Multimedia Tools and Applications (2023) 82:29689–29712
https://doi.org/10.1007/s11042-023-14910-3

An analytical review of current S-box design methodologies, performance evaluation criteria, and major challenges

Adil Waheed[1,2] · Fazli Subhan[1,3] · Mazliham Mohd Suud[3] · Mansoor Alam[3] · Sohaib Ahmad[4]

Received: 6 September 2022 / Revised: 22 December 2022 / Accepted: 12 February 2023 /
Published online: 4 March 2023

Abstract
The expansion of worldwide networking has created new possibilities for management, development, and presentation in the form of digital data. The uncomplicated accessibility to digital resources i.e., internet banking, electronic advertising, digital marketing, and libraries has resulted in grave security concerns. Consequently, rapid use of digital information and technology, security of digital transactions is a big concern. Although many data security solutions exist, still they need further improvement. In symmetric cryptography, the strength of a Substitution Box (S-box) assures the strength of block ciphers. S-box is a critical nonlinear element of cryptosystem that creates turmoil in transactions. This study aims to formulate a variety of methodologies to measure the effectiveness of an S-box against linear and differential algebraic attacks. These malicious attacks may disrupt and leak confidential information. Therefore, a comparative analysis is presented to understand the S-box construction methodologies, key characteristics of eminent S-boxes, major challenges, and their weak cryptographic properties. S-box is considered to be secure if it meets a number of criteria, i.e., maximum linear probability, bijection, nonlinearity, input/output XOR distribution, bit independence criterion, and strict avalanche criterion. These criteria are analyzed in detail to evaluate the performance, reliability, and effectiveness of S-box.

✉ Adil Waheed
numl–f20–26352@numls.edu.pk

[1] Faculty of Engineering and Computer Sciences, National University of Modern Languages, Islamabad, Pakistan

[2] Department of Information Sciences, Division of Science and Technology, University of Education, Lahore, Pakistan

[3] Faculty of Computer and Information, Multimedia University, Cyberjaya, Malaysia

[4] Universiti Putra Malaysia, Seri Serdang, Malaysia

Keywords S-box · Nonlinearity, cryptography · Attacks · Ciphertext

1 Introduction

Cryptography is currently being used to obscure information to secure the digital marketing transactions over the network. In this contemporary world, cryptography is a technique to convert an original message into coded format (by using ciphers) with the purpose to create confusion in the data and converting back coded data into plaintext at the receiver end (decryption). In digital marketing, a security concern is a big challenge. The speedy, hassle free, and reliable transactions via the internet are a necessity of the digital age as the general public is totally relying on the internet for routine life activities and marketing transactions. In the connection to data protection, confidentiality, authentication, non-repudiation and data integrity are core concerns. These concerns motivate computer scientists for designing cryptographic algorithms to bring ease to an individual's life. Cryptography is divided into two branches, called as substitution and transposition. In substitution, each letter of the message alters its identity but maintains its position whereas in transposition letters of the actual data are rearranged [29] .Two types of cryptographic models exist for secure digital communications i.e., Symmetric and Asymmetric. In symmetric encryption technique, only one secret key is used for encryption and decryption of plaintext. A cipher system is called symmetric if the decryption key can be easily guessed from the encryption key [43]. The key must be exchanged among both parties with the aim to use in the encryption and decryption process. Whereas, in an asymmetric encryption scheme, two keys are used to encrypt and decrypt the message: one is public and the other is private [41]. Actually, data is "scrambled" using private encryption methods, making it meaningless to the third party which does not have the crypto key to decrypt it. Once the message has been transmitted to the chosen receiver who has the key, the algorithm returns the cipher text to its original message. Secret key is a specific password/code or a random number which is generated through some secure key generator algorithms. Symmetric encryption algorithms are divided into two categories: Block algorithms: The data bits are bound into blocks and encrypted using a particular secret key. As the encryption is in process, the system holds the data into memory till the completion of the block. In stream Algorithms, there is no concept of storing data into memory, data is encrypted as it streams.

