IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 15 October 2022, accepted 21 October 2022, date of publication 26 October 2022, date of current version 9 January 2023.

Digital Object Identifier 10.1109/ACCESS.2022.3217211

RESEARCH ARTICLE

Design of Nonlinear Component of Block Cipher Using Gravesian Octonion Integers

MUHAMMAD IRFAN[1], TARIQ SHAH[1], GHAZANFAR FAROOQ SIDDIQUI[2], AMJAD REHMAN[3], (Senior Member, IEEE), TANZILA SABA[3], (Senior Member, IEEE), AND SAEED ALI BAHAJ[4,5]

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad 45320, Pakistan
[2]Department of Computer Sciences, Quaid-i-Azam University, Islamabad 45320, Pakistan
[3]Artificial Intelligence & Data Analytics Lab, CCIS, Prince Sultan University, Riyadh 11586, Saudi Arabia
[4]MIS Department, College of Business Administration, Prince Sattam bin Abdulaziz University, Alkharj 11942, Saudi Arabia
[5]Department of Computer Engineering, College of Engineering and Petroleum, Hadhramaut University, Mukalla, Hadhramout 50511, Yemen

Corresponding authors: Ghazanfar Farooq Siddiqui (ghazanfar@qau.edu.pk) and Saeed Ali Bahaj (saeedalibahaj@gmail.com)

This work was supported by the Artificial Intelligence & Data Analytics Laboratory (AIDA), CCIS, Prince Sultan University, Riyadh, Saudi Arabia.

ABSTRACT Being the only nonlinear component in many cryptosystems, an S-box is an integral part of modern symmetric ciphering techniques that creates randomness and increases confidentiality at the substitution stage of the encryption. The ability to construct a cryptographically strong S-box solely depends on its construction scheme. The primary purpose of an S-box in encryption standards is to establish confusion between the m-bit input into the n-bit output (both $m, n >= 2$). This article proposed a robust way to construct S-boxes based on the Gravesian octonion integers. We chunk the paper into threefold: firstly, a comprehensive technique for constructing S-box using affine mapping is described. The presented work is developed in such a way that for every valid input, it generates two S-boxes. Secondly, the strength of the newly generated S-box is evaluated by passing through a rigorous security analysis. Finally, a thorough comparison of the newly developed method with some well-known existing schemes is conducted. We mainly targeted some elliptic curve-based S-boxes in comparison by taking the same parameters in our scheme. The computational results and performance analysis reveal that the propose algorithm can construct a large number of distinct S-boxes that are cryptographically secured and create high resistance against various cryptanalysis attacks.

INDEX TERMS Security, substitution-box, encryption, block ciphers, Gravesian octonion integers.

I. INTRODUCTION

We are living in the information age where information is considered an asset, just like other assets. In the past few decades, the security of confidential data has attained reputable attention and vastly opened new research directions in the area of cryptography. Researchers proposed several types of data security schemes based on different mathematical structures. The main idea of these techniques is to transform confidential data into an unreadable and non-understandable form to protect it from unauthorized access. Most of the traditional symmetric cryptosystems, like Advance Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and Data Encryption Standard (DES), practically rely on the usage of substitution boxes (S-boxes) to achieve confusion in the input data up to a certain level [1]. Therefore, the efficiency of these systems primarily depends only on the cryptographic properties of their S-boxes. An S-box plays a pivotal role in strengthening the quality of encryption. It has always remained a goal of cryptosystem designers to construct an S-box with strong cryptographic performance.

A. RELATED WORK

Researchers have proposed several methods to construct highly nonlinear S-boxes. An efficient S-box is constructed by Lambić in [2] based on discrete chaotic maps. Çavuşoğlu et al. [3] described an S-box construction

The associate editor coordinating the review of this manuscript and approving it for publication was S. K. Hafizul Islam.

technique based on a chaotic scaled Zhongtang system. A new S-box construction method using triangle groups was proposed by Khan et al. in [4]. Furthermore, some investigations on the S-boxes based on chaotic neural networks and hyperchaotic systems are conducted [5], [6]. Altaleb et al. in [7] proposed the construction of an S-box by using the projective general linear group. An efficient approach to assembling S-boxes based on a Latin square is presented by El-Ramly et al. [8]. Wu et al. [9] proposed the construction of S-boxes by Latin square doubly stochastic matrix. Peng et al. [10] developed dynamic S-boxes using a spatiotemporal chaotic system. An S-box construction based on chaos theory is proposed by Wang et al. [11]. Alkhaldi et al. [12] proposed an approach for constructing S-boxes using tangent delay for ellipse chaotic sequence and a particular permutation. The resultant S-boxes showed high resistance against various cryptanalysis attacks. Khan and Azam [13] proposed an algorithm for constructing S-Boxes using affine and power mappings. Meanwhile, Khan and Azam [14] discussed the generation of multiple S-boxes based on group action and Gray code. In a study by Ahmed et al. [15], innovative construction of an S-box based on Gaussian distribution and linear fractional transformation is proposed. Similarly, Khan et al. [16] developed a systematic technique to generate an S-box using a difference distribution table. Meanwhile, Isa et al. [17] established a heuristic method called the bee waggle dance for assembling an S-box. An S-box retrieval system using artificial bee colony and optimization and the chaotic map was introduced by Ahmad et al. [18]. Zahid et al. [19] presented an innovative scheme for constructing an S-box through cubic polynomial mapping. Moreover, Tian et al. [20] suggested a method for an S-box designing based on the intertwining logistic map and bacterial foraging optimization. Furthermore, Shahzad et al. [21] developed an algorithm for designing an S-box using the action of the quotient of the modular group for multimedia security. In addition, Belazi and El-Latif [22] proposed a simple algorithm for constructing an S-box using sine chaotic maps. Furthermore, Musheer et al. [43] proposed an algorithm to assemble an S-box using generalized fusion fractal structure. Elliptic curves (ECs) have recently gained reputable attention in cryptography and are being used to design strong cryptosystems. Some cryptographers have developed algorithms for constructing S-boxes using elliptic curves [23], [24], [25], [26], [27]. Jung et al. [23] constructed S-boxes over hyperelliptic curves. Furthermore, Azam et al. [24], [26] used an elliptic curve over an ordered isomorphic elliptic curve and used typical orderings on a class of Mordell elliptic curves over a finite field and assembled 8×8 S-boxes, respectively. Hayat et al. [25], [27] developed different methods for constructing 8×8 S-boxes using an elliptic curve over prime fields. All these schemes based on elliptic curves can generate at most one S-box either on x or y-coordinates [24], [25], [26], [27].

B. OUR CONTRIBUTION

In this manuscript, we proposed a robust way for constructing S-boxes using Gravesian octonion integers. In general, octonions are non-commutative and non-associative [34], but under certain conditions, they are commutative; we discussed that study throughout this paper. The presented work is developed so that for every valid input, it yields two S-Boxes with strong cryptographic properties, while in [24], [25], [26], and [27], there is no guarantee of establishing S-boxes on both coordinates. The rest of the paper is arranged as follows: Section II comprises some definitions and concepts necessary to understand the article. The newly proposed algorithm for the construction of S-boxes is discussed in Section III. A comprehensive analysis and detailed comparison of the newly established S-boxes with some existing schemes are given in Section IV. The summary of the obtained results is highlighted in Section V.

