IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 December 2023, accepted 22 December 2023, date of publication 29 December 2023,
date of current version 5 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3348144

RESEARCH ARTICLE

Elevating Network Security: A Novel S-Box Algorithm for Robust Data Encryption

JARALLAH ALQAHTANI[1], MUHAMMAD AKRAM[1], GHASSAN AHMED ALI[2], NADEEM IQBAL[3], ALI ALQAHTANI[4], AND ROOBAEA ALROOBAEA[5]

[1]Department of Computer Science, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia
[2]Faculty of Islamic Technology, Universiti Islam Sultan Sharif Ali, Brunei Darussalam
[3]Department of Computer Science and IT, The University of Lahore, Lahore 54000, Pakistan
[4]Department of Networks and Communications Engineering, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia
[5]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia

Corresponding author: Nadeem Iqbal (nadeem.iqbal537@gmail.com)

This work was supported by the Deputy for Research and Innovation-Ministry of Education, Saudi Arabia under the Institutional Funding Committee at Najran University, Saudi Arabia, under Grant NU/IFC/2/SERC/-/9.

ABSTRACT In an era characterized by ever-increasing data exchange across different networks, the importance of robust network security measures cannot be overemphasized. Cryptographic algorithms, on the other hand, perform a vital role in imparting security to the sensitive information during transmission, with S-Boxes (Substitution Boxes) serving as a fundamental component of symmetric-key ciphers. This study has endeavored to engineer a novel S-Box algorithm to bolster the network security. Moreover, the core focus of the suggested algorithm lies in enhancing the confidentiality, defiance to nefarious designs of cryptanalysis savvy, and overall cryptographic strength of data encryption in network communication. Random numbers spawned by the 5D multi-wing hyperchaotic system have been employed to design the proposed box. Apart from that, Rook —a chess piece has been used in this regard. Particularly, the random walk of Rook on the 16×16 hypothetical chessboard has been capitalized to sufficiently permute the data of the potential S-Box. Through a comprehensive performance evaluation and cryptographic analyses, the proposed S-Box algorithm exhibits superior resilience against diverse threats thus fortifying network security effectively. In particular, the state of the art security parameters like bijectivity, non-linearity (NL), strict-avalanche criterion (SAC), bit-independence criterion (BIC), linear probability (LP) and differential probability (DP) have been used. This work, no doubt, contributes significantly to the ever-evolving field of network security.

INDEX TERMS Network security, chaos, random numbers, S-Box, Rook, chess.

I. INTRODUCTION

In the realm of network security, where the protection of precious data is of prime importance, varied cryptographic techniques play an essential role in the protection of information from the malicious actors and prying eyes [1], [2], [3], [4], [5]. Out of these large number of techniques, the notion of S-Box (Substitution Box) enjoys a special status. S-Boxes are the necessary components while devising any new symmetric-key cryptosystems [6]. Symmetric-key cryptosystems, also referred to as secret-key cryptosystems, are essentially cryptographic algorithms which employ the same key for both the decryption and encryption processes [7]. These cryptosystems and ciphers depend upon the fundamental operations normally dubbed as substitution-permutation network (SPN) [8]. At the very heart of these operations lies the construct of S-Box. The particular modus operandi of S-Box works like this. It is basically a sort of lookup table which replaces all input values with some corresponding output values [9]. Although both the size and

The associate editor coordinating the review of this manuscript and approving it for publication was Shuangqing Wei.

design of these boxes may vary depending upon the particular requirements of the cipher but they must be designed in such a way that they are non-linear in their character and orientation and must be resistant to the potential cryptanalytic attacks. Here, the significance of the S-box would be discussed in the context of network security.

- *Confidentiality*: S-Boxes serve as a major driver in maintaining the confidentiality of the precious data of the different organizations [10]. The primary job of these boxes is to introduce the layer of non-linearity into the encryption processes thus making it too much challenging for the hackers to infer the relationship between the ciphertext and the plaintext without having the slightest inkling of the secret key. This feature of non-linearity inherent within the "DNA" of the S-boxes plays a very crucial role in foiling the brute-force and varied statistical attacks potentially launched by the opponents.
- *Diffusion and Avalanche Effect*: These effects are very crucial and play a significant role in the different cryptographic products. One of the jobs of S-Boxes is that a very little change in the key or the plaintext results in a sea change in the output of ciphertext [11]. This feature is normally called as avalanche effect and is very crucial in spreading the changes in the very fabric of the encryption process. Change of a single bit in an input to the S-Box can render a significantly different result. This phenomenon makes the decryption process of the encryption algorithm more challenging to the adversaries.
- *Resistance to Cryptanalysis*: Well-engineered S-Boxes are defiant to the different cryptographic attacks which include linear and differential cryptanalysis [12]. The cryptographers while designing new products, select S-Box designs which are amenable to their peculiar requirements to ensure that their products may withstand the future rigorous scrutiny.
- *Strengthening the Key*: S-Boxes are, no doubt, integral parts of key mixing and key expansion in the symmetric key ciphers [13]. These boxes ensure that the secret key is applied in an uncertain and complex manner thus cementing the whole encryption process.
- *Enhanced Security Layers*: In the Advanced Encryption Standard (AES) cipher, the inclusion of S-Box contributes to the multiple layers of security [14]. There are series of S-Boxes in the design principle of AES, each one with its unique transformation thus rendering it exceptionally robust against the varied attacks.

Despite seminal contributions to the realm of network security, S-Boxes remained the unsung heroes of this domain. They render the requisite cryptographic strength and resilience needed to protect sensitive data during the storage and transmission. As cyber threats continue to evolve and become more sophisticated in their character, the need for still stronger encryption mechanisms, including well-crafted S-Boxes, becomes increasingly more pronounced. The construct of S-Boxes contributes to the trio of network security, i.e., *confidentiality*, *integrity*, and *authenticity* of data, making them an indispensable component. In an era where cyber-attacks and data breaches are commonplace, the importance of S-Boxes in preserving the security and privacy of our digital assets cannot be exaggerated.

Many studies have developed novel algorithms for the construction of S-Boxes. For instance, the work [15] constructed an S-Box to address the shortcomings of classical ciphers like 3DES, AES and SM4. The reported work generated three S-Boxes by using the 3D discrete memristor-based chaotic map (3D-MCM). Security analysis demonstrated that the newly constructed S-Box is effective and defiant to the various threats in network security. An other work [16] identified various attacks over the cyber security products including Gröbner-based attacks, linear and differential attacks, SAT solver, XL-based attacks, interpolation attacks etc. The focus of the reported research was to design a novel algorithm for dynamic generation of S-Boxes which could defy the various algebraic structure-based and chaos-based cryptanalysis techniques. The random numbers were spawned through the true random bits of underwater acoustic waves. Further, a chain of knight's tour was employed to dynamically generate the S-Box. An other work [17] in this domain designed a 5-bit S-box. Chaotic maps were employed to generate the required stream of random numbers in the reported work. The simulation results of this study indicated that the suggested algoirthm was cost-effective and efficient as far as the performance is concerned. Besides, the suggested 5-bit S-box design was subjected to an array of analyses like bijectivity, nonlinearity, linear & differential cryptanalysis, differential style boomerang attack, avalanche effect, bit independence criterion, etc.

This study has employed the chess piece Rook (aka Castle) to impart the notion of nonlinearity in the suggested S-Box. The work [18] has already employed this chess piece for writing an image encryption algorithm. Moreover, 4D chaotic map [19] and DNA computing [20] were also employed in that study. In contrast, we have selected the 5D hyperchaotic map [21] to spawn the streams of random numbers. The chess piece Rook walks randomly over the entire chessboard depending upon the values of random numbers. This movement of the Rook has been iterated a large number to times to inject the feature of nonlinearity satisfactorily in the proposed S-Box.