Asymmetric-key algorithms are known as "public-key algorithms". They employ public and private keys, which are logically connected to each other. The pair of public and private keys is considered a 'key-pair'. From key-pair, one is used for data encryption, while the other is used in the decryption process. Public key is accessible to the general public, while the owner keeps the private key hidden at all times. There is no logical connection between public and private so, one cannot be used to determine the other. To preserve an individual's privacy, the Statistical Transformation with 3-Dimensional Shearing Algorithm (ST3DSA) distorts the data utilizing three-dimensional shearing transformations, information value, and weight of evidence even without exchanging the mining results. For the sake of analysis, the recommended ST3DSA procedure is applied to both numerical and categorical parameters in the bank marketing, adult income, and lung cancer datasets. The experimental results confirmed that ST3DSA has the capacity to cope with a person's privacy issues [30]. In order to secure cloud storage and sharing, Kumar et al. [55] presented a certificate-less encoding technique. In this technique, the user gets character-based cryptography to provide attribute - based

encryption in the certificate less encryption scheme. Clients can design their own personality via open and private key match using any open public key encryption algorithm. The general public key is sent to the cloud with the character for approval. After confirming the personality of the comparing client, the cloud will generate two or three open keys and private keys. So, each user has their own open public and private key and both of these keys are generated by the cloud. This scheme is composed of RSA and Blowfish algorithms and both of these algorithms belong to a symmetric cryptosystem. Secondly, it is important to know all codes being used in cryptography as code performs real mathematics like twisted path code, shift code, and reverse tail etc. [27]. There are numerous strong arguments why algorithms/crypto codes should be made public. Actually, it is incredibly easy to make a minor change and create a weak cryptographic algorithm. If the algorithm is not accessible to general public, no one will notice the flaw until an attacker attempts to exploit it [17].

In 1997, the National Institute of Standards and Technology started the process of selecting cryptographic encryption algorithms. Finally, the Rinjdael Algorithm (Advanced Encryption Standard) of Symmetric Key Cryptosystem was accepted as a standard for secure digital communication. This recognition led to its widespread usage in the implementation of critical applications requiring reliable architecture. The only nonlinear key component of AES is S-box which is used to obscure the correlation between plaintext and ciphertext and produces resistance to cyber-attacks. Actually, S-box is the indispensable part of a secure block cipher scheme which is also used to build relations between key and ciphertext as complex as possible. The nonlinearity, strict avalanche criterion and differential uniformity are considered as fitness functions in the evaluation of S-box. Crypto S-box should have different and unique values and there should not be a correlation among the values to assure the quality of S-box. Various variants of S-box are more robust and capable of providing interesting properties to cryptographic algorithms. There are several S-box construction methodologies presented in literature to design high quality S-boxes with increased algebraic complexity, nonlinearity and other good cryptographic properties. Chaotic maps play an important role in the generation of random numbers to construct quality S-boxes by using heuristic techniques. A significant number of articles is available in literature based on chaotic maps to generate dynamic and complicated S-boxes.

This article primarily focuses on S-Box analysis for the purpose of securing the digital transmission of multimedia:

1) A detailed review of S-box and its basic anatomy, and an extensive analysis of current S-box construction methodologies.
2) A comparative analysis of old known and the latest newly proposed S-boxes for investigating their cryptographic features.
3) A Comprehensive study of S-box performance evaluation criteria including nonlinearity, strict avalanche criterion, bit independence criterion, differential uniformity, linear probability, and fixed points is conducted. In addition, we propose the challenges in order to judge the quality of an S-box.

Organization of the Paper: The rest of the arrangement of this article is given as follows. In Section 2, we reviewed the S-box construction techniques and their mathematical formulas as presented in literature. In Section 3, a study of S-box performance evaluation criterion is discussed. In Section 4, a comparative study and challenges are presented. In Section 5, a conclusion is given Fig. 1.