II. PRELIMINARIES

A. OCTONION INTEGERS

After the discovery of quaternion algebra, Cayley and Graves independently discovered octonion algebra. The octonions $\mathbb{O}(\mathbb{R})$ are an eight-dimensional normed division algebra over $\mathbb{R}$, a kind of hypercomplex number system, with basis elements $e_0, e_1, e_2, \ldots, e_7$ twice as the number of dimensions of quaternion, $\mathbb{O}(\mathbb{R})$ is an extension of quaternion algebra. It is non-commutative and non-associative unital algebra; however, it is power associative. In the basis set e_0 is the unit element so that it can be denoted as 1. Any $h \in \mathbb{O}(\mathbb{R})$ can be written as a linear combination of unit octonions, i.e.,

$$h = h_0 + \sum_{i=1}^{7} h_i e_i, \text{ where } h_j \in \mathbb{R} \text{ for } j \in \{0, 1, 2, \ldots, 7\}$$

We may write an octonion h as the sum of its real part $\Re(h)$ and its vector part $\vec{v}(h)$, likewise quaternion and Gaussian integers:

$$h = h_0 + \sum_{i=1}^{7} h_i e_i = h_0 + \vec{h} = \Re(h) + \vec{v}(h).$$

An octonion is said to be pure if its real part is 0. i.e., $h = 0 + \vec{h} = 0 + \vec{v}(h)$. Addition and subtraction of any two octonions are done simply by adding and subtracting the coefficients of corresponding elements, likewise, quaternions. However, the multiplication is complex like quaternions and is discussed briefly in the following sub-section.

B. THE PRODUCT OF OCTONIONS

For any two octonions m and n given by, $m = \sum_{i=0}^{7} m_i e_i$, $n = \sum_{i=0}^{7} n_i e_i$, their product $\mathrm{o} = m \cdot \mathrm{n} = \sum_{i=0}^{7} \mathrm{o_i e_i}$. There are two methods for multiplying octonions: by using a table explained later and via matrix multiplication [38]. We have used the table method for multiplying two octonions. Let $(\mathbb{O}, *)$ be the

TABLE 1. Multiplication table of octonions [37].

$*$	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_0	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	$-e_0$	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	$-e_0$	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	$-e_0$	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	$-e_0$	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	$-e_0$	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	$-e_0$	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	$-e_0$

classical real algebra of the octonions with the basis elements $e_0, e_1, e_2, \ldots, e_7$ and multiplication table 1:

Where e_0 is the identity element. From the above table, by bilinearity, the multiplication of any two octonions can be attained. The multiplication of the octonions is verified by using an example from [39], i.e., if we have $A = [1\ 2\ 3\ 4\ 1\ 2\ 1\ -1]$, and $B = [2\ -1\ 1\ 2\ 3\ -4\ 1\ 2]$ then, $A \cdot B = [-1\ -8\ -3\ 14\ -1\ 2\ 34\ -7]$, in the same way, we can multiply any two octonions using multiplication code.

In general, the commutative property of multiplication does not hold for octonion integers; however, commutativity holds if the vector parts of octonion integers are parallel to each other. Defining $\mathbb{O}(\mathbb{K})$ as, $\mathbb{O}(\mathbb{K}) = \{h_0 + h_1(e_1 + e_2 + \ldots + e_7) : h_0, h_1 \in \mathbb{Z}\}$ which is a subring of Octavian integers [34], the commutativity property of multiplications holds over $\mathbb{O}(\mathbb{K})$.

In the exhibited Table 1, one can easily observe that:

1) $e_1, e_2, \ldots, e_7$ are square roots of $-e_0$ i.e., $e_i^2 = -e_0$ for all $i \in \{1, 2, \ldots, 7\}$
2) e_i and e_j are noncommutative whenever $i \neq j$, $e_ie_j = -e_je_i$ where $i, j = \{1, 2, 3, 4, 5, 6, 7\}$
3) While dealing different e_i and e_j $(i \neq j)$, the only non-zero product attain are $e_1e_2 = e_3, e_1e_4 = e_5, e_1e_7 = e_6, e_6e_2 = e_4, e_5e_7 = e_2, e_3e_4 = e_7, e_3e_7 = e_5$ and their cyclic permutation.

As e_0 is the identity element; thus, Table 1 can be expressed more generally as,

$$e_ie_j = \begin{cases} e_i & \text{if } j = 0 \\ e_j & \text{if } i = 0 \\ \varepsilon_{ijk} \cdot e_k - \delta_{ij}e_0 & \text{otherwise} \end{cases}$$

where δ_{ij} is the Kronecker delta (equal to 1 if and only if $(i = j)$ and ε_{ijk} is a completely antisymmetric tensor with value 1 when $ijk = 123, 145, 176, 246, 257, 347, 365$ and equal zero in the remaining cases [35].

The plane mnemonic totally describes the algebra structure of the octonions and the previous octonion multiplication table. In figure 1, one can see a little gadget with 7 points and 7 lines. The lines are the sides of a triangle, its altitudes, and the circle containing all midpoints of the sides. Each pair of distinct points lie on a unique line. Each line contains three points, and each of these triplets has a cyclic ordering shown by the arrows [36]. Some notations and results related to octonions are presented in the next sub-sections.

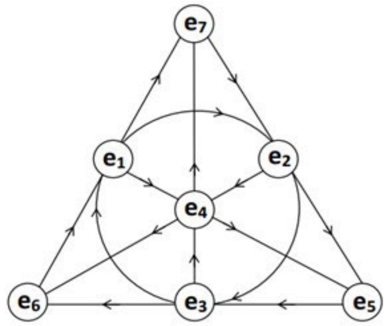


FIGURE 1. Fano plane for the octonion multiplication.

C. CONJUGATE AND NORM OF OCTONIONS

For any general element $h \in \mathbb{O}(\mathbb{R})$, $h = h_0 + \sum_{i=1}^{7} h_ie_i$ where $h_j \in R$ for $j \in \{0, 1, 2, \ldots, 7\}$, its conjugate is the octonion $\overline{h} = h_0 - \sum_{i=1}^{7} h_ie_i = h_0 - \vec{h} = \Re(h) - \vec{v}(h)$ and the norm $\mathcal{N}(h)$ is defined as,

$$\mathcal{N}(h) = h \cdot \overline{h} = \overline{h} \cdot h = h_0^2 + h_1^2 + h_2^2 + h_3^2 + h_4^2 + h_5^2 + h_6^2 + h_7^2.$$

Furthermore, for any $m, n \in \mathbb{O}(\mathbb{R})$,

$$\overline{(m+n)} = \overline{m} + \overline{n}, \overline{(m \cdot n)} = \overline{m} \cdot \overline{n}$$

and

$$\mathcal{N}(m \cdot n) = \mathcal{N}(m) \cdot \mathcal{N}(n)$$

this shows that the octonionic norm is multiplicative. In this work, we focus on Gravesian octonion integers $\mathbb{O}(\mathbb{Z})$, the octonions with all coordinates in $\mathbb{Z}$ [34]. Let $\vee = \mathbb{O}(\mathbb{K}) = \{a + bw : a, b \in \mathbb{Z}\} \subset \mathbb{O}(\mathbb{Z})$, where $w = \sum_{i=1}^{7} e_i$, the octonion $x \in \mathbb{O}(\mathbb{K})$ is prime if $\mathcal{N}(x)$ is prime in $\mathbb{N}$. Let $u = c + dw \in \mathbb{O}(\mathbb{K})$; we have $\mathcal{N}(u) = u \cdot \bar{u} = c^2 + 7d^2$. We have successfully extended some of the results of Hamiltonian quaternion integers [40], which are applicable for the above discussed associative and commutative ring $\vee$ where $\vee \subset \mathbb{O}$ (Octavian integers) [34].