A. CONTRIBUTIONS OF THE PROPOSED WORK

Apart from the other salient features of this work, this study contributes the following in an objective fashion to the business of network security.

- This work has unlocked the inherent potential of 5D multi-wing hyperchaotic system. This system enjoys the marvellous properties of randomness, ergodicity, mixing and unpredictability. Of course, these properties got "transferred" to the proposed S-Box.

- The random walk of chess piece Rook has performed a seminal role while designing a novel S-Box. Rook depending upon the random numbers manoeuvres over the entire hypothetical chessboard with the size of 16×16. The introduction of chess piece Rook contributed an added layer of security to the novel S-Box.
- The comprehensive security analyses of the novel S-Box rendered very promising results. Given these results, we contend that the proposed S-Box can be embedded in the varied network cryptographic products to heighten the security effects.

The rest of the study has been structured like this. Section II covers the needed related work of this study. Different researches have been discussed in this section. There are two preliminaries of this work, i.e., chaotic systems and chess piece Rook which have been discussed in the Section III. The Section IV describes in detail the way, the chaotic and random data has been generated. Apart from that, the way novel S-Box has been created, has been discussed in this section. Section V covers the security analyses of the proposed S-Box using various state of the art security parameters like bijectivity, non-linearity, strict-avalanche criterion, bit independence criterion, linear and differential probabilities. Lastly the discussion, conclusion and future work have been covered in the Sections VI, VII and VIII.

II. RELATED WORK

In the past, many S-Boxes have already been written by the cryptographers to enhance the network security of the different processes. The work [22], for example, developed an S-Box by using the capabilities of the 3D chaotic map. The security analysis of their work indicated that the proposed S-Box was furnished with nice security properties and has the potential to withstand the different security attacks. Apart from that, the newly devised S-Box has been used while writing a novel algorithm for the image encryption. In an other work [23], by intertwining the inherent capabilities of the chaotic system and the Latin square, an S-Box has been built. The algorithm developed by the authors works like this. First of all, a complete Latin square was generated by igniting the chaotic system. After that, an S-Box was developed by exploiting the complete Latin square. The security and performance analysis demonstrated that their newly devised S-Box was equipped with a nice performance and has the potential to frustrate the diverse security attacks like differential attack and linear attack. Moreover, their constructed S-Box was also applied while developing a novel image encryption scheme. The performance analysis further depicted that the developed algorithm has the ability to encrypt varied types of images and they rendered the histograms with the uniform bar. This uniformity of the bar, no doubt, acts as a great resistance to the potential threats of hackers. The research project [24] produced a yet another S-Box through the clever amalgamation of the constructs of particle swarm optimization, Hénon map, and quantum-inspired quantum walks. The security analysis of this new S-Box was carried out by taking different validation metrics. It proved its reliability and effectiveness while devising new ciphers. By using this S-Box, a novel image cipher was also developed. Various validation metrics rendered very nice results. For example, the information entropy came out to be 7.99977, Chi-square to be 249.481, NPCR 99.618% and UACI 33.484%.

Some works on the S-box were also carried out to optimize them. For example, the work [25] wrote a new variant of metaheuristic algorithm for substitution box construction and optimization through the implementation of naked mole rat (NMR) algorithm. This is also sometimes termed as Q-learning naked mole rat algorithm (QL-NMR). Moreover, QL-NMR amalgamated many chaotic maps like Sinusoidal, Singer, circle, logistic and Chebyshev. Apart from that, QL-NMR keeps track of the past performance of every choatic system during the construction of S-Box using a Q-learning table. The simulation results for the generation of 8×8 S-Box showed that their suggested QL-NMR technique outshined many other published works. In particular, it beat the other works in terms of strict avalanche criteria and nonlinearity. In the same way, the study [26] developed a new S-box algorithm by using the improved particle swarm optimization and the 4D hyperchaotic system. First of all, this work improved the Lorenz chaotic system and suggested a new chaotic map called as 4D chaotic system along with more complex dynamics and nicer Lyapunov exponent. Besides, the notion of simulated annealing was added in particle swarm optimization scheme. Additionally, a heightened particle swarm optimization scheme was employed for optimizing the idea of non-linearity of S-Box. This developed S-Box was imported while writing a new image cipher. The performance analyses vividly exhibited that the new S-Box was furnished with nice security properties of linear and differential probabilities, nonlinearity, SAC and BIC-NL.

Few works also employed the 5D hyperchaotic system to spawn the streams of random numbers and to exploit them while crafting new nonlinear cryptographic constructs like S - Box [27]. The reported work comprises of KY dimension, hyperchaotic phenomenon, complex phase attractors, unstable equilibrium point and conservativity. Apart from that, the newly developed S-Box was highly optimized in order to be defiant against the varied attacks. An other work [28] wrote an algorithm for constructing cryptographically robust S-Box using the complex dynamics of 5D chaotic map. The evaluation benchmarks included bit-independent criteria, a good avalanche effect, low differential uniformity and high nonlinearity. Besides, the developed S-Box was also investigated in varied applications where batch-generation of 8×8 boxes are possible. Apart from that, the examination revealed that by employing a novel method based solely on chaos, it was possible to generate an 8×8 S-box with a remarkable average high nonlinearity of up to 108.5 or S-boxes featuring differentials uniformity as low as 8. Additionally, it was feasible to obtain small-sized S-boxes characterized by both high nonlinearity and low differential

TABLE 1. A comparison of hyperchaotic/chaotic systems for creating S-Boxes.

S-Box Algorithm	Chaotic map chosen	Dimensions
Ref. [30]	Hyperchaotic	4D
Ref. [31]	fractional Rössler chaotic	3D
Ref. [32]	fractional Chen chaotic	3D
Ref. [33]	chaotic	3D
Ref. [28]	Hyperchaotic	5D
Ref. [34]	Hyperchaotic	5D
Proposed	Hyperchaotic	5D

uniformity. A comparative analysis of the proposed approach against recent S-box proposals demonstrated its superiority and effectiveness in constructing robust and bijective S-boxes. The study [29] constructed an S-Box by harnessing the power of 5-D chaotic map. The security analyses rendered very superior results like good cryptographic characteristics and high nonlinearity. Additionally, the newly developed S-Box was embedded in writing a novel image encryption scheme rendering very competitive results. Moreover, the Table 1 gives an overview of the different works using the kind of chaotic system being employed and the dimensions of the chaotic streams.

III. PRELIMINARIES

Preliminaries of this study include the chaotic system and the historic chess game. Particularly, the five dimensional chaotic system along with its attractors and Lyapunov exponents would be discussed. Moreover, the chess pieces and specially the Rook would be covered a little bit more so that we may understand the next sections easily.

A. THEORY OF CHAOS AND 5D MULTI-WING HYPERCHAOTIC SYSTEM

According to the marvellous theory of chaos, the slightest change in the primitive and initial conditions of a system causes a sea change in the output. Mathematicians harnessed this power of chaos and produced a large number of chaotic maps and systems. Many properties characterize these maps including aperiodicity, randomness, ergodicity, mixing and unpredictability [35], [36]. Different flavours of these maps exist like 1D, 2D, higher dimensions and the hyperchaotic maps. These maps have performed a great job in developing a number of S-boxes [37]. In this work, we have chosen the five dimensional chaotic map [21]. The mathematical form of this map is

$$\begin{aligned} \dot{v} &= -mv + wx \\ \dot{w} &= -nw + rz \\ \dot{x} &= -ox + sy + vw \\ \dot{y} &= py - tv \\ \dot{z} &= qz - v^2 w \end{aligned} \tag{1}$$

In this map, v, w, x, y, z are the initial values and the list m, n, o, p, q, r, s, t are the system parameters. The nonlinear terms included in the system are wx, vw and v^2w. The research work [38] explains the various properties like periodic orbit *etc* of this map. 0.001 step value has been taken to draw the different attractors of this chaotic system. In the same way, Figure 1 depicts the chaotic conduct of this map (1). Lastly, Lyapunov exponents of this system are $\{L_1, L_2, L_3, L_4, L_5 = 9.979, 1.96, 0.005362, -19.13, -27.82\}$ as shown in the Figure 2.