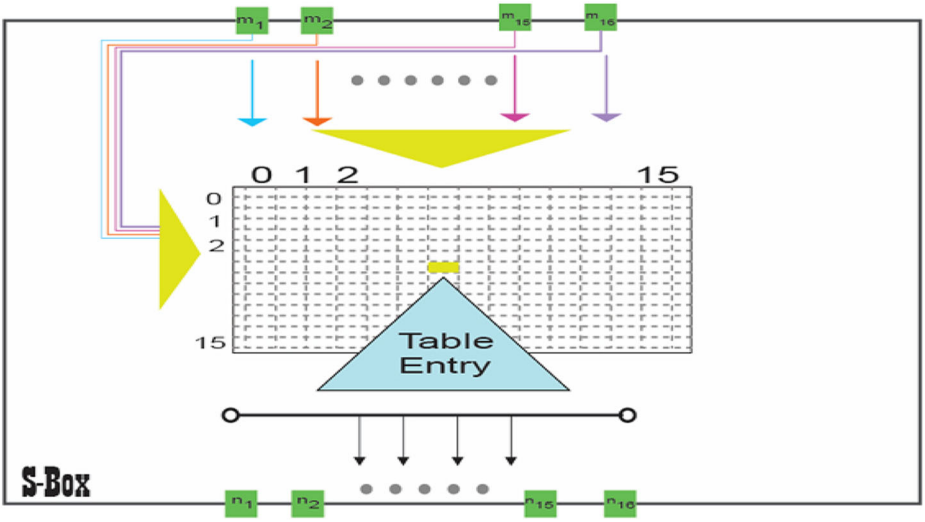

Fig. 1 Block diagram of 8*8 S-box

2 S-box structure and key methodologies for S-box construction

Security development is a key to communication technologies. Currently, advanced encryption standard (AES) is considered to be a reliable encryption algorithm for encryption of electronic data for secure transmission. A variety of approaches have been made to evaluate the security and performance of AES and it is important to note that Substitution box (S-box) is key in designing and implementing of AES and it is used in the development of advanced cryptographic algorithms as well. S-box is a confusion component and mathematically it is represented as a mapping S: $\{0, 1\}^n \rightarrow \{0,1\}^n$, where $\{0,1\}^n$ denotes a vector of n elements from Galois field $GF(2^n)$. In other words, S-box receives n input bits and alters them into m output bits. It's referred to as S-box and frequently utilized as a lookup table. A high-quality S-box is considered to have statistical properties of cryptography like confusion and diffusion that make it resistant to various attacks and in cryptosystem, playing a vital role in cryptography for data transmission and secure communication over the network. Generally, S-box is a table of m rows and n columns and each element of S-box should be an integer with size of one byte and in range of {0,1, 2,3,….,255}.

2.1 Key methodologies for S-box construction

S-box is the only nonlinear component in the AES encryption process which is fixed throughout the algorithm and due to its fixation, the cryptanalysts tried to exploit this weakness. The key idea of the research is that the background Galois field and its underlying primitive polynomial have an impact on the S-boxes' function and performance. This finding leads to the interesting notion that, rather than developing new algorithms, improving current algorithms is worth researching since it is the least time-consuming yet more successful. An S-box is carefully chosen to give security against any linear or differential cryptanalysis. The Mobius transformation, complete Latin square, linear trigonometric transformation, affine transformation and Lightweight S-box construction methodologies are explored for the

structure of newly constructed S-boxes because of its wider use and complicated features. So, the researchers are currently working on construction of those dynamic S-boxes which are more immune against linear and differential attacks. We have covered review of those S-boxes' construction methodologies in this section.

2.1.1 A. Linear Trigonometric Transformation

An $n \times n$ S-box is generated through following trigonometric transformation [69].

$$T(z) = Cos((A+B)*X*z+C)$$

Where,

$$\begin{gathered} 0 \le z \le (2^n - 1), \\ n = 8, \\ 0 < X < 1, \\ A, C \in \{1, 3, \ldots, 2^n - 1\}, \\ B \in z \; and \\ B = Array \; of \; size \; 256 \end{gathered} \tag{1}$$

The values of the variables A, B, C, and X in the above equation are used by the encryption key. This equation is capable of producing dynamic S-boxes using different values of above-mentioned parameters.

2.1.2 S-box construction using complete Latin Square

A Latin square is a square matrix and consists of rows and columns with the condition that each row and column contains unique values. Complete Latin square can be constructed in one of the following ways.

Method 1: Latin square of size N × N (N = 2y and y∈ {1, 2, 3, …, *N*}) is generated as

$$0, 1, 2m-1, 2, 2m-2, 3, 2m-3, \ldots, m-1, m+1, m \tag{2}$$

Method 2: Primitive root g of prime number N + 1 is calculated as

$$a_i = g^i mod\ N + 1, i \in \{1, 2, 3, \ldots, N\} \tag{3}$$

Determine the primitive roots g of N + 1; if N + 1 is a prime number. For completion of Latin square, uses of chaotic sequences are very important and generated by the enhanced logistic map. Logistic map is comprised of following three steps for S-box construction [21].