Theorem: If $u = a + b \cdot \sum_{i=1}^{7} e_i$, where a and b are relatively prime, then $\mathbb{O}(\mathbb{K})/\langle u \rangle$ is isomorphic to $\mathbb{Z}_{a^2+7b^2}$ where $\mathcal{N}(u) = p = a^2 + 7b^2$ and p is a prime.

Proof: Suppose that a and b are positive integers and relatively prime to each other, and b is relatively prime to $a^2 + 7b^2$, clearly without any loss of generality $a^2 + 7b^2 \equiv 0 \left(\text{mod} a^2 + 7b^2\right), a^2 \equiv -7b^2 \left(\text{mod} a^2 + 7b^2\right), a^2b^{-2} \equiv -7 \left(\text{mod} a^2 + 7b^2\right), \left(ab^{-1}\right)^2 \equiv -7(\text{mod } a^2 + 7b^2)$, defining $f : \mathbb{O}(\mathbb{K}) \rightarrow \mathbb{Z}_{a^2+7b^2}$ by $f\left(x + y \cdot \sum_{i=1}^{7} e_i\right) = x - \left(ab^{-1}\right)y$
$\left(\text{mod} a^2 + 7b^2\right)$, clearly, f is surjective and preserve addition. Let $\alpha_1 = x_1 + y_1 \cdot \sum_{i=1}^{7} e_i$, and $\alpha_2 = x_2 + y_2 \cdot \sum_{i=1}^{7} e_i$ be in $\mathbb{O}(\mathbb{K})$. Since

$$f(\alpha_1) \cdot f(\alpha_2) = \left(x_1 - \left(ab^{-1}\right)y_1\right) \cdot \left(x_2 - \left(ab^{-1}\right)y_2\right)$$

$$\equiv \left(x_1x_2 + \left(ab^{-1}\right)^2 y_1y_2\right) - \left(ab^{-1}\right)(y_1x_2 + y_2x_1)$$
$$\equiv (x_1x_2 - 7y_1y_2) - \left(ab^{-1}\right)(y_1x_2 + y_2x_1)$$
$$= f\left[(x_1x_2 - 7y_1y_2) + (y_1x_2 + y_2x_1)\sum_{i=1}^{7} e_i\right]$$
$$= f\left[\left(x_1 + y_1 \cdot \sum_{i=1}^{7} e_i\right) + \left(x_2 + y_2\sum_{i=1}^{7} e_i\right)\right] = f\left(\alpha_1 \cdot \alpha_2\right)$$

This shows that f also preservers multiplication, however because

$$f\left(a + b \cdot \sum_{i=1}^{7} e_i\right) = a - \left(ab^{-1}\right) \cdot b \equiv 0$$

This implies,

$$\langle a + b.\sum_{i=1}^{7} e_i\rangle \subseteq \text{Ker}(f)$$

where $\langle\cdot\rangle$ denotes the ideal generated by the element $\left(a + b \cdot \sum_{i=1}^{7} e_i\right)$ and Ker(f) is the kernel of function f. Let $c + d.\sum_{i=1}^{7} e_i \in$ Ker(f) and let $c + d \cdot \sum_{i=1}^{7} e_i = \left(a + b \cdot \sum_{i=1}^{7} e_i\right) \cdot \left(x + y \cdot \sum_{i=1}^{7} e_i\right)$ where x and y are rational numbers, since,

$$f\left(c + d.\sum_{i=1}^{7} e_i\right) = c - \left(ab^{-1}\right) \cdot d \equiv 0$$

This implies,

$$bc - ad \equiv 0$$
$$(x + y\sum_{i=1}^{7} e_i\Big) = \frac{\left(c + d \cdot \sum_{i=1}^{7} e_i\right)}{\left(a + b \cdot \sum_{i=1}^{7} e_i\right)})$$
$$= \frac{(ac + 7bd)}{(a^2 + 7b^2)} + \frac{(ad - bc)}{(a^2 + 7b^2)}\sum_{i=1}^{7} e_i$$

This makes y an integer, now multiplying the equation $bc - ad \equiv 0$ by ab yields $ac - \left(ab^{-1}\right)^2 \cdot bd \equiv 0, \Rightarrow ac - (-7) \cdot bd \equiv 0$, so $ac + 7 \cdot bd \equiv 0$, proving that x is also an integer. Thus, we conclude that Ker(f) $\subseteq \left\langle a + b \cdot \sum_{i=1}^{7} e_i\right\rangle$, so this implies that Ker(f) $= \left\langle a + b \cdot \sum_{i=1}^{7} e_i\right\rangle$, and hence demonstrated that $\mathbb{O}(\mathbb{K})/\left\langle a + b \cdot \sum_{i=1}^{7} e_i\right\rangle$ is isomorphic to $\mathbb{Z}_{a^2+7b^2}$. Similarly, *observation*2 is also an extension from the results of Hamiltonian quaternions, which are applicable for the above-discussed subring $\vee$ of Octavian integers $\mathbb{O}(\mathbb{Z})$.

D. RESIDUE CLASS OF $\mathbb{O}(\mathbb{K})$ MODULO u^k

Let $\mathbb{O}(\mathbb{K})_{u^k}$ be the residue class of $\mathbb{O}(\mathbb{K})$ modulo u^k, where k is any positive integer and u is prime octonion integer. According to modulo function $\mu : \mathbb{O}(\mathbb{K}) \rightarrow \mathbb{O}(\mathbb{K})_{u^k}$ defined by

$$f \mapsto f - \left[\frac{f\overline{u^k}}{u\overline{u^k}}\right]u^k \tag{1}$$

$\mathbb{O}(\mathbb{K})_{u^k}$ is isomorphic to $\mathbb{Z}_{p^k}$, where $p = u.\bar{u}$ and p is an odd prime, u^k can be replaced by $u_1 \cdot u_2 \cdot u_3 \cdots u_k$ in equation (1), where $u_1, u_2, u_3, \cdots, u_k$ are distinct octonion prime integers. In equation (1), the symbol of [.] is rounding to the closest integer. The rounding of octonion can be done by rounding the real part and the coefficients of the vector part separately to the nearest integer.

Observation: Let $u = c + d\,(e_1 + e_2 + \ldots + e_7)$ be a prime in $\mathbb{O}(\mathbb{K})$ and let $p = c^2 + 7d^2$ be prime in $\mathbb{Z}$. If f is a generator of $\mathbb{O}(\mathbb{K})^*_{u^2}$ then $f^{\phi(p^2)/2} \equiv -1\left(\text{mod}u^2\right)$ where ϕ denotes the Euler phi function. Similarly, let $u_k = c_k + d_k\,(e_1 + e_2 + \ldots + e_7)$ be distinct primes in $\mathbb{O}(\mathbb{K})$ and let $p_k = c_k^2 + 7d_k^2$ be distinct primes in $\mathbb{Z}$, where $k = 1, 2, 3, \ldots, m$. If f is a generator of $\mathbb{O}(\mathbb{K})^*_{u^k}$, then $f^{\phi(p^k)/2} \equiv -1\left(\text{mod}u^k\right)$ and there exists an element h_k in $\mathbb{O}(\mathbb{K})^*$ such that $h_k^{\phi(p_k)} \equiv 1\left(\text{mod}u^k\right)$.

