 0  | 0  | 4  | 0  | 0  | 0  | 4  | 0  | 0  | 0  | 0 |   |
| 4  | 0  | 0 | 0 | 0 | 0 | 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 8 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 8  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 8  | 0 |   |
| 5  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4  | 0  | 4  | 4  | 0  | 4  | 0  | 4  | 0  | 4  | 0  | 4  | 0  | 0  | 4  | 0  | 4 |   |
| 6  | 0  | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0 | 2 |
| 7  | 0  | 0 | 4 | 4 | 0 | 0 | 4 | 4 | 0 | 0 | 4 | 4 | 0 | 0 | 4 | 4 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 |   |
| 8  | 0  | 0 | 0 | 0 | 0 | 0 | 4 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 4 | 0  | 0  | 0  | 0  | 0  | 0  | 4  | 4  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 4  | 4 |   |
| 9  | 0  | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 2  | 0  | 2  | 0  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 2  | 0  | 2 | 0 |
| a  | 0  | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 0  | 2  | 2  | 0  | 2  | 0  | 0  | 2  | 0  | 2  | 2  | 0  | 2  | 0  | 2  | 0  | 0 | 2 |
| b  | 0  | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0  | 0  | 2  | 2  | 0  | 0  | 2  | 2  | 0  | 0  | 2  | 2  | 0  | 0  | 2  | 0  | 2 | 2 |
| c  | 0  | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 8  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 8  | 0  | 0  | 0  | 0  | 0  | 0  | 0 |   |
| d  | 0  | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0 | 2 |
| e  | 0  | 4 | 4 | 0 | 4 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4  | 4  | 0  | 4  | 0  | 0  | 4  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |
| f  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 4 | 0 | 0 | 4 | 4 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 4  | 4  | 0  | 0  | 4  | 4  | 0  | 0 |   |
| 10 | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 8 | 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 8  | 0  | 8  | 0  | 0  | 0  | 0  | 0 |   |
| 11 | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 8  | 0  | 8  | 0  | 8  | 0  | 8  | 0  | 8  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |
| 12 | 0  | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2  | 0  | 2 | 0 |
| 13 | 0  | 0 | 8 | 0 | 8 | 0 | 0 | 0 | 0 | 0 | 8 | 0 | 8 | 0 | 0 | 0 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |
| 14 | 0  | 0 | 0 | 0 | 4 | 4 | 4 | 4 | 0 | 0 | 0 | 0 | 4 | 4 | 4 | 4 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |
| 15 | 0  | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 4  | 0  | 4  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 4  | 0  | 4 | 0 |
| 16 | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2 | 2 |
| 17 | 0  | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 0  | 4  | 0  | 4  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 4  | 0  | 4  | 0  | 0  | 0 | 0 |
| 18 | 0  | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0  | 0  | 0  | 0  | 2  | 2  | 2  | 2  | 0  | 0  | 0  | 0  | 0  | 2  | 2  | 2  | 2 | 2 |
| 19 | 0  | 0 | 0 | 4 | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 4  | 0  | 0  | 0  | 0  | 0  | 4  | 0  | 0  | 0  | 0  | 0  | 4  | 0  | 0  | 4  | 0 | 0 |
| 1a | 0  | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 0  | 2  | 2  | 0  | 0  | 2  | 2  | 0  | 2  | 0  | 0  | 2  | 2  | 0  | 0  | 0  | 2 | 0 |
| 1b | 0  | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 0  | 0  | 2  | 2  | 2  | 2  | 0  | 0  | 0  | 0  | 0  | 2  | 2  | 2  | 2  | 0  | 0 | 0 |
| 1c | 0  | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 4  | 0  | 4  | 0  | 0  | 0  | 0  | 0  | 0  | 4  | 0  | 4  | 0  | 0  | 0  | 0  | 0 | 0 |
| 1d | 0  | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4  | 0  | 0  | 0  | 0  | 0  | 4  | 0  | 0  | 0  | 0  | 4  | 0  | 4  | 0  | 4  | 0 | 0 |
| 1e | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2 | 2 |
| 1f | 0  | 0 | 4 | 4 | 4 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 4  | 4  | 4  | 4  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 |

Figure 4. Ascon 5-bit S-box Distributed Differential Table.

$$\begin{bmatrix}
 0.25 & 0.4375 & 0.5 & 0.4375 & 0.5 & 0.5625 & 0.4375 \\
 0.5 & 0.65625 & 0.5 & 0.4375 & 0.5 & 0.5 & 0.5 \\
 0.4375 & 0.5625 & 0.25 & 0.53125 & 0.625 & 0.40625 & 0.4375 \\
 0.375 & 0.5 & 0.75 & 0.40625 & 0.4375 & 0.4375 & 0.5 \\
 0.5 & 0.4375 & 0.375 & 0.5 & 0.375 & 0.46875 & 0.625 \\
 0.375 & 0.5 & 0.5 & 0.5625 & 0.5 & 0.25 & 0.5 \\
 0.75 & 0.5 & 0.5 & 0.46875 & 0.375 & 0.5 & 0.375
 \end{bmatrix}$$