B. CHESS GAME AND ROOK

Chess is a popular game and is normally played between the intellectuals of the world [39]. Figure 3 shows the chess board and all its pieces/players. The numbers $\{1, 2, 3, 4, 5, 6, 7, 8\}$ serve as the labels of the various pieces in rows and columns. These labels form the addresses of the pieces. For instance, (1,1) and (8, 1) are the addresses of the white colored Rooks. There are a total of 32 pieces in this game owned equally for each player. The names of the pieces are Pawn, Knight, Bishop, Rook, Queen and King. These pieces move according to their own rules and regulations. Figure 3 shows the chessboard with its players and all the movements of the Rook. As the Figure 3c shows, Rook can move both horizontally and vertically.

IV. PROPOSED SCHEME FOR THE S-BOX

A. ALGORITHM FOR THE KEY STREAM GENERATION

In this section, we will explain the way, the key streams of random numbers have been created for the construction of S-Box. Spark the chaotic map (1) with the set of values: $v = 1, w = 1, x = 1, y = 1, z = 1, m = 10, n = 60, o = 20, p = 15, q = 40, r = 1, s = 50, t = 10$. Moreover, invoke the Algorithm 1 (*Key Streams*) for the generation of the key streams with the parameters' tuple $\{v, w, x, y, z, 1280000, 5000\}$. The *for* loop at line 1 is iterating for *iterations* times. Three streams $\{control_t\}_{t=1}^{iterations}$, $\{move1_t\}_{t=1}^{iterations}$ and $\{move2_t\}_{t=1}^{iterations}$ are being introduced at the lines 2, 3 and 4 respectively. Each of these three streams contains the integers in the range $[0, 1, \ldots., 255]$. The symbol $\lfloor . \rfloor$ denotes the floor function. The *for* loop of the line 6 is translating the ranges of these streams to $[1, 2]$, $[-15, -14, \ldots, 15]$ and $[-15, -14, \ldots, 15]$ respectively. The numbers $[1, 2]$ of the stream *control* corresponds to the horizontal and vertical movements of the Rook. Further, maximum movement of the Rook may be 15 or -15 in the positive and negative directions. Similarly, the lines 16 and 17 are populating the initial addresses of the Rook in the arrays *init*1 and *init*2 each in the range of $[1, 2, \ldots, 16]$.

B. PROPOSED ALGORITHM FOR CONSTRUCTION OF S-BOX

Invoke the Algorithm 2 ($S - Box\ Rounds$) with the parameters of $\{0, 1, 2, 3, \ldots, 255\}$, *control*, *move*1, *move*2, *init*1, *init*2 and ξ. This algorithm, in turn, calls the Algorithm 3 ($SBox - Maker$) for $\xi + 1$ times to construct the required

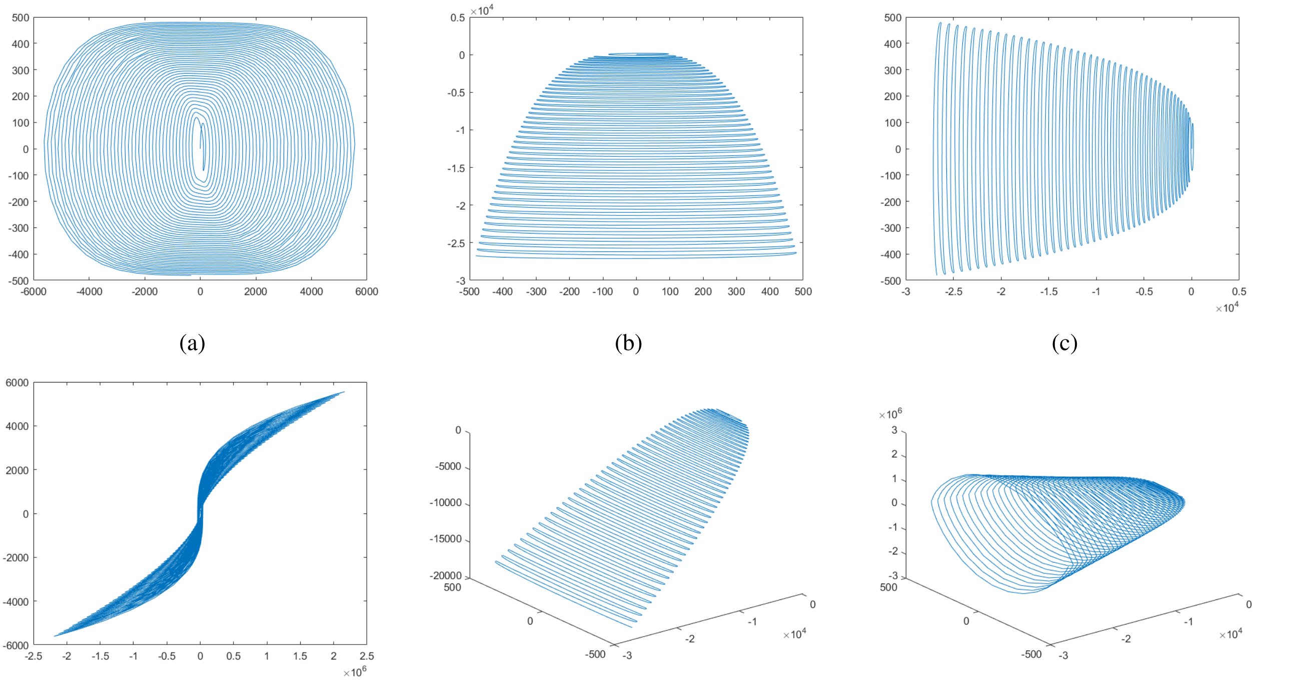

FIGURE 1. Different attractors of the System (1) in planes and space: (a) *vw* plane; (b) *wx* plane; (c) *xw* plane; (d) *zv* plane; (e) 3D view of *xwy* space; (f) 3D view of *xwz* space.

Algorithm 1 *Key Streams*

```
Input: v, w, x, y, z, iterations, ξ
Output: control, move1, move2, init1, init2
for i ← 1 to iterations do
    control(i) ← ⌊mod((v(i)) − ⌊abs(v(i))⌋ × 10^14, 256)⌋
    move1(i) ← ⌊mod(abs(w(i)) − ⌊abs(w(i))⌋ × 10^14, 256)⌋
    move2(i) ← ⌊mod(abs(x(i)) − ⌊abs(x(i))⌋ × 10^14, 256)⌋
end for
for i ← 1 to iterations do
    control(i) ← control(i) mod 2 + 1
    move1(i) ← move1(i) mod 31 − 15
    move2(i) ← move2(i) mod 31 − 15
end for
for i ← 1 to ξ do
    init1(i) ← ⌊mod(abs(y(i)) − ⌊abs(y(i))⌋ × 10^14, 256)⌋
    init2(i) ← ⌊mod(abs(z(i)) − ⌊abs(z(i))⌋ × 10^14, 256)⌋
end for
for i ← 1 to ξ do
    init1(i) ← init1(i) mod 16 + 1
    init2(i) ← init2(i) mod 16 + 1
end for
```

S-Box. In each iteration for $k = 0$ to ξ, this algorithm is called with the following parameters *sbox*, $control(256k+1 : 256k+256)$, $move1(256k+1 : 256k+256)$, $move2(256k+1 : 256k+256)$, $init1(k)$, $init2(k)$, where $a : b$ in $control(a : b)$ refers to the notion of slicing. Here, we will explain the Algorithm 3 in a step by step fashion (Kindly see the Figure 4 for its visual version).