III. PROPOSED SCHEME FOR THE CONSTRUCTION OF S-BOXES

This section presents the algebraic structure and the proposed scheme used to construct the S-boxes. The S-boxes have been generated using the field elements built by a mapping f explained earlier. The detailed steps of the proposed method are described briefly in the steps given below,

Step 1: Select a prime octonion or an octonion $u = a + b \cdot \sum_{i=1}^{7} e_i$ such that the coefficients of real and vector parts are relatively prime, i.e., $(a, b) = 1$ and $\mathcal{N}(u) = \text{prime} = p$.

Step 2: Choose a primitive octonion integer $v = 1 + t.\sum_{i=1}^{7} e_i$, such that $\mathcal{N}(v) < \mathcal{N}(u)$, taking real part as one yields efficient results in the construction of the field.

Step 3: Construct field $\mathcal{G}$ by using the map $f \mapsto f - \left[\frac{f\overline{u^k}}{u\overline{u^k}}\right]u^k$ which is described briefly in earlier section.

Step 4: Apply mod p on the elements of $\mathcal{G}$, name the new set of elements as $\mathcal{G}^*$

Step 5: Calculate the inverses of all elements of $\mathcal{G}^*$, i.e., if $\alpha, \beta \in \mathcal{G}^*$ and $\alpha \cdot \beta(\text{mod}u)$ =[1 0 0 0 0 0 0 0].

Step 6: Choose $A = [a\ b\ b\ b\ b\ b\ b\ b]$ such that a and b are relatively prime and B without any condition from $\mathcal{G}^*$ and apply the affine transformation as $AX_i^{-1} + B, \forall X_i \in \mathcal{G}^*$.

Step 7: After that, enforce mod 256 on the results obtained from **step 6** to restrict the values between 0 to 255.

Step 8: Separate the real and vector parts and consider them as x and y coordinates.

Step 9: Apply unique command to get two arrays of random numbers between 0 to 255, then reshape the resulted elements of both coordinates into 16 by 16 matrices (lookup tables),

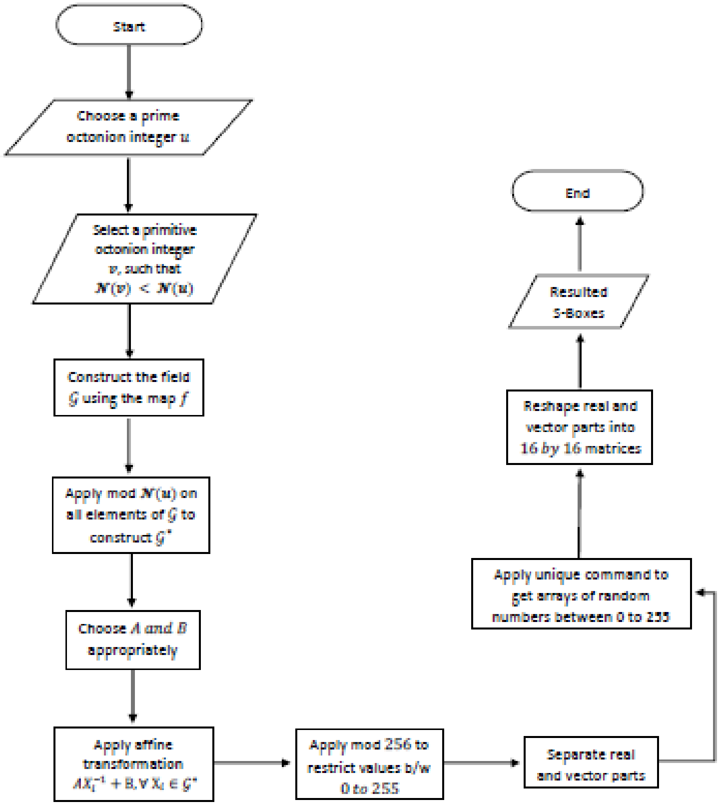


FIGURE 2. Flowchart of the newly proposed algorithm.

TABLE 2. Elements obtained after implementation of the algorithm.

Sr. No.	Elements of $\mathcal{G}$ generated by mapping f.	The values $\mathcal{G}^*$ after applying mod p on the elements of $\mathcal{G}$.	After implementing affine transformation $AX_i^{-1} + B, \forall X_i \in \mathcal{G}^*$ with mod 256.	Separating the real and vector parts as x, y coordinates.
1.	[1 10 10 . . . 10]	[1 10 10 . . . 10]	[3 157 157 . . . 157]	[3 157]
2.	[71 -5 -5 . . . -5]	[71 3408 3408 . . . 3408]	[212 88 88 . . . 88]	[212 88]
3.	[-47 11 11 . . . 11]	[3366 11 11 . . . 11]	[30 150 150 . . . 150]	[30 150]
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
1706.	[-1 0 0 . . . 0]	[3412 0 0 . . . 0]	[233 223 223 . . . 223]	[233 223]
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
3410.	[-60 -9 -9 . . . -9]	[3353 3404 3404 . . . 3404]	[34 178 178 . . . 178]	[34 178]
3411.	[-65 10 10 . . . 10]	[3348 10 10 . . . 10]	[58 154 154 . . . 154]	[58 154]
3412.	[1 0 0 . . . 0]	[1 0 0 . . . 0]	[96 156 156 . . . 156]	[96 156]

TABLE 3. The newly generated S-box $S_{A,B}^{2557}$ by x-coordinate.

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

these are the resulting S-boxes. More generally, the flowchart of the construction of the proposed S-box is presented in figure 2.

TABLE 4. The newly generated S-box $S_{A,B}^{2557}$ by y-coordinate.

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

TABLE 5. The newly generated S-box $S_{A,B}^{3413}$ by x-coordinate.

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

Repeating **step 6** by using all the possible distinct values of A, B from $\mathcal{G}^*$ yields a large number of distinct and cryptographically strong S-boxes; experimental results reveal that for each appropriate input of A, and B, one can obtain two S-boxes.

TABLE 6. The newly generated S-box $S_{A,B}^{3413}$ by y-coordinate.

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

TABLE 7. The newly generated S-box $S_{A,B}^{3613}$ by x-coordinate.

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

TABLE 8. The newly generated S-box $S_{A,B}^{3613}$ by y-coordinate.

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

TABLE 9. The newly generated S-box $S_{A,B}^{3917}$ by x-coordinate.

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

For comparing the results with some elliptic curve-based S-boxes, the algorithm is implemented for some specific prime octonions, of course, those having their norms as prime, including 2557, 3413, 3613, and 3917. The newly generated S-boxes are illustrated in tables 3-10. Elements obtained after the implementation of the algorithm are described in table 2.

Elementary representation of the scheme using $u = 5+22$. $\sum_{i=1}^{7} e_i$ = [5 22 22 22 22 22 22 22] *with* $\mathcal{N}(\mathrm{u}) = p$ = 3413, and $v = 1 + 10$. $\sum_{i=1}^{7} e_i$ =[1 10 10 10 10 10 10 10] having $\mathcal{N}(v) = 701$, satisfying $\mathcal{N}(v) < \mathcal{N}(u)$, taking A =[3379 3409 3409 3409 3409 3409 3409 3409] and B =[45 3403 3403 3403 3403 3403 3403 3403] from $\mathcal{G}^*$

TABLE 10. The newly generated S-box $S_{A,B}^{3917}$ by y-coordinate.