**Figure 5.** Wage 7-bit S-Box SAC matrix values.

$$\begin{bmatrix}
 0.5625 & 0.9375 & 0.0625 & 0.0625 & 0.0625 & 0.0625 & 0.0625 & 0.5625 & 0.375 \\
 0.5 & 0.5 & 0.9375 & 0.9375 & 0.0625 & 0.0625 & 0.0625 & 0.0625 & 0.625 \\
 0.5 & 0.46875 & 0.9375 & 0.9375 & 0. & 0. & 0. & 0. & 0. \\
 0.0625 & 0.53125 & 0.46875 & 0.46875 & 0.9375 & 0.9375 & 0. & 0. & 0. \\
 0.0625 & 0.0625 & 0.46875 & 0.46875 & 0.9375 & 0.9375 & 0. & 0. & 0. \\
 0.03125 & 0.03125 & 0.0625 & 0.53125 & 0.46875 & 0.46875 & 0.9375 & 0.9375 & 0. \\
 0.03125 & 0.03125 & 0.0625 & 0.0625 & 0.46875 & 0.46875 & 0.9375 & 0.9375 & 0. \\
 0.9375 & 0.0625 & 0.0625 & 0.0625 & 0.0625 & 0.5 & 0.4375 & 0.4375 & 0.875 \\
 0.4375 & 0.9375 & 0.0625 & 0.0625 & 0.0625 & 0.0625 & 0.4375 & 0.4375 & 0.625
 \end{bmatrix}$$

**Figure 6.** DRYGASCON256 9-bit S-Box SAC matrix values.

**Table 2.** Cryptanalysis of some well-known odd-size S-boxes.

| S-Box Size | Algorithm                   | $A_{HD}$ | LU  | DU  | SAC    | Algebraic Immunity |
|------------|-----------------------------|----------|-----|-----|--------|--------------------|
| 3-bit      | <i>Pyjmask</i> <sub>3</sub> | 1.7142   | 2   | 2   | 66%    | 2                  |
|            | PRINTCipher                 | 1.7142   | 2   | 2   | 66%    | 2                  |
| 5-bit      | Ascon                       | 2.5      | 8   | 8   | 57%    | 2                  |
|            | Shamash                     | 2.5      | 4   | 2   | 60%    | 2                  |
|            | <i>Fides</i> <sub>5</sub>   | 2.5      | 4   | 2   | 54%    | 2                  |
| 7-bit      | Wage                        | 3.156    | 20  | 8   | 47.57% | 3                  |
| 9-bit      | DRYGASCON256                | 3.75     | 160 | 130 | 35%    | 3                  |

## 5. Discussion

Building on the aforementioned information, S-box pattern security needs progressive enhancement since the cyber information world has developed so quickly. This fact can jeopardize the cryptographic properties of any proposed scheme. From the cryptanalysis results we have, it can be seen that smaller S-boxes are a little bit immune to some sort of cryptanalysis measurement. Nevertheless, their search space is not that large for brute-

forced searches. For example, 3-bit possibilities scale to 40,320 combinations, which are not that hard to be audited. For 5-bit built-in substitution boxes,  $32! \simeq 2.63 \times 10^{35}$  is the number of possibilities. This fact denotes that the larger the size of the S-box, the harder it is for it to be hijacked. However, resource requirements also need to be considered, since the larger size stipulates more time and energy to process one permutation. As a consequence, several endeavors have been made by researchers to mitigate as much as possible the aforesaid assault probabilities. We can cite the work presented by El Gaabouri et al. [4], where the random search method was used to provide good security, where the latter can be distinguished as the only 5-bit S-box that offers an algebraic immunity value equal to 3. Moreover, there have been other attempts to increase the number of bits used by the S-box, where lately, Prévost et al. [17] attempted the design of a 10-bit S-box that might encourage great extensions. However, considerations of the required computational resources and also the design compatibility with the block size used by any cipher are some of the enormous challenges that cryptographic designers face.

## 6. Conclusions

Achieving an ideal S-box will always be a challenging task. Thus, this topic is an open field for development. This article can be approached from the point of view that cryptographers should be aware of several challenges and how an S-box is evaluated on a cryptanalysis basis. The different outcomes emphasize the need for additional considerations of larger odd S-box sizes, which are unconventional due to the narrow regard given to them in the literature. On the other side, small ones are commonly utilized, but they have limited search spaces, which makes their fraud a question of time. For this matter, a research question can be spotlighted: How can we arrange a secure substitution box without neglecting its resource requirements? If so, can this be easily integrated into traditional cryptosystems without requiring any changes to the fundamental core of their encryption and decryption processes?