Step 1: Line 1 initializes the 2D array $sbox'$ (size of 16×16) with the value of -1.

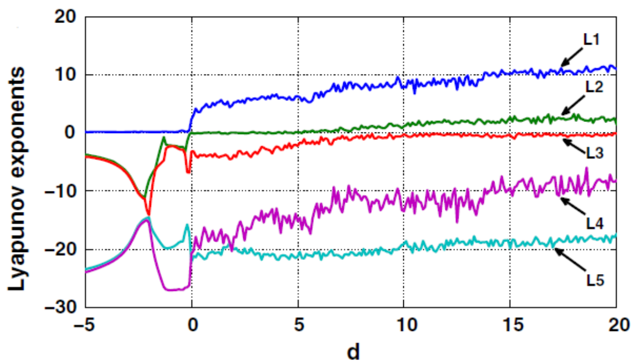

FIGURE 2. System (1)'s Lyapunov exponents.

Step 2: Lines 2 and 3 initialize the variables p and q with $i1$ and $i2$ respectively. These serve as the initial positions of the chess piece Rook on the chessboard.

Step 3: The *for* loop at the line 4 extends its reach till the line 43. In each iteration of this loop, the index $control(loop)$ of the switch-case structure decides whether the Rook will move in the horizontal or vertical direction. If *case* 1 matches, then the *if* condition at the line 7 checks whether the random number in the variable $move1(loop)$ is positive? If it is, then line 8 further checks whether $p - move1(loop) \geq 1$? If it becomes true, then the value of p is being updated at the line 9, otherwise, it is being updated at the line 11.

Step 4: The *else if* control structure (Line 13) further copes with the situation where $move1(loop)$ renders a negative value.

Step 5: In case, the value of $move1(loop)$ is zero, the *continue* statement on the line 20 is being executed

(a) (b) (c)

FIGURE 3. **Chessboard and rook: (a) Chessboard; (b) Rook; (c) Rook with its moves.**

Algorithm 2 *S − Box Rounds*

Input: *sbox, control, move*1*, move*2*, init*1*, init*2*, ξ*
Output: *sbox′*

for $k \leftarrow 0$ to ξ **do**
  $sbox' \leftarrow SBox-Maker(sbox, control(256k+1:256k+256), move1(256k+1:256k+256), move2(256k+1:256k+256), init1(k), init2(k))$
end for

to shift the control at the start of the *for* loop on the line 4.

Step 6: In the same way, the *case* 2 spanning the lines 20 to 37 handles the vertical movement of the chess piece Rook.

Step 7: The *if* condition at the line 39 checks whether $sbox'(p, q) = -1$. If it is, then the value of $sbox(loop)$ is being assigned to the position $sbox'(p, q)$. Moreover, a track that value of *sbox* at index *loop* has been shifted to its required position is being kept at the line 41.

Step 8: Lastly, the Algorithm 4 (*Complete−SBox*) is being called at the line 44 with the parameters *sbox* and *sbox′*. This algorithm is meant to fill the vacant positions of the required S-Box. Actually, sometimes, Rook happens to land on the address of the board which has already been filled. In those cases, no shifting becomes possible at the line 40 of the Algorithm 3.

The output of the Algorithm 3 is the required generated S-Box which can be seen in the Table 2.

V. SIMULATION, RESULTS AND DISCUSSION

Just the development of cryptographic products is not sufficient, rather, they must be subjected to the state of the art criteria, yardsticks and other benchmarks agreed upon among the cryptographers, security experts and analysts. In this section, we will demonstrate the robustness and defiance of the proposed S-Box using these benchmarks. They include bijectivity, nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), linear probability (LP), and differential probability (DP) [40].

A. BIJECTIVITY

Generally speaking, an $n \times n$ S-Box is bijective if it contains 2^{n-1} distinct integers [24]. Further, all these integers fall within the range of $[0, 2^{n-1}]$. The Table 2 clearly fulfills the property of bijectivity.

B. NON-LINEARITY

Linear cryptanalysis attacks are occasionally launched on the security products by the potential hackers [41]. To counter this threat, a substantial amount of non-linearity in the developed S-Boxes must be embedded. In case, if there exists a linear mapping between the ciphertext and plaintext, then the employed S-Box can be attacked by the adversaries and other opponents. In order to evaluate the inherent non-linearity of some n-bit Boolean function say $b(k)$, the following mathematical equation (2) can be employed [42].

$$NL(b) = \frac{1}{2}\{2^n - max_{h\in\{0,1\}^n}|WS_b(h)|\} \tag{2}$$

In this equation, $WS_b(h)$ refers to the Walsh spectrum of some given function b. Moreover, the following mathematical equation helps in calculating the non-linearity of n-bit Boolean function $b(k)$.

$$WS_{b(h)} = \sum_{x\in\{0,1\}^n} (-1)^{b(x)\oplus h.x} \tag{3}$$

In this equation, $h \in \{0, 1\}^n$. Moreover, $h.x$ refers to dot product of h and x. This dot product can be computed through

$$h.x = (h_1 \oplus x_1) + \ldots + (h_n \oplus x_n) \tag{4}$$

The list of non-linearity values for the proposed S-Box are: 103, 102, 106, 110, 107, 108, 108, and 105. Besides, 102, 110, 106.125 are the minimum, maximum and the average values. Moreover, Table 3 presents the non-linearity values for all eight constituent Boolean functions.