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

and applying the affine mapping as discussed earlier, the results are demonstrated in table 2.

IV. SECURITY ANALYSIS

After constructing the S-boxes, it is necessary to investigate their performance. In this section, we evaluated the cryptographic strength of the newly generated S-boxes by passing them through some rigorous security analysis. Generally, six parameters exist in the literature [22] that are used to examine the effectiveness of an S-box: Bijective, NL, SAC, BIC, LAP, and DAP. A brief explanation of these analyses and a thorough comparison of the resulting S-boxes with some of the recently developed S-boxes are presented in sub-sections *A* to *G*.

A. BIJECTIVE

An $n \times n$ S-box is bijective if it has every integer value from 0 to $2^n - 1$ [2]. In our case, when n=8, an S-box is bijective if it has all distinct values from the interval [0, 255]. All the proposed S-boxes are experimentally verified to hold the bijective property; the claim can be verified from tables 3-10.

B. NONLINEARITY

In order to ensure that the data is safe from an adversary, an S-box must induce a certain level of data confusion. The confusion-generating ability of an S-box over the Galois field $GF\left(2^8\right)$ is assessed by its nonlinearity $N(S)$, defined as:

$$N(S) = \min_{\varphi,\mu,\omega} \left\{ y \in GF\left(2^8\right) : \varphi \cdot S(x) \neq \mu \cdot y \oplus \omega \right\}$$

where $\varphi \in GF\left(2^8\right)$, $\mu \in GF\left(2^8\right) \backslash 0$, $\omega \in GF(2)$ and "." represent the dot product over GF (2). A highly nonlinear S-box is strong enough to generate an up to level of confusion in the data. However, Meier and Staffelbach demonstrated that an S-box with a high NL might lack other cryptographic characteristics [42]. The upper bound of nonlinearity is $N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ for S-box in GF (2^n), as S-box used in AES, is in GF $\left(2^8\right)$, so the optimal value of N is 120 . It is observed that the proposed S-box has the considerable capability to produce confusion if evaluated in terms of nonlinearity analysis. The NL of some of the newly established S-boxes is listed in Table 12-13. Note that the table contains an S-box $S_{A,B}^{3613}$ with minimum NL of 106, which is sufficient to produce high confusion.

TABLE 11. NL of the boolean functions of the proposed s-box.

Boolean function	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
Nonlinearity	106	106	108	108	106	108	106	106

TABLE 12. Detailed nonlinearities of the newly constructed S-boxes.

		Nonlinearity			
S-boxes	p	A, B	Minimum	Maximum	Average
$S^p_{A,B}$	2557	[2537 2555 . . . 2555],[10 6 . . . 6]	104	108	106.75
$S^p_{A,B}$	3413	[3403 3379 . . . 3379],[45 3403 . . . 3403]	104	110	107.25
$S^p_{A,B}$	3613	[17 3603 . . . 3603],[3585 3612 . . . 3612]	106	108	106.75
$S^p_{A,B}$	3917	[13 4 . . . 4],[31 7 . . . 7]	104	108	106.75

TABLE 13. Average NLs on *x* and *y* coordinates.

S-boxes	x-coordinate	y-coordinate
$S^{2557}_{A,B}$	106.75	105.25
$S^{3413}_{A,B}$	107.25	104.50
$S^{3613}_{A,B}$	106.75	104.00
$S^{3917}_{A,B}$	105.00	106.75

TABLE 14. BIC-nonlinearity of the proposed s-box.

...	100	106	104	104	106	104	106
100	...	100	106	104	104	100	106
106	100	...	106	98	104	106	106
104	106	106	...	96	104	100	108
104	104	98	96	...	102	102	106
106	104	104	104	102	...	102	106
104	100	106	100	102	102	...	102
106	106	106	108	106	106	102	...

TABLE 15. BIC of the proposed S-boxes.

S-boxes	Minimum	Maximum	Average
$S^{2557}_{A,B}$	0.46094	0.535156	0.50056
$S^{3413}_{A,B}$	0.45117	0.542969	0.50042
$S^{3613}_{A,B}$	0.46289	0.525391	0.50028
$S^{3917}_{A,B}$	0.48242	0.529297	0.50439

TABLE 16. BIC-SAC criterion of the proposed s-box.

...	0.505859	0.494140	0.501953	0.492187	0.490234	0.515625	0.539062
0.505859	...	0.501953	0.511718	0.486328	0.484375	0.492187	0.503906
0.494140	0.501953	...	0.492187	0.529296	0.496093	0.474609	0.505859
0.501953	0.511718	0.492187	...	0.490234	0.496093	0.525390	0.503906
0.492187	0.486328	0.529296	0.490234	...	0.511718	0.478515	0.490234
0.490234	0.484375	0.496093	0.496093	0.511718	...	0.498046	0.488281
0.515625	0.492187	0.474609	0.525390	0.478515	0.498046	...	0.513671
0.539062	0.503906	0.505859	0.503906	0.490234	0.488281	0.513670	...

C. BIT INDEPENDENCE CRITERION

Webster and Tavares were the first who introduced the criterion of bit independence [41], which is used to assess the behaviour of bit patterns at the output. The criterion's primary objective is to evaluate the dependency of a pair of output bits on an inverted input bit. An S-box is considered to have strong diffusion creation capability if all non-diagonal entries of its BIC matrix are closer to 0.5. The BIC of an S-box S over the GF (2^n) with S_i Boolean functions are evaluated by computing an n-dimensional matrix, i.e., $N(S) = [n_{ij}]$, measured as shown in the equation at the bottom of the next page, surely $n_{ii} = 0$.

D. STRICT AVALANCHE CRITERION

The idea of the Strict Avalanche Criterion was firstly presented by Webster and Tavares [41], which calculates the diffusion creation strength of an S-box. It is the measure of change in output bits when a single input bit is altered; all of the output bits vary with a probability of $\frac{1}{2}$. In general, a function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is said to fulfill SAC if for a change in an input bit $i \in \{1, 2, 3, \ldots, n\}$, the probability of change in the output bit $j \in \{1, 2, 3, \ldots, n\}$ is $\frac{1}{2}$. The offset of the dependence matrix of our proposed S-box is 0.0352, while the minimum, maximum and average values of SAC of the proposed S-box are 0.3906, 0.6406, and 0.4931, respectively. The average value of SAC is much closer to 0.5, which is considered an ideal SAC value.

TABLE 17. SAC of the proposed S-box.

0.515625	0.515625	0.437500	0.515625	0.484375	0.500000	0.546875	0.484375
0.421875	0.421875	0.468750	0.562500	0.453125	0.531250	0.500000	0.562500
0.500000	0.468750	0.484375	0.484375	0.453125	0.406250	0.515625	0.531250
0.531250	0.500000	0.500000	0.453125	0.640625	0.484375	0.515625	0.453125
0.390625	0.468750	0.578125	0.500000	0.500000	0.515625	0.468750	0.437500
0.500000	0.421875	0.421875	0.562500	0.515625	0.515625	0.468750	0.500000
0.500000	0.484375	0.484375	0.500000	0.546875	0.484375	0.468750	0.468750
0.453125	0.515625	0.453125	0.609375	0.500000	0.468750	0.453125	0.562500

TABLE 18. Detailed values of SAC.