1) Latin Square Generation
2) Generation of two orthogonal matrices
3) Using chaotic sequences, S-box is constructed by scrambling the orthogonal matrices.

2.1.3 Mobius Transformation and Permutation Function

Linear transformation function is also known as Mobius transformation and it is written as given below

$$Z(x) = \frac{ax + b}{cx + d} \tag{4}$$

Where, $ad - bc \neq 0$ *and* a, b, c *and* d *belongs to Galois Field* (GF)

The Galois field GF has a fixed number of elements and it is applicable on data which has a vector representation. A finite field has addition and multiplication operations. In cryptographic encryption Galois Field is represented as M^n, where M = 2 and 256 order Galois field $GF(2^8)$ is used in AES. In this transformation, elements are represented as bytes (one byte contains 8 bits) which are denoted as a polynomial with coefficients from binary Galois field $GF(2)$ as

$$a_7x^7 + a_6x^6 + a_5x^5 + a_{47}x^{47} + a_3x^3 + a_2x^2 + a_1x + a_0 \tag{5}$$

Permutation is the process of rearranging the function f from set D into C such that each element of D has unique output as $f: D \rightarrow C$ *is one to one if* and only if $f(x) = f(y)$ implies $x = y$.

Function $f: D \rightarrow C$ is onto if for each element c ∈ C, there exists some $d \in D$ *with* $f(d) = c$. A function which has properties of one-to-one and onto is known as bijective function. Total number of permutations is given by n! for a set of n elements. Linear fractional property is utilized for construction of S-box and its application on Galois Field (2^n, $n = 8$) having elements from 0 to 255 in decimal form. By using $GF(2^n)$, the generated S-box will consist of 256 elements. Traditional AES S-box uses fixed irreducible polynomial $P(x) = x^8 + x^4 + x^3 + x + 1$ to find out multiplicative inverse. In [16, 40], $P(x) = x^8 + x^4 + x^3 + x^2 + x + 1$ polynomial was also used for construction of S-box and here is a complete procedure as discussed in [40].

i. Chosen linear fractional transformation $f(z) = \frac{35z+15}{9z+5}$ and $P(x) = x^8 + x^4 + x^3 + x^2 + x + 1$
ii. Calculating f(z)by taking all values of GF(2^8)
iii. Matrix generated from linear fractional transformation
iv. Applied permutation to the matrix and produced required S-box.

2.1.4 S-box construction based on Bent Function and Logistic Chaotic System

Here are the steps to construct S-box with high nonlinearity based on bent function and discrete chaotic system [26].

i. Logistic chaotic system
ii. Constructing Boolean function $g(x)$
iii. Construction of Maiorana MC Farland type bent function
iv. Construction of MM type Multi output bent function
v. Constructed S-box did not meet the standard properties as S-box should have unique values from 0 to 256. To maintain this property; all duplicate values will be removed and replaced with missing numbers.
vi. Generating S-boxes with high nonlinearity

S-boxes generated through this method to be used in symmetric cryptography techniques/ algorithms and made full use of the properties of chaotic system.

2.1.5 S-box construction using discrete chaotic maps and cuckoo search algorithm

This method has used the properties of 1-D discrete chaotic maps including pseudo random sequence generator to design optimized S-box with high values of bijectivity, nonlinearity, strict avalanche criteria etc. Here is a pseudo code to construct S-box based on chaotic map and cuckoo search algorithm [3].

i. A discrete chaotic map is chosen
ii. Set the chaotic map's starting settings
iii. Start iteration from *0* to *n* for chaotic map i.e. S-box[i] = i + 1
iv. Keep continue the iteration process until all cells of S-box have been filled
v. Use the generated S-box as initialization for optimization
vi. Applied Cuckoo search algorithm
vii. Compute Nonlinearity as a fitness function

This was all about the process of S-box generation using a chaotic system with the use of a cuckoo search algorithm. However, cuckoos are interesting birds due to their behavior during egg-laying or hatching period as they prefer to store their eggs into nests of cuckoos to increase the hatchability or to gain higher possibility of feeding. Hers are the steps for a cuckoo's search to design a S-box

i. Host nest generation using chaotic map
ii. Get cuckoos using levy flight
iii. Maintain balance
iv. Evaluate fitness
v. Select a nest (S-box), n randomly

2.1.6 Affine Transformation Based S-box Construction

S-box construction consists of three affine equations with their corresponding convenient vector. Through affine transformation, there are following ways to design compact nonlinear substitution boxes [13].