**Author Contributions:** Methodology, I.E.G.; concept validation, I.E.G., M.S., M.B. and B.E.B.; analysis, I.E.G.; writing—original draft, I.E.G.; results validation, M.S., M.B. and B.E.B. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Ethical review and approval were not required for this study in accordance with the local legislation and institutional requirements.

**Data Availability Statement:** No new data were created or analyzed in this study. Data sharing is not applicable to this article.

**Conflicts of Interest:** Brahim El Bhiri was employed by the company Harmony Technology and declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## References

1. Al-Kadit, I.A. Origins of cryptology: The Arab contributions. *Cryptologia* **1992**, *16*, 97–126. [\[CrossRef\]](#)
2. El Gaabouri, I.; Senhadji, M.; Belkasmi, M.; El Bhiri, B. A systematic literature review on authentication and threat challenges on RFID based NFC applications. *Future Internet* **2023**, *15*, 354. [\[CrossRef\]](#)
3. El Gaabouri, I.; Senhadji, M.; Belkasmi, M. A survey on lightweight cryptography approach for IoT devices security. In Proceedings of the 2022 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5g / 6G-based Interconnected Digital Worlds (NISS), Marrakech, Morocco, 30 May–1 June 2022; pp. 1–8.
4. El Gaabouri, I.; Senhadji, M.; Belkasmi, M.; El Bhiri, B. A new S-box pattern generation based on chaotic enhanced logistic map: Case of 5-bit S-box. *Cybersecurity* **2024**, *7*, 59. [\[CrossRef\]](#)

5. Naseer, M.; Tariq, S.; Riaz, N.; Ahmed, N.; Hussain, M. S-box Security Analysis of NIST Lightweight Cryptography Candidates: A Critical Empirical Study. *arXiv* **2024**, arXiv:2404.06094. [[CrossRef](#)]
6. Thakor, V.A.; Razzaque, M.A.; Darji, A.D.; Patel, A.R. A novel 5-bit S-box design for lightweight cryptography algorithms. *J. Inf. Secur. Appl.* **2023**, *73*, 103444. [[CrossRef](#)]
7. Thakor, V. Lightweight Cryptography for Resource Constrained IoT Devices. Ph.D. Thesis, Teesside University, Middlesbrough, UK, 2022.
8. Feistel, H. Cryptography and computer privacy. *Sci. Am.* **1973**, *228*, 15–23. [[CrossRef](#)]
9. Sasaki, Y.; Ling, S.; Guo, J.; Bao, Z. PEIGEN—A Platform for Evaluation, Implementation, and Generation of S-boxes. *IACR Trans. Symmetric Cryptol.* **2019**, *2019*, 330–394.
10. Goudarzi, D.; Jean, J.; Kölbl, S.; Peyrin, T.; Rivain, M.; Sasaki, Y.; Sim, S.M. Pyjamask: Block cipher and authenticated encryption with highly efficient masked implementation. *IACR Trans. Symmetric Cryptol.* **2020**, *2020*, 31–59. [[CrossRef](#)]
11. Knudsen, L.; Leander, G.; Poschmann, A.; Robshaw, M.J. PRINTcipher: A block cipher for IC-printing. In Proceedings of the Cryptographic Hardware and Embedded Systems, CHES 2010: 12th International Workshop, Santa Barbara, CA, USA, 17–20 August 2010; pp. 16–32.
12. Dobraunig, C.; Eichlseder, M.; Mendel, F.; Schläffer, M. Ascon v1. 2: Lightweight authenticated encryption and hashing. *J. Cryptol.* **2021**, *34*, 33. [[CrossRef](#)]
13. Bilgin, B.; Bogdanov, A.; Knežević, M.; Mendel, F.; Wang, Q. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware. In Proceedings of the Cryptographic Hardware and Embedded Systems—CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, 20–23 August 2013; pp. 142–158.
14. Penazzi, D.; Montes, M. Shamash & Shamashash, Lightweight Cryptography. Available online: <https://csrc.nist.gov/projects/lightweight-cryptography/round-1-candidates> (accessed on 19 April 2025).
15. AlTawy, R.; Gong, G.; Mandal, K.; Rohit, R. WAGE: An authenticated encryption with a twist. *IACR Trans. Symmetric Cryptol.* **2020**, *2020*, 132–159. [[CrossRef](#)]
16. Riou, S. DryGASCON, Lightweight Cryptography. Available online: <https://github.com/sebastien-riou/DryGASCON> (accessed on 1 January 2025).
17. Prévost, T.; Martin, B. A 10-bit S-box generated by Feistel construction from cellular automata. *arXiv* **2025**, arXiv:2507.02489. [[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.