S-boxes	Minimum	Maximum	Average	Offset
$S^{2557}_{A,B}$	0.421875	0.609375	0.502441	0.0342
$S^{3413}_{A,B}$	0.421875	0.562500	0.498770	0.0320
$S^{3613}_{A,B}$	0.390625	0.640625	0.493164	0.0352
$S^{3917}_{A,B}$	0.406250	0.593750	0.496582	0.0293

E. LINEAR APPROXIMATION PROBABILITY

Linear approximation probability configures the strength of an S-box S in terms of resistance against linear attacks. An S-box with a smaller LAP value is considered to have strong properties and vice versa. The LAP of the newly generated S-box $L(S)$ is mathematically expressed as shown in the equation at the bottom of the next page.

The LAP of the proposed S-boxes is 0.125, 0.1563, 0.1328, 0.125, respectively, which are comparatively lesser than those of [24] and [25]. This shows that the presented algorithm can construct robust and cryptographically secure S-boxes that are highly resistant against linear attacks.

F. DIFFERENTIAL APPROXIMATION PROBABILITY

Biham and Shamir [42] figured out the differential cryptanalysis for an S-box based on the imbalance in the input/output *XOR* distribution. The resistance of an S-box against differential attacks is assessed by measuring its DAP. An S-box with a smaller value of DAP is considered to have the greater capability to resist differential attacks. The results of the Approximation Probabilities are demonstrated in table 19. The DAP of an S-box S is expressed as,

$$DP(S) = n_{ij} = \frac{1}{2^n}[\#\{y \in Y \mid S(y) \oplus S(y \oplus \Delta y) = \Delta z\}]$$

where Δy and Δz are input and output differentials, respectively.

G. RUN TIME TO CONSTRUCT TWO S-BOXES

We used a PC with a processor: Intel® core i-5-6300U CPU @ 2.40 GHz 2.50 GHz, Memory: 8GB (7.89 usable)

TABLE 19. Results of approximation probabilities.

S-boxes	DAP	LAP
$S_{A,B}^{2557}$	0.039062	0.125000
$S_{A,B}^{3413}$	0.046875	0.156250
$S_{A,B}^{3613}$	0.039062	0.132813
$S_{A,B}^{3917}$	0.039062	0.125000

TABLE 20. Time efficiency of the proposed algorithm.

S-box	$S_{A,B}^{2557}$	$S_{A,B}^{3413}$	$S_{A,B}^{3613}$	$S_{A,B}^{3917}$
Time (seconds)	1.05000	1.53981	1.70685	1.95587

and MATLAB version R2021a to run the proposed algorithm for the construction of S-boxes. It has been observed that the algorithm's run time solely depends on the prime chosen; the larger the prime we take, the more time the algorithm will take for execution. The list of the average computation time in seconds for construction of the S-boxes averaged over ten times can be observed clearly in table 20, from prime 2557 to 3917. The time efficiency of our scheme is much better than the final S-box generation in [48] and lesser than [49].

H. COMPARISON WITH S-BOXES BASED ON ELLIPTIC CURVE AND SOME OTHER SCHEMES

In this section, we compare the strength of the proposed S-boxes with some elliptic curve-based S-boxes constructions schemes by discussing two critical aspects: the S-box generation capacity and the cryptographic properties of both schemes. While designing an S-box generation scheme, ensuring that the algorithm yields distinct S-boxes for every valid input is essential.

In this proposed scheme, whenever one chooses $A = [a\ b\ b\ b\ b\ b\ b\ b]$ such that a and b are relatively prime, a large number of distinct S-boxes resulted regardless of any condition on the selection of B. On the other hand, the results by schemes [24], [25], [26], [27] are uncertain and do not ensure the generation of S-boxes for every given input. Like, in [24] and [27], there is no guarantee of establishing S-boxes on both coordinates x and y. Furthermore, in [24] and [26], Azam et al. constructed S-boxes using y coordinates of the points satisfying the elliptic curve. Similarly, in [25] and [27], Hayat et al. proposed a technique that uses x-coordinates of the points satisfying elliptic curves; in our proposed algorithm, S-boxes obtained on both real and vector parts named as x and y-coordinates, irrespective of

TABLE 21. Comparison of the proposed S-boxes with some existing schemes.

S-box	NL	SAC		BIC		DAP	LAP
		Min	Max	Min	Max		
Ref. [2]	106	0.4218	0.6250	0.4746	0.5015	0.0391	0.1328
Ref. [5]	106	0.4375	0.5938	0.4648	0.5033	0.0391	0.1406
$S_{3917,353,16}^{8,8,N}$[24]	106	0.4062	0.6093	0.4648	0.5009	0.0391	0.1875
$S_{3613,1}^{1195,2950}$ [25]	104	0.4063	0.5938	0.4629	0.5254	0.0391	0.1328
$S_{3413,1}^{2266,2155}$ [25]	104	0.4063	0.5938	0.4668	0.5430	0.0391	0.1328
$S_{2557,4}^{843,669}$ [25]	104	0.4063	0.5938	0.4570	0.5293	0.0391	0.1406
Ref. [26]	106	0.3750	0.5937	0.4687	0.4988	0.0390	0.1328
Ref. [27]	104	0.4218	0.5937	0.4687	0.4965	0.0391	0.1328
Ref. [28]	104	0.3900	0.5930	0.4540	0.4990	0.0469	0.1090
Ref. [29]	103	0.4414	0.5703	0.4961	0.5039	0.0391	0.0352
Ref. [30]	106	0.4218	0.5781	0.4726	0.5004	0.0391	0.1328
Ref. [31]	102	0.3750	0.6094	0.4707	0.5215	0.0391	0.1484
Ref. [32]	106	0.4375	0.5937	0.4551	0.5029	0.0391	0.1328
Ref. [33]	106	0.4062	0.5781	0.4589	0.5016	0.0391	0.1328
Ref. [44]	104	0.4060	0.6400	0.4414	0.4993	0.0390	0.1250
Ref. [45]	106	0.4218	0.5781	0.4726	0.5039	0.0390	0.1560
Ref. [46]	104	0.4062	0.5937	0.4609	0.4997	0.0540	0.1406
Ref. [47]	106	0.4062	0.5781	0.4804	0.5038	0.0391	0.1250
$S_{A,B}^{2557}$	104	0.4219	0.6094	0.4609	0.5352	0.0391	0.1250
$S_{A,B}^{3413}$	104	0.4219	0.5625	0.4512	0.5429	0.0469	0.1562
$S_{A,B}^{3613}$	106	0.3906	0.6406	0.4629	0.5254	0.0391	0.1328
$S_{A,B}^{3917}$	104	0.4063	0.5937	0.4824	0.5293	0.0391	0.1250

having good results from either x or y-coordinates. Results have revealed that both ends can generate S-boxes having sufficiently strong cryptographic characteristics at one time. Lastly, as we targeted similar parameters, specific primes from [24], [25], [26], and [27], for a thorough comparison, i.e., 2557, 3413, 3613, and 3917, it has been revealed that the nonlinearity of the proposed S-box is comparable with [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], and [47]. The minimum nonlinearity of $S_{A,B}^{2557}$, $S_{A,B}^{3413}$, $S_{A,B}^{3613}$, $S_{A,B}^{3917}$ are 104, 104, 106, 104 respectively, while on the other side with the same primes, the NLs in [24], [25], [26], [27], and [47] are 106, 104, 106, 104, 106 respectively, which are almost similar to the proposed S-box. In addition, the cryptographic properties of proposed S-boxes are better.