- Forward S-box construction
- Backward S-box designing

The steps involved in the forward S-box construction are explained as follows

i. As per irreducible polynomial $f(z) = x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$, taking the multiplicative inverse of 256 values.
ii. Compute affine transform and XORed the output with the first constant vector
iii. Repeated the above procedure with the second affine transform and the output XORed with the second constant vector.
iv. Kept repeating the same procedure with the third affine transform and the result XORed with third constant vector. In this way, by applying multi affine transformation, a compact nonlinear S-box will be generated.

2.1.7 Lightweight 8-bit S-box construction

In 8-bit S-box construction each element is replaced with its inverse and applied suitable affine transformation. To make it convenient, the selected field inversion composite field was $F(2^4)^2$. Let $ax + b$ is a random number in the said function, where a ϵ 4 *most signficant bits*, $b \in 4$ *least significant bits*. The inversion $cx + d = (ax + b)^{-1}$ can be calculated as follows [46].

$$(ax+b)^{-1} = a\left(a^2B + abA + b^2\right)^{-1}x + (b+aA)\left(a^2b + abA + b^2\right)^{-1} \tag{6}$$

Where, A = 1, B = λ, the simplified form of the equation is

$$\begin{aligned}(ax+b)^{-1} &= a\left(a^2\lambda + b(a+b)\right)^{-1}x + (b+a)\left(a^2\lambda + b(a+b)\right)^{-1} \\ &= aD^{-1}x + (b+a)D^{-1}\end{aligned} \tag{7}$$

The irreducible polynomials are written as follows

$$F_2 = F_{2^2} \qquad Q_0(x) = x^2 + x + 1 \tag{8}$$

$$F_{2^2} = F_{(2^2)^2} \qquad Q_1(x) = x^2 + x + \varnothing \tag{9}$$

$$F_{2^4} = F_{(2^4)^2} \qquad Q_2(x) = x^2 + x + \lambda \tag{10}$$

To ensure the irreducible property of above polynomials, the values of $\varnothing and\ \lambda$ need to be selected carefully.

2.1.8 Lightweight S-box Designing for IoT Devices

The term "interconnection" is used to describe the internet of things between the physical computing devices or devices embedded with sensors, processing power having ability to communicate and exchange data with other devices. Developing IoT based devices without security does not make sense and definitely will make the users' privacy vulnerable. So, IoT integration with security protocols is a challenge. IoT architecture is explained as follows:

For IoT applications, the three-layer (Perception, Network and Application) architecture has become the most popular paradigm.

Perception: This layer contains the sensor devices. This is where the information originates. The information might come from any of the linked device's sensors.
Network: The network layer defines how huge volumes of data are transferred across an application. This layer connects all of the devices together and transmits data to the relevant back-end applications.
Application: This is the layer that consumers view. This might be an app for controlling a device in an intelligent environment, or a platform that displays the integrity of the system's components. IoT architecture is illustrated in Fig. 2.