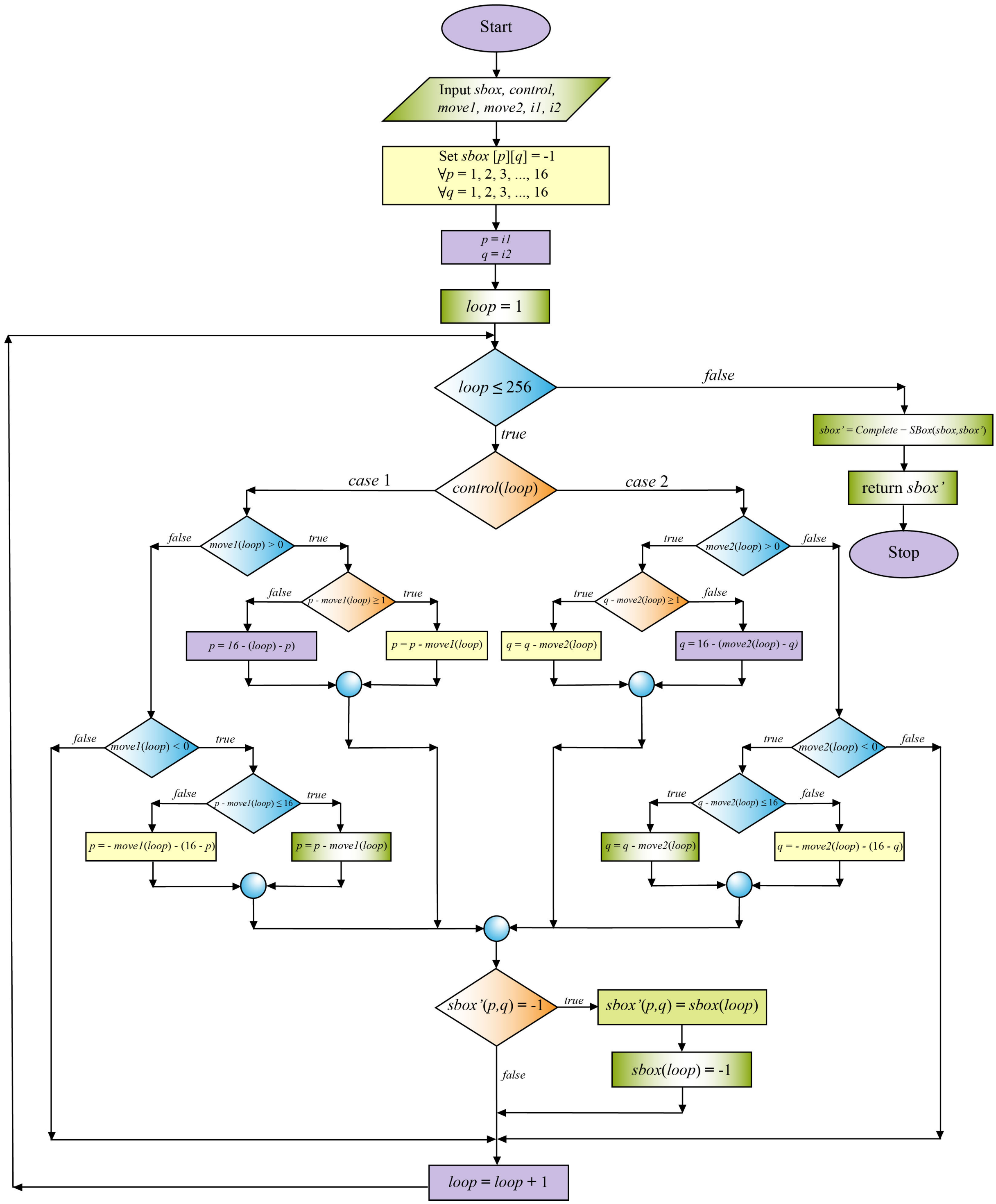

FIGURE 4. Flowchart of *SBox - Maker*.

C. STRICT-AVALANCHE CRITERION (SAC)

To satisfy the strict avalanche criterion, when a single input bit n is modified, there should be a 50% probability that the resulting output bit m will change [42]. To put this in other words, if its SAC value is nearly equal to 0.5, the S-Box in question is furnished with the sufficient amount of randomness and chaoticity. Moreover, the Table 4 depicts computed values of suggested S-Box. This matrix is also termed as dependence matrix. Furthermore, the average SAC value for the proposed S-Box is 0.5077, meeting the established criterion.

D. BIT-INDEPENDENCE CRITERION (BIC)

This is an other benchmark used by the cryptographers to check the robustness of their product. According to this benchmark, if a change in some input bit say q results in

Algorithm 3 *SBox − Maker*

```
Input: sbox, control, move1, move2, i1, i2
Output: sbox'
Set sbox'[p][q] ← −1
  ∀p ← 1, 2, 3, ..., 16
  ∀q ← 1, 2, 3, ..., 16
p ← i1
q ← i2
for loop ← 1 to 256 do
  switch (control(loop))
  case 1:
    if move1(loop) is positive then
      if p − move1(loop) ≥ 1 then
        p ← p − move1(loop)
      else
        p ← 16 − (move1(loop) − p)
      end if
    else if move1(loop) is negative then
      if p − move1(loop) ≤ 16 then
        p ← p − move1(loop)
      else
        p ← −move1(loop) − (16 − p)
      end if
    else
      continue
    end if
  case 2:
    if move2(loop) is positive then
      if q − move2(loop) ≥ 1 then
        q ← q − move2(loop)
      else
        q ← 16 − (move2(loop) − q)
      end if
    else if move2(loop) is negative then
      if q − move2(loop) ≤ 16 then
        q ← q − move2(loop)
      else
        q ← −move2(loop) − (16 − q)
      end if
    else
      continue
    end if
  end switch
  if sbox'(p, q) = −1 then
    sbox'(p, q) ← sbox(loop)
    sbox(loop) ← −1
  end if
end for
sbox' ← Complete − SBox(sbox, sbox')
```

the change of output bits r and s separately, then S-Box is dubbed as a successful in separating the output bits with each other [42]. For satisfying this property, S-Box's constituent Boolean functions should comply with the nonlinearity conditionality. The calculation of the expression $(T_a[p] \oplus T_b[q]) - (T_a[p] \oplus T_b[p])$ is performed over the entire range

Algorithm 4 *Complete − SBox*

```
Input: sbox, sbox'
Output: sbox'
loopIndex ← 0
for p ← 1 to 16 do
  for q ← 1 to 16 do
    if sbox'(p, q) = −1 then
      while sbox(loopIndex + 1) = −1 do
        loopIndex ← loopIndex + 1
      end while
      sbox'(p, q) ← sbox(loopIndex + 1)
      loopIndex ← loopIndex + 1
    end if
  end for
end for
```

of input values for p spanning from 0 to 255. Here T is the S-Box. This computation is used to assess the BIC-SAC performance of an S-Box. It's worth noting that in this evaluation, q and p differ by only one bit. Furthermore, the effectiveness of an S-Box is determined by the average BIC-SAC values computed across all input values, with an optimal performance indicated by values near 0.5. Tables 5 and 6 illustrate the criteria used to evaluate the non-linearity and SAC for the constituent Boolean functions within the proposed S-Box. Moreover, the mean non-linearity and SAC values corresponding to the proposed S-Box, are 103.17 and 0.5061, respectively in these tables. In accordance with the research conducted by Carlisle and Stafford [43], an S-box that satisfies the non-linearity and SAC criteria is considered to fulfill the BIC property. For the proposed S-box, the values 103.17 and 0.5061 indicate a notably weak linear relationship among the output bits. These statistics unequivocally validate the BIC property for the proposed S-box.

E. LINEAR-PROBABILITY (LP)

The inherent correlation between the input and output of an S-Box is also checked through the notion of linear probability [44]. Lower value of LP is desirable for the robust S-Box. The equation (5) yields a maximum LP value of 0.1328 for the proposed S-Box. This indicates that the S-Box possesses sufficient strength to resist linear cryptanalytic attacks.

$$LP = max_{a_z, b_z \neq 0} \left| \frac{\#\{z \in N | z.a_z = T(z).b_z\}}{2^n} - \frac{1}{2} \right| \quad (5)$$

In this equation, T, a_z and b_z represent the S-Box, input and output masks, respectively. Additionally, the variable N encompasses a set of integers spanning from 0 to 255.

F. DIFFERENTIAL-PROBABILITY (DP)

In this cryptanalysis, original plaintext is tried to recover from the given ciphertext by inspecting the differences between the pairs of ciphertexts and the corresponding plaintexts [45]. By inspecting these differences, the potential hackers can

TABLE 2. S-box generated using the proposed algorithm.

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

TABLE 3. Results of non-linearities for suggested S-box.