Furthermore, we also compared the properties of newly established S-boxes with some already existing schemes [28], [29], [30], [31], [32], [33], [44], [45], [46], [47] in table 21. The proposed S-boxes are capable of creating better confusion likewise other schemes. This shows that the proposed scheme can produce up-to-level confusion along with the existing techniques based explicitly on elliptic curves and others.

V. CONCLUSION

In this work, a robust technique for constructing a large number of distinct and dynamic S-boxes is presented; the

$$n_{ij} = \frac{1}{2^n}\left[\sum_{\substack{x\in GF(2^n)\\ 1\le k\le 8}} w\left(S_i\left(x\oplus\alpha_j\right)\oplus S_i(x)\oplus S_k\left(x+\alpha_j\right)\oplus S_k(x)\right)\right]$$

$$L = \frac{1}{2^8}\left\{\max_{\beta,\eta}\left\{\text{abs}\left(\left|\left\{y\in \text{GF}\left(2^8\right) \mid \beta\cdot y = \eta\cdot S(y)\right\}\right| - 2^7\right)\right\}\right\}$$

proposed work is developed to generate two S-boxes for each valid input. The proposed scheme solely depends upon selecting prime octonion u, primitive octonion v, A and B. By changing these parameters, several dynamic and secure S-boxes can be obtained, which can be used efficiently in various cryptosystems, including symmetric and asymmetric ciphers for encryption purposes.

In addition, the strength of the proposed S-boxes is assessed by applying various security analyses. Furthermore, a detailed comparison of the newly constructed S-boxes with elliptic curve-based and some existing S-boxes is conducted. The computational results and performance analysis reveal that the proposed algorithm is capable of generating a large number of distinct dynamic S-boxes that are cryptographically strong against various attacks and are helpful for secure data communication purposes.

The understudy work is based on commutative Gravesian octonion integers; for future research, one can work on its non-commutative side that will yield eight S-boxes against a single input. Furthermore, the work can be extended to sedenions; 16-dimensional algebra, which is non-associative and non-commutative. More secure and dynamic S-boxes can be produced by working in these directions.

REFERENCES

[1] L. R. Knudsen and M. & Robshaw (2011), *The Block Cipher Companion*. Cham, Switzerland: Springer, 2011.
[2] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, Mar. 2017.
[3] Ü. Çavuşoğlu, A. Zengin, I. Pehlivan, and S. Kaçar, "A novel approach for strong S-box generation algorithm design based on chaotic scaled Zhongtang system," *Nonlinear Dyn.*, vol. 87, no. 2, pp. 1081–1094, 2017.
[4] A. Rafiq and M. Khan, "Construction of new S-boxes based on triangle groups and its applications in copyright protection," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 15527–15544, Jun. 2019.
[5] Y. Wang, L. Yang, M. Li, and S. Song, "A method for designing S-box based on chaotic neural network," in *Proc. 6th Int. Conf. Natural Comput. (ICNC)*, vol. 2, Aug. 2010, pp. 1033–1037.
[6] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, Jul. 2018.
[7] A. Altaleb, M. S. Saeed, I. Hussain, and M. Aslam, "An algorithm for the construction of substitution box for block ciphers based on projective general linear group," *AIP Adv.*, vol. 7, no. 3, Mar. 2017, Art. no. 035116.
[8] S. H. El-Ramly, T. El-Garf, and A. H. Soliman, "Dynamic generation of s-boxes in block cipher systems," in *Proc. 18th Nat. Radio Sci. Conf. (NRSC)*, Mar. 2001, pp. 389–397.
[9] Y. Wu, J. P. Noonan, and S. Agaian, "Dynamic and implicit Latin square doubly stochastic S-boxes with reversibility," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Oct. 2011, pp. 3358–3364.
[10] J. Peng, S. Jin, L. Lei, and X. Liao, "Construction and analysis of dynamic S-boxes based on spatiotemporal chaos," in *Proc. IEEE 11th Int. Conf. Cognit. Informat. Cognit. Comput.*, Aug. 2012, pp. 274–278.
[11] Y. Wang, K.-W. Wong, C. Li, and Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm," *Phys. Lett. A*, vol. 376, nos. 6–7, pp. 827–833, Jan. 2012.
[12] A. H. Alkhaldi, I. Hussain, and M. A. Gondal, "A novel design for the construction of safe S-boxes based on TDERC sequence," *Alexandria Eng. J.*, vol. 54, no. 1, pp. 65–69, Mar. 2015.
[13] M. Khan and N. A. Azam, "S-boxes based on affine mapping and orbit of power function," *3D Res.*, vol. 6, no. 2, pp. 1–15, Jun. 2015.
[14] M. Khan and N. A. Azam, "Right translated AES gray S-boxes," *Secur. Commun. Netw.*, vol. 8, no. 9, pp. 1627–1635, 2015.
[15] M. F. Khan, A. Ahmed, and K. Saleem, "A novel cryptographic substitution box design using Gaussian distribution," *IEEE Access*, vol. 7, pp. 15999–16007, 2019.
[16] M. A. Khan, A. Ali, V. Jeoti, and S. Manzoor, "A chaos-based substitution box (S-box) design with improved differential approximation probability (DP)," *Iranian J. Sci. Technol., Trans. Electr. Eng.*, vol. 42, no. 2, pp. 219–238, 2018.
[17] H. Isa, N. Jamil, and M. R. Z'aba, "Construction of cryptographically strong S-Boxes inspired by bee waggle dance," *New Gener. Comput.*, vol. 34, no. 3, pp. 221–238, Aug. 2016.
[18] M. Ahmad, M. N. Doja, and M. M. S. Beg, "ABC optimization based construction of strong substitution-boxes," *Wireless Pers. Commun.*, vol. 101, no. 3, pp. 1715–1729, Aug. 2018.
[19] A. Zahid and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, Mar. 2019.
[20] Y. Tian and Z. Lu, "Chaotic S-box: Intertwining logistic map and bacterial foraging optimization," *Math. Problems Eng.*, vol. 2017, pp. 1–11, Nov. 2017.
[21] I. Shahzad, Q. Mushtaq, and A. Razaq, "Construction of new S-box using action of quotient of the modular group for multimedia security," *Secur. Commun. Netw.*, vol. 2019, pp. 1–13, Nov. 2019.
[22] A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik*, vol. 130, pp. 1438–1444, Feb. 2017.
[23] J. H. Cheon, S. Chee, and C. Park, "S-boxes with controllable nonlinearity," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Berlin, Germany: Springer, May 1999, pp. 286–294.
[24] N. A. Azam, U. Hayat, and I. Ullah, "An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization," *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, Dec. 2018.
[25] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Process.*, vol. 155, no. 3, pp. 391–402, 2019.
[26] N. A. Azam, U. Hayat, and I. Ullah, "Efficient construction of a substitution box based on a mordell elliptic curve over a finite field," *Frontiers Inf. Technol. Electron. Eng.*, vol. 20, no. 10, pp. 1378–1389, Oct. 2019.
[27] U. Hayat, N. A. Azam, and M. Asif, "A method of generating 8 × 8 substitution boxes based on elliptic curves," *Wireless Pers. Commun.*, vol. 101, no. 1, pp. 439–451, Jul. 2018.
[28] J. Kim* and R. C.-W. Phan, "Advanced differential-style cryptanalysis of the NSA's skipjack block cipher," *Cryptologia*, vol. 33, no. 3, pp. 246–270, Jul. 2009.
[29] G. Tang, X. Liao, and Y. Chen, "A novel method for designing S-boxes based on chaotic maps," *Chaos, Solitons Fractals*, vol. 23, no. 2, pp. 413–419, 2005.
[30] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dyn.*, vol. 100, no. 1, pp. 699–711, 2020.
[31] G. Chen, "A novel heuristic method for obtaining S-boxes," *Chaos, Solitons Fractals*, vol. 36, no. 4, pp. 1028–1036, 2008.
[32] D. Lambić, "S-box design method based on improved one-dimensional discrete chaotic map," *J. Inf. Telecommun.*, vol. 2, no. 2, pp. 181–191, Dec. 2018.
[33] H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, "A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7333–7350, Feb. 2021.
[34] C. Flaut, "Codes over a subset of octonion integers," *Results Math.*, vol. 68, nos. 3–4, pp. 345–359, Nov. 2015.
[35] L. Sabinin, L. Sbitneva, and I. Shestakov, Eds., *Non-Associative Algebra and its Applications*. Boca Raton, FL, USA: CRC Press, 2006, p. 235.
[36] F. S. Leite, "The geometry of hypercomplex matrices," *Linear Multilinear Algebra*, vol. 34, no. 2, pp. 123–132, Mar. 1993.
[37] R. S. Kraußhar, "Function theories in Cayley–Dickson algebras and number theory," *Milan J. Math.*, vol. 89, no. 1, pp. 19–44, Jun. 2021.
[38] P. Saraiva, P. D. Beites, J. Fernandes, C. Costa, and J. Vitória, "Best pair of two skew lines over the octonions," *Adv. Appl. Clifford Algebras*, vol. 25, no. 3, pp. 657–672, Sep. 2015.
[39] A. M. Grigoryan and S. S. Agaian, *Quaternion and Octonion Color Image Processing With MATLAB*. Bellingham, WA, USA: SPIE, 2018, p. 89.
[40] M. Özen and M. Güzeltepe, "Cyclic codes over some finite quaternion integer rings," *J. Franklin Inst.*, vol. 348, no. 7, pp. 1312–1317, Sep. 2011.
[41] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, Berlin, Germany: Springer, Aug. 1985, pp. 523–534.
[42] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*. Cham, Switzerland: Springer, 2012.