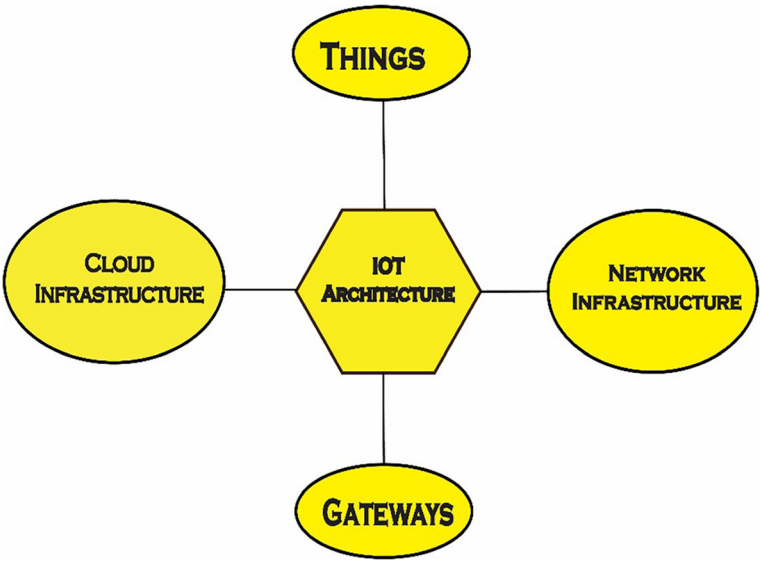

Fig. 2 IoT Architecture

In connection with IoT, Alshammari et al. [4] presented a symmetric lightweight cryptosystem in IoT devices using a chaotic S-box, based on the conventional AES. The permutation and diffusion phases are implemented using the Hilbert curve scan pattern and the Lorenz system. Here are the key steps to generate IoT based S-box

i. Create a set of Chaotic Map of 2048 bits
ii. Generate empty binary set S
iii. Iterate 200 times following Lorenz Map equation

$$\begin{aligned} x^{'} &= a(y-x), \\ y^{'} &= cx - y - xz \\ z^{'} &= xy - bz \end{aligned} \tag{11}$$

iv. Iterate 2048 times above equation and represent the current values as $x^{'}$, $y^{'}$, $z^{'}$. x is obtained as $x = mod\ (floor(10^4 * x^{'}),\ 2)$
v. Divide the empty set S into 8 binary sub sets of 256 bits for getting m Boolean functions.
vi. S-box created

In context of IoT security, Sohal et al. [59] uses three technologies for identification of hostile edge devices in a fog computing environment: the Markov model, the Intrusion Detection System, and the Virtual Honeypot Device.

2.1.9 S-box Construction using Subgroup of Galois Field (GF)

In all types of block ciphers, S-box is used to create confusion in the data as it is only nonlinear transformation component. Size of the S-box depends on the application's scope. In [56], S-

box is designed based on fifteen order subgroup of the GF of order 256. The method is explained as follows:

i. Inversion function representation p: Subgroup named as K_{15}

$$\begin{array}{c} p : K_{15} \cup \{0\} \rightarrow K_{15} \cup \{0\} \; by \; 0 \\ y^{-1}, if \; y \in K_{15} \\ 0, if \; y = 0 \end{array} \tag{12}$$

Here is a way to calculate inversion function P(y)

ii. Linear scalar multiplication is defined as

$$\begin{array}{c} q : K_{15} \cup \{0\} \rightarrow K_{15} \cup \{0\} \; by \\ q(y) = uy, For \; all \; y \in K_{15} \cup \{0\}, u \in K_{15} \; is \; fixed \end{array} \tag{13}$$

iii. In the result of composing p and q, 8 × 8 bit S-box would be produced.

As discussed above fifteen linear scalar functions can be defined on the basis of $K_{15} \cup \{0\}$. So, therefore as a result 15 different S-boxes would be constructed Tables 1 and 2.

2.2 Analysis of above discussed S-box design methodologies

A block cipher is an encryption method that divides the plaintext into fixed-length groups called blocks. Encryption is carried for the whole block rather than one bit at a time as in stream ciphers. Confusion and diffusion are two wide ranging operations of secure cipher which were proposed by Claude Shannon in the domain of cryptography. The diffusion deals with the changing effects of a single bit of plaintext to cipher text to obscure the relationship between plaintext and cipher text and vice versa. Confusion means each bit of cipher text alters as per change in key or plaintext that obscures the relationship between plaintext and key. The concept of round recurrence plays a key role to attain the concepts of confusion and diffusion. Block cipher cryptosystem consists of four major conversions: substitution, permutation, mixing and key adding. We frequently reuse certain well-known and extensively used S-boxes, but there is always a need for new S-box construction methods for ensuring confusion properties of the cryptosystem. In the discussed cryptosystems, connected chaotic systems and different S-boxes are employed. The chaotic range is improved by combining chaotic systems, which is important for increasing the level of confusion in cryptosystems. So, the main contribution of S-box in discussed methodologies is to create confusion while also enhancing security and robustness. Linear Cryptanalysis is a powerful method used widely on block cipher for cryptanalysis and it is an effective method for developing powerful and complex attachments. By using the concept of high probability and taking its advantage, it posits a relationship between plaintext bits, ciphertext bits and the key. This one is a well-known plaintext attack where the attacker has random information about plaintext bits and corresponding ciphertext bits. Therefore, a linear approximation is a way to find out the action of cipher, i.e. *Encrypted text* = f(*plaintext*, *key*). Linear cryptanalysis refers to mod-2 bit-wise