Boolean functions	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
Calculated non-linearity	103	102	106	110	107	108	108	105

TABLE 4. Results of SAC for proposed S-Box.

i/j	1	2	3	4	5	6	7	8
1	0.5643	0.5076	0.5289	0.5178	0.4890	0.4934	0.4790	0.5084
2	0.4865	0.5127	0.4694	0.49657	0.4865	0.4860	0.4890	0.5673
3	0.5409	0.5278	0.5390	0.5217	0.5388	0.4987	0.5198	0.5001
4	0.5123	0.5271	0.4943	0.5127	0.4698	0.4808	0.5098	0.5128
5	0.5321	0.4590	0.4905	0.5037	0.5121	0.5238	0.4878	0.5210
6	0.5234	0.4773	0.4865	0.5237	0.5123	0.5234	0.5123	0.5190
7	0.5123	0.4627	0.4976	0.5237	0.5128	0.4968	0.5238	0.5278
8	0.5180	0.4967	0.5004	0.4897	0.5208	0.5178	0.4980	0.5034

TABLE 5. Suggested S-Box's BIC non-linearity results.

i/j	1	2	3	4	5	6	7	8
1	-	106	102	100	102	101	108	104
2	106	-	102	104	102	99	103	104
3	102	102	-	106	104	103	104	106
4	100	104	106	-	108	100	105	102
5	102	102	104	108	-	104	100	101
6	98	102	104	100	104	-	104	104
7	108	105	103	102	100	105	-	100
8	102	104	106	102	105	104	100	-

TABLE 6. BIC-SAC results of suggested S-Box.

i/j	1	2	3	4	5	6	7	8
1	-	0.4766	0.5317	0.4987	0.5190	0.5098	0.5134	0.4930
2	0.5189	-	0.4987	0.5123	0.5098	0.4980	0.4954	0.5123
3	0.5098	0.5123	-	0.4787	0.4980	0.5143	0.5321	0.5023
4	0.5123	0.4734	0.5223	-	0.5172	0.5076	0.4987	0.5087
5	0.5043	0.4912	0.5189	0.4890	-	0.5209	0.4987	0.5176
6	0.5012	0.5189	0.4987	0.5212	0.5145	-	0.4735	0.5289
7	0.5243	0.5165	0.4865	0.5012	0.5089	0.5119	-	0.4854
8	0.5087	0.5124	0.4954	0.5032	0.5012	0.4974	0.5187	-

have an access over the secret key. For the robust S-Box, this metric should have the relatively lower value. The differential probability is found through the usage of equation (6).

The information in Table 7 illustrates that proposed S-box demonstrates the result of differential probability which is $12/256 = 0.0469$. This result signals towards robust resistance to varied attacks of differential cryptanalysis. The following equation (6) defines the calculation of the differential probability (DP):

TABLE 7. Suggested S-box DP table.

i/j	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	6	6	6	8	6	6	6	6	8	6	6	6	8	6	6	6
1	6	8	6	6	8	6	6	6	6	6	6	8	6	6	6	6
2	6	8	6	6	6	8	6	6	6	6	6	8	6	6	8	6
3	6	6	8	6	6	6	6	6	8	6	6	6	8	6	6	6
4	6	6	8	6	6	6	6	6	6	6	6	6	8	6	6	6
5	8	6	6	6	6	6	6	8	6	6	6	6	6	6	6	6
6	6	6	6	6	6	8	6	6	6	6	6	6	6	6	6	6
7	6	6	6	8	6	6	6	6	6	6	8	6	6	6	6	6
8	6	6	8	6	6	6	6	6	6	6	6	6	6	6	6	6
9	8	6	6	6	8	6	6	6	6	8	8	6	6	8	6	8
A	6	8	10	6	6	6	8	8	8	8	6	10	8	12	6	8
B	6	8	6	6	6	6	8	6	8	6	8	6	8	6	8	6
C	4	6	6	6	6	8	6	6	6	6	8	6	8	6	8	8
D	8	6	6	6	6	8	6	6	6	6	6	6	8	6	8	6
E	6	6	6	6	6	8	6	8	6	8	6	6	6	6	6	8
F	8	6	6	6	8	6	6	6	6	6	8	6	6	6	6	-

$$DP = max_{\triangle z \neq 0, \triangle y} \left| \frac{\#\{z \in N | T_{(z)} \oplus T_{(z \oplus \triangle z)} = \triangle y\}}{2^n} \right| \quad (6)$$

In this equation, $\triangle z$ and $\triangle y$ represent the respective input and output differentials.

VI. DISCUSSION

The development of a novel S-Box algorithm based on the 5D multi-wing hyperchaotic system and the chess piece Rook given in this study has yielded significant insights and contributions to the field of network security. Our primary focus while writing this new S-Box was to enhance the security of data transmission across the different networks. Apart from that, the resilience of the proposed algorithm to the various threats like differential and linear cryptanalysis is a testament to its intrinsic robust cryptographic design. The proposed algorithm underwent rigorous testing, evaluating its performance against state-of-the-art security parameters such as bijectivity, non-linearity, strict avalanche criterion, bit independence criterion, linear probability, and differential probability. Table 8 presents a comparison between the results achieved by the suggested algorithm and those reported in other published works.

Proposed algorithm's computational efficiency and low latency make it well-suited for the varied practical network

TABLE 8. A comparison of the performance of several S-boxes including the proposed one.

Study	Algorithm	NL	BIC-NL	SAC	BIC-SAC	LP	DP
Ref. [24]	Based on quantum-inspired QW and the customized PSO	107.00	103.0	0.5044	0.5066	0.1172	0.0313
Ref. [46]	Mackey–Glass equation	104.00	102.9	0.5000	0.4980	0.1328	0.0391
Ref. [23]	Enhanced logistic map and Latin square	105.25	103.2	0.5351	0.5000	–	0.0391
Ref. [47]	Jaya optimization algorithm	106.25	103.64	0.5009	0.4996	0.1171	0.0391
Ref. [22]	3D chaotic map	106.00	104.2	0.4993	0.5030	0.1250	0.0391
Ref. [48]	Gingerbreadman chaotic system	102.00	102.9	0.5178	0.4999	0.1250	0.0313
Ref. [49]	logistic-sine map	105.25	103.8	0.4956	0.4996	0.1562	0.0391
Ref. [50]	quantum-inspired QW	106.00	103.9	0.4958	0.5023	0.1250	0.0313
Ref. [51]	Teaching-learning-based optimization	106.50	104.6	0.4995	0.4983	0.1172	0.0391
Proposed	Rook and 5D chaotic system	106.125	103.17	0.5077	0.5061	0.1328	0.0469

security applications. In an era where real-time data exchange is one of the most demanding feature, the algorithm's ability to complete its task without introducing significant processing overhead is, no doubt, a valuable asset. Apart from that, this endeavor has not only addressed the theoretical requirements but it also focused on the practical integration of the S-Box into existing network security protocols.

VII. CONCLUSION

The significance of network security in the interconnected world of ours is self evident. Further, as the cyber threats and other data breaches are becoming increasingly sophisticated, there is a pressing need to contain these threats and to come up with innovative cryptographic solutions. The present research endeavor has written and evaluated a novel S-Box algorithm aimed at enhancing the network security. Two constructs of Rook —a chess piece and 5D multi-wing hyperchaotic system have been employed while crafting this new S-Box. Rook walks over the large chessboard. As it walks over the various boxes of the chess, the data of S-Box gets scrambled. This process has been iterated for a number of times to satisfactorily create the S-Box. Moreover, the suggested S-Box algorithm has demonstrated its efficacy in many key facets of network security. For instance, it vividly enhanced the confidentiality of data as the metrics of non-linearity and strong avalanche effect show. A thorough analysis and evaluation given in this study attest to the proposed algorithm's robustness in the face of varied cyber threats. Concluding, this study has yielded a promising solution to the exciting field of network security. No doubt, the suggested S-Box algorithm with its intrinsic cryptographic properties renders a notable addition to the arsenal of different constructs available to the network security practitioners.