[43] M. Ahmad, S. Agarwal, A. Alkhayyat, A. Alhudhaif, F. Alenezi, A. H. Zahid, and N. O. Aljehane, "An image encryption algorithm based on new generalized fusion fractal structure," *Inf. Sci.*, vol. 592, pp. 1–20, May 2022.

[44] N. Siddiqui, A. Naseer, and M. Ehatisham-ul-Haq, "A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve," *Wireless Pers. Commun.*, vol. 116, no. 4, pp. 3015–3030, Feb. 2021.

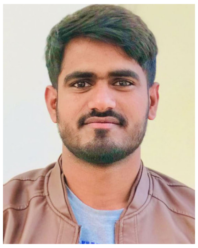
[45] A. Zahid, M. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, p. 245, Mar. 2019.

[46] A. Zahid and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, Mar. 2019.

[47] S. Ibrahim and A. M. Abbas, "Efficient key-dependent dynamic S-boxes based on permutated elliptic curves," *Inf. Sci.*, vol. 558, pp. 246–264, May 2021.

[48] A. Manzoor, A. H. Zahid, and M. T. Hassan, "A new dynamic substitution box for data security using an innovative chaotic map," *IEEE Access*, vol. 10, pp. 74164–74174, 2022.

[49] N. A. Azam, U. Hayat, and M. Ayub, "A substitution box generator, its analysis, and applications in image encryption," *Signal Process.*, vol. 187, Oct. 2021, Art. no. 108144.



MUHAMMAD IRFAN received the M.Phil. degree in mathematics from the Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan. Furthermore, he has done a career prep fellowship funded by Stanford University and Acumen. His research interests include number theory, algebraic cryptography, and information security.

TARIQ SHAH received the Ph.D. degree in mathematics from the University of Bucharest, Romania, in 2000. He is currently working as a Professor and the Chairperson of the Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan. His research interests include commutative algebra, non-associative algebra, error-correcting codes, and algebraic cryptography.

GHAZANFAR FAROOQ SIDDIQUI received the Ph.D. degree from Vrije Universiteit Amsterdam, The Netherlands, in 2010. He is currently an Associate Prof. at the Department of Computer Science, Quaid-i-Azam University, Islamabad. Previously, he was a Research Scholar with the Department of Computer Science, Vrije Universiteit Amsterdam. The Ph.D. scholarship was funded by Higher Education Commission, Pakistan. He is a reviewer of a number of peer reviewed conferences and journals. He also published numerous research papers in reputed conferences and journals. He is a member of Federal Public Service Commission and Khyber Pakhtunkhwa Public Service Commission. He is also serving as an Evaluator for scientific projects of Directorate of Science and Technology (DoST), Khyber Pakhtunkhwa. Furthermore, he is a member of Board of Studies of Quaid-i-Azam University, and National Textile University, Faisalabad.

AMJAD REHMAN (Senior Member, IEEE) received the dual Ph.D. degree (Hons.) from the Faculty of Computing, Universiti Teknologi Malaysia, with a specialization in forensic documents analysis and security, in 2010 and 2011, respectively. He is currently a Senior Researcher with the Artificial Intelligence and Data Analytics Laboratory, CCIS, Prince Sultan University, Riyadh, Saudi Arabia. He received Rector Award for 2010 best student in the university. Currently, he is a PI in several funded projects and also completed projects funded from MOHE, Malaysia, Saudi Arabia. His research interests include data mining, health informatics, and pattern recognition. He is the author of more than 200 ISI journals and conference papers.

TANZILA SABA (Senior Member, IEEE) received the Ph.D. degree in document information security and management from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia, in 2012. She won the Best Student Award from the Faculty of Computing, UTM, in 2012. Currently, she is serving as an Associate Chair of the Information Systems Department, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia. Her research interests include medical imaging, pattern recognition, data mining, MRI analysis, and soft-computing. She has above 100 publications that have around 5000 citations with H-index 43. Her mostly publications are in biomedical research published in ISI/SCIE indexed. Due to her excellent research achievement, she is included in Marquis Who's Who (S & T), in 2012. Currently, she is an editor and a reviewer of reputed journals and on the panel of TPC of international conferences. She has full command of a variety of subjects and taught several courses at the graduate and postgraduate levels. On the accreditation side, she is a Skilled Lady with ABET; NCAAA Quality Assurance. She is the Leader of the Artificial Intelligence with the Data Analytics Research Laboratory, PSU, and an Active Professional Member of ACM, AIS, and IAENG organizations. She is the PSU Women in Data Science (WiDS) Ambassador at Stanford University and Global Women Tech Conference. She received the Best Researcher Award at PSU for consecutive four years. She has been nominated as a Research Professor at PSU, since September 2019.

SAEED ALI BAHAJ received the Ph.D. degree from Pune University, India, in 2006. He is currently an Associate Professor with Hadhramaut University, Hadhramaut, Yemen. He is also an Associate Prof. with the MIS Department, CBA, PSAU, Al-Kharj, Saudi Arabia. His research interests include artificial intelligence, information management, forecasting, information engineering, big data mining, and information security.