Table 1 Summary of Novel Methodologies

Sr. No.	Methodology	Key Features	Strengths	Weaknesses
1	Mobius Transformation	Mobius transformation is a configuration of inversions, rotations, translations and magnifications. When Mobius transformation is performed, symmetry is always maintained without any loss. It can be defined as a transformation where, $f(z) = \frac{az+b}{cz+d}$ In above equation, az+b and cz+d both are linear and a, b, c and d belongs to Galois Field (2^8).	The main strength of Mobius transformation is that linear time varying systems that depend rationally on parameters can be described as an interconnection of a nominal linear time invariant system and a structured parameter block.	Mobius transformation is based on the degree 8 irreducible polynomial. That's why, we have to be very careful while selecting the degree 8 irreducible polynomial for constructing GF (2^8) because this selection may heavily affect the calculations and disturb the confusion creating potency of obtained S-box.
2	Linear Trigonometric Transformation	Mathematical representation of dynamic linear trigonometric transformation for generating an n×m S-box is given as: $T(z)=Cos((A+B)*X*z+C)$ Where, $0 \leq z \leq (2^n-1)$, n=8, $0 < X < 1$, A, $C \in \{1, 3, \ldots, 2^n-1\}$, $B \in z$, B= *Array of size* 256. The encryption key uses the values of variables A, B, C, and X in above equation.	The dynamic nature of this technique yields huge key space to an S-box designer compared to float type variable. Secondly, it returns large number of keydependent dynamic S-boxes.	One of the variables X has data type as double and consider 15 significant decimal digits for the generation of S-box. The computation using such a variable is a bit slow as comparedto float type.
3	Complete Latin Square	A Latin square is a $n \times n$ array containing n distinct symbols in form of matrix, each of which appears precisely once in each row and column. In this methodology, improved logistic map uses the provided base state to produce chaotic sequences. The Latin square is generated using a portion of chaotic sequences. Two orthogonal matrices are generated using the entire Latin square. An S-box may be created by disrupting the orthogonal matrices using chaotic sequences.	This S-box generation process does not contain complex matrix row, column or transform operations. Its time complexity is low and thus can achieve a high generation efficiency.	In this procedure, to make the distributions of all the elements in a matrix more uniform, element positions of the matrix are randomly scramble but in decrypting process this randomization fashion makes it impossible to trace the actual position of the element.
4	Bent Function and Logistic	To generate the components of the S-boxes, the	Balancing method of this technique remove the	The threshold quantization method is used in the

Table 1 (continued)