VIII. FUTURE WORK

The present work has written a novel S-Box algorithm to bolster network security. Potentially, there are many promising avenues for further exploration and refinement of the current work. For instance, 1)*Performance Optimization*: As the network settings continue to evolve in different directions, the need for efficient ciphers becomes of primary importance. Future work may focus for the optimization of the computational performance of suggested S-Box algorithm without striking any sort of compromise of the requisite security. This may be investigating hardware acceleration algorithms or parallel computing algorithms for enhancing the encryption speed. 2) *Resilience to Quantum Attacks*: As the quantum computing is emerging on the landscape, classical cryptographic techniques face new threats. Probing the algorithm's defiance to the quantum attacks and exploring the quantum-resistant cryptographic techniques may be an other notable research direction. 3) *Integration with Existing Cryptosystems*: Network security occasionally depends upon the interoperability of heterogeneous cryptographic components. Future research may investigate the prospects of integration of the novel S-Box algorithm into existing cryptographic systems, like VPN solutions or TLS/SSL protocols or to appraise its real-world applicability and compatibility.

REFERENCES

[1] M. S. Akter, "Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions," 2023, *arXiv:2306.09248*.

[2] G. N. M. Chowdary, M. P. S. R. Lakshmi, Y. Nylu, B. Deepthi, K. Prasad, and S. K. Kannaiah, "Elliptic curve cryptography for network security," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, Apr. 2023, pp. 1500–1503.

[3] C. Prabha, N. Sharma, J. Singh, A. Sharma, and A. Mittal, "A review of cyber security in cryptography: Services, attacks, and key approach," in *Proc. 3rd Int. Conf. Artif. Intell. Smart Energy (ICAIS)*, Feb. 2023, pp. 1300–1306.

[4] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman, R. Alroobaea, and W. J. Buchanan, "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, 2020.

[5] I. Ashraf, Y. Park, S. Hur, S. W. Kim, R. Alroobaea, Y. B. Zikria, and S. Nosheen, "A survey on cyber security threats in IoT-enabled maritime industry," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2677–2690, Feb. 2023.

[6] L. E. Sunny, V. Paul, and U. Narayanan, "A novel and dynamic S-box for improving the security of audio and video for various crypto— Applications," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 7, pp. 545–560, 2023.

[7] A. K. Yadav, A. Braeken, and M. Misra, "Symmetric key-based authentication and key agreement scheme resistant against semi-trusted third party for fog and dew computing," *J. Supercomput.*, vol. 79, no. 10, pp. 11261–11299, Jul. 2023.

[8] R. Mishra, S. Dutta, M. Okade, and K. Mahapatra, "Substitution permutation network based lightweight ciphers with improved substitution layers for secure IoT applications," in *Proc. 2nd Int. Conf. Range Technol. (ICORT)*, Aug. 2021, pp. 1–6.

[9] M. Gupta and A. Sinha, "Enhanced-AES encryption mechanism with S-box splitting for wireless sensor networks," *Int. J. Inf. Technol.*, vol. 13, no. 3, pp. 933–941, Jun. 2021.

[10] F. Artuğer, "A new S-box generator algorithm based on 3D chaotic maps and whale optimization algorithm," *Wireless Pers. Commun.*, vol. 131, no. 2, pp. 835–853, Jul. 2023.

[11] L. Yan, L. Li, and Y. Guo, "DBST: A lightweight block cipher based on dynamic S-box," *Frontiers Comput. Sci.*, vol. 17, no. 3, Jun. 2023, Art. no. 173805.

[12] S. Fahd, M. Afzal, D. Shah, W. Iqbal, and A. Hai, "Robustness of affine and extended affine equivalent surjective S-box(es) against differential cryptanalysis," in *Proc. Int. Symp. Found. Pract. Secur.* Cham, Switzerland: Springer, 2022, pp. 461–471.

[13] G. Manjula and H. S. Mohan, "Improved dynamic S-box generation using hash function for AES and its performance analysis," in *Proc. 2nd Int. Conf. Green Comput. Internet Things (ICGCIoT)*, Aug. 2018, pp. 109–115.

[14] C. A. Murugan, P. Karthigaikumar, and S. S. Priya, "FPGA implementation of hardware architecture with AES encryptor using sub-pipelined S-box techniques for compact applications," *Automatika*, vol. 61, no. 4, pp. 682–693, Oct. 2020.

[15] M. Wang, H. Liu, and M. Zhao, "Bit-level image encryption algorithm based on random-time S-box substitution," *Eur. Phys. J. Special Topics*, vol. 231, nos. 16–17, pp. 3225–3237, Nov. 2022.

[16] M. F. Khan, K. Saleem, T. Shah, M. M. Hazzazi, I. Bahkali, and P. K. Shukla, "Block cipher's substitution box generation based on natural randomness in underwater acoustics and knight's tour chain," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–17, May 2022.

[17] V. A. Thakor, M. A. Razzaque, A. D. Darji, and A. R. Patel, "A novel 5-bit S-box design for lightweight cryptography algorithms," *J. Inf. Secur. Appl.*, vol. 73, Mar. 2023, Art. no. 103444.

[18] N. Iqbal, R. A. Naqvi, M. Atif, M. A. Khan, M. Hanif, S. Abbas, and D. Hussain, "On the image encryption algorithm based on the chaotic system, DNA encoding, and castle," *IEEE Access*, vol. 9, pp. 118253–118270, 2021.

[19] Y. Chen and Y.-Q. Yang, "A new four-dimensional chaotic system," *Chin. Phys. B*, vol. 19, no. 12, Dec. 2010, Art. no. 120510, doi: 10.1088/1674-1056/19/12/120510.

[20] S. Mansoor and S. A. Parah, "HAIE: A hybrid adaptive image encryption algorithm using chaos and DNA computing," *Multimedia Tools Appl.*, vol. 82, no. 19, pp. 28769–28796, Aug. 2023.

[21] Z. Bashir, N. Iqbal, and M. Hanif, "A novel gray scale image encryption scheme based on pixels' swapping operations," *Multimedia Tools Appl.*, vol. 80, no. 1, pp. 1029–1054, Jan. 2021.

[22] A. A. A. El-Latif, B. Abd-El-Atty, A. Belazi, and A. M. Iliyasu, "Efficient chaos-based substitution-box and its application to image encryption," *Electronics*, vol. 10, no. 12, p. 1392, Jun. 2021.

[23] Z. Hua, J. Li, Y. Chen, and S. Yi, "Design and application of an S-box using complete Latin square," *Nonlinear Dyn.*, vol. 104, no. 1, pp. 807–825, Mar. 2021.

[24] B. Abd-El-Atty, "Efficient S-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem," *Complex Intell. Syst.*, vol. 9, no. 5, pp. 4817–4835, Oct. 2023.

[25] K. Z. Zamli, F. Din, and H. S. Alhadawi, "Exploring a Q-learning-based chaotic naked mole rat algorithm for S-box construction and optimization," *Neural Comput. Appl.*, vol. 35, no. 14, pp. 10449–10471, May 2023.

[26] S. Yang, X. Tong, Z. Wang, and M. Zhang, "S-box generation algorithm based on hyperchaotic system and its application in image encryption," *Multimedia Tools Appl.*, vol. 82, no. 17, pp. 25559–25583, Jul. 2023.

[27] A. Alhudhaif, M. Ahmad, A. Alkhayyat, N. Tsafack, A. K. Farhan, and R. Ahmed, "Block cipher nonlinear confusion components based on new 5-D hyperchaotic system," *IEEE Access*, vol. 9, pp. 87686–87696, 2021.

[28] 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.

[29] B. Abd-El-Atty, A. Belazi, and A. A. Abd El-Latif, "A novel approach for robust S-box construction using a 5-D chaotic map and its application to image cryptosystem," in *Cybersecurity: A New Approach Using Chaotic Systems*. Berlin, Germany: Springer, 2022, pp. 1–17.

[30] F. U. Islam and G. Liu, "Designing S-box based on 4D-4wing hyperchaotic system," *3D Res.*, vol. 8, no. 1, pp. 1–9, Mar. 2017.

[31] M. Khan and T. Shah, "An efficient construction of substitution box with fractional chaotic system," *Signal, Image Video Process.*, vol. 9, no. 6, pp. 1335–1338, Sep. 2015.

[32] F. Özkaynak, V. Çelik, and A. B. Özer, "A new S-box construction method based on the fractional-order chaotic Chen system," *Signal, Image Video Process.*, vol. 11, no. 4, pp. 659–664, May 2017.

[33] 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, Jan. 2017.

[34] Q. Lu, C. Zhu, and G. Wang, "A novel S-box design algorithm based on a new compound chaotic system," *Entropy*, vol. 21, no. 10, p. 1004, Oct. 2019.

[35] N. Iqbal, S. Abbas, M. A. Khan, T. Alyas, A. Fatima, and A. Ahmad, "An RGB image cipher using chaotic systems, 15-puzzle problem and DNA computing," *IEEE Access*, vol. 7, pp. 174051–174071, 2019.

[36] H. Ning, G. Zhao, Y. Dong, Y. Ma, and J. Jia, "Spatiotemporal chaos in two-dimensional dynamic coupled map lattices system based on elementary cellular automata," *Nonlinear Dyn.*, vol. 109, no. 3, pp. 2143–2161, Aug. 2022.

[37] H. Liu, J. Liu, and C. Ma, "Constructing dynamic strong S-box using 3D chaotic map and application to image encryption," *Multimedia Tools Appl.*, vol. 82, no. 16, pp. 23899–23914, Jul. 2023.

[38] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017.

[39] C. S. Yusof, T. S. Low, A. W. Ismail, and M. S. Sunar, "Collaborative augmented reality for chess game in handheld devices," in *Proc. IEEE Conf. Graph. Media (GAME)*, Nov. 2019, pp. 32–37.

[40] L. Liu, Y. Zhang, and X. Wang, "A novel method for constructing the S-box based on spatiotemporal chaotic dynamics," *Appl. Sci.*, vol. 8, no. 12, p. 2650, Dec. 2018.

[41] H. Zhu, X. Tong, Z. Wang, and J. Ma, "A novel method of dynamic S-box design based on combined chaotic map and fitness function," *Multimedia Tools Appl.*, vol. 79, nos. 17–18, pp. 12329–12347, May 2020.

[42] A. W. Malik, A. H. Zahid, D. S. Bhatti, H. J. Kim, and K.-I. Kim, "Designing S-box using tent-sine chaotic system while combining the traits of tent and sine map," *IEEE Access*, vol. 11, pp. 79265–79274, 2023.

[43] A. Sevin and A. A. O. Mohammed, "A survey on software implementation of lightweight block ciphers for IoT devices," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 3, pp. 1801–1815, Mar. 2023.

[44] A. Waheed, F. Subhan, M. M. Suud, M. Alam, and S. Ahmad, "An analytical review of current S-box design methodologies, performance evaluation criteria, and major challenges," *Multimedia Tools Appl.*, vol. 82, no. 19, pp. 29689–29712, Aug. 2023.

[45] A. Ali, M. A. Khan, R. K. Ayyasamy, and M. Wasif, "A novel systematic byte substitution method to design strong bijective substitution box (S-box) using piece-wise-linear chaotic map," *PeerJ Comput. Sci.*, vol. 8, p. e940, May 2022.

[46] N. A. Khan, M. Altaf, and F. A. Khan, "Selective encryption of JPEG images with chaotic based novel S-box," *Multimedia Tools Appl.*, vol. 80, no. 6, pp. 9639–9656, Mar. 2021.

[47] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dyn.*, vol. 99, no. 4, pp. 3041–3064, Mar. 2020.

[48] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and S_8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018.

[49] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, Jan. 2017.

[50] A. A. Abd El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Sci. Rep.*, vol. 10, no. 1, p. 1930, Feb. 2020.

[51] T. Farah, R. Rhouma, and S. Belghith, "A novel method for designing S-box based on chaotic map and teaching-learning-based optimization," *Nonlinear Dyn.*, vol. 88, no. 2, pp. 1059–1074, Apr. 2017.

JARALLAH ALQAHTANI received the M.S. degree from the Illinois Institute of Technology and the Ph.D. degree from Oregon State University, USA. Since 2022, he has been an Assistant Professor with the College of Computer Science and Information Systems, Najran University, Saudi Arabia. He specializes in data center networks, vehicular ad-hoc networks, cloud computing, machine learning, and artificial intelligence.

MUHAMMAD AKRAM received the M.Sc. degree in computer science from The University of Azad Jammu & Kashmir and the M.S. degree in computer science from the Blekinge Institute of Technology, Sweden. Currently, he is pursuing the Ph.D. degree in ICT with Universiti Tenaga Nasional, Malaysia. He is also a Coordinator of Development and Quality Unit with the College of Computer Science and Information Systems (CCSIS), Najran University, Saudi Arabia. He is also a Lecturer with CCSIS. He has more than 25 research publications in various national/international research journals and conferences. He is the author of two books. His research interests include human–computer interaction, web accessibility, usability, and computer networks.

GHASSAN AHMED ALI received the master's degree in cybersecurity and the Ph.D. degree in digital forensics. He is currently an Associate Professor with the Faculty of Islamic Technology, Universiti Islam Sultan Sharif Ali, Brunei. He has professional academic experience in several universities in Malaysia, Saudi Arabia, and Brunei Darussalam, and he has been teaching various courses in the domain of cybersecurity, digital forensics, ICT, and information systems. He is supervising the master's and Ph.D. students. His research interests include cyber security, digital forensics, quality and assurance systems, ICT, and information systems.

NADEEM IQBAL received the Master of Science (M.S.) degree from the prestigious National University of Sciences and Technology (NUST), Islamabad, Pakistan, specializing in theorem proving, and the Ph.D. degree from the National College of Business Administration and Economics (NCBA&E). He is currently an Assistant Professor with the Department of Computer Science and IT, The University of Lahore (UOL), Lahore, Pakistan. He is an accomplished Researcher in the field of cyber security, with a strong foundation in computational science and engineering. His primary research focus has been in the domain of cryptography, where he has made significant contributions to enhancing the security of digital systems and data protection. His research extends to various facets of cyber security, including encryption algorithms, data science, and the philosophical aspects of mathematics. His academic excellence is underscored by his outstanding GRE scores, with a perfect quantitative score of 800/800, showcasing his exceptional analytical and problem-solving skills. His passion for knowledge and continuous learning is evident through his attainment of the IBM professional certification in data science. With a rich academic background, a keen interest in algorithms, data science, and the philosophy of mathematics, he stands as a dedicated Researcher and a Scholar in the field of cyber security, making valuable contributions to the ever-evolving landscape of digital security.

ALI ALQAHTANI received the Ph.D. degree in computer engineering and networking from Oakland University, Rochester Hills, MI, USA, in 2020. He is currently an Assistant Professor with Najran University (NU). His research interests include the use of machine learning in general and deep learning in particular in image and signal processing, wireless vehicular networks (VANETs), wireless sensor networks, and cyber-physical systems.

ROOBAEA ALROOBAEA received the bachelor's degree (Hons.) in computer science from King Abdulaziz University (KAU), Saudi Arabia, in 2008, and the master's degree in information system and the Ph.D. degree in computer science from the University of East Anglia, U.K., in 2012 and 2016, respectively. He is currently an Associate Professor with the College of Computers and Information Technology, Taif University, Saudi Arabia. His research interests include human–computer interaction, software engendering, cloud computing, the Internet of Thing, artificial intelligent, and machine learning.