Sr. No.	Methodology	Key Features	Strengths	Weaknesses
	Chaotic System	logistic chaotic map combined with Bent functions. The features of chaotic functions fully utilized in this strategy. Bent functions with high nonlinear values are mostly generated via logistic mapping.	duplicate outputs and all elements with the same output are replaced with 256. This procedure ensures bijective property of an S-box.	selection of the value quantizationmethod of the chaotic sequence but the quantized binary sequence is constant and it should be dynamic.
5	Discrete chaotic maps and cuckoo search algorithm	Cuckoos are fascinating to watch because of their unique behavior during egg laying period. Most of the cuckoos choose to lay their eggs in the nests of other cuckoos to increase the hatchability and even sometimes they remove eggs of nest holder for better breeding process. In this methodology, a composition of chaotic map and cuckoo search algorithm is applied to generate cryptographically strong S-boxes. The addition of Cuckoo search optimization to the previously created S-boxes resulted in an effective S-box, with the goal of obtaining maximal nonlinearity.	S-box generation using discrete space chaotic map to help the search process to start from good positions and avoid trapping in local optima.	The weakness in Cuckoo search algorithm include the considerable amount of time required to compute fitness functions, the relatively low convergence rate and the possibility of failure in executing a full global search.
6	Affine Transformation	To achieve high nonlinearity, this methodology constructs the S-box by multiplying multiple separate affine transformations with multiple distinct overlapping vectors of 8 bits.	This scheme put some additional conditions on the nonlinear layer of a sub-byte stage that will enhance the avalanche and completeness comprehensions for the intended S-box.	This design methodology requires more constant vectors to increase the complexity of the S-box and make it difficult computationally.
7	Lightweight 8-bit S-box construction	A lightweight 8-bit S-box that may be coupled with S-box-1 to get a security level that is nearly comparable to the AES S-box.	The sub-blocks of the S-box are implemented based on efficient circuits. A large number of gates, in the structure, have been implemented by the 2-input NAND gate to reduce delay and area.	This designing procedure is specific to field inversion in $\mathbf{F}_2{}^4$. It should be dynamic to all possible field inversion instead of dealing with individual ones.
8	Lightweight S-box for IoT Devices	This is totally AES based lightweight encryption procedures for IoT	This S-box construction algorithm is based on chaotic Boolean function and	This S-box generation method is just designed in order to address the

Table 1 (continued)

Sr. No.	Methodology	Key Features	Strengths	Weaknesses
		devices. To demonstrate the scheme's efficiency, it is used to encrypt a grayscale image using an XM1000 sensor. As a result, this approach might be used to securely encrypt images and transmission across networked smart devices.	the Hilbert curve that is used to permute values of the initial S-box. At each iteration calculate the nonlinearity value of the generated S-box. Whenever high value of nonlinearity is returned, corresponding S-box is saved.	vulnerabilities of IoT devices. It would be better to enhance the scope of this algorithm in general perspective, not limited to IoT devices.
9	Subgroup of Galois Field	Instead of using a Galois field, this methodology uses a novel substitution box (S-box) structure based on the members of the maximum cyclic subgroup of the multiplicative group of units in a finite Galois ring.	The main strength of this scheme is that is based on Boolean functions over the maximal cyclic subgroup adjoining zero, with the extension0→0. That's why it is very efficient and easily satisfy the majority logic criterion and useful in watermarking as well.	In this designing method mapping of the S-box is one-one from $G_n \cup \{0\}$ *to* $GF(2^8)$ that is not bijective.
10	Symmetric Group composition	This construction technique uses method of composition of permutation [9].	Ensures that created S-box is balanced.	Uses large set of irreducible polynomials.
11	TDERC sequence based designing	S-box design is based on tangent delay for elliptic cavity chaotic sequence and a particular permutation of symmetric group of permutations [22]	Linear and differential types of attack are easily avoided by using this technique based S-box.	Nonlinearity is not up to the mark. It should be equal to the standard AES S-box.
12	Artificial Immune algorithm	This designing approach based on clone selection criteria [24].	In reasonable search time, generated S-boxes have low differential uniformity.	A large set of S-boxes are generated instead of creating one best fit for AES.
13	Chaotic map and composition system	This construction technique based on composition of S-boxes but starting from one reference point [31].	Chaotic map is used to get sequence of starting S-boxes. Produced S-boxes have low complexity and larger key space.	It is good to use with key dependent S-boxes.
14	Keyed based S-boxes	Design based on 2D hyper chaotic map and algebraic operation [58].	Generated S-boxes have high nonlinearity.	The focus in only on keyed S-boxes instead of constructing generic ones.
15	Multi chaotic System	This study uses two dimensions (Lorenz and Henon map) to design strong S-box	This S-box is specifically designed for image encryption with good statistical properties and large key space.	Other chaotic maps should be utilized to construct S-boxes for comparison purpose.

Table 2 Boolean function representation for n = 2

X	y	z	x.y	$x.y \oplus z$
0	0	0	0	0
0	0	1	0	1
0	1	0	0	0
0	1	1	0	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	1
1	1	1	1	0

chain of exclusive-OR operation denoted by ⊕. $X_{i_1} \oplus X_{i_2} \oplus \ldots \oplus X_{i_n} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \ldots \oplus Y_{j_m} = Z_{k_1} \oplus Z_{k_2} \oplus \ldots \oplus Z_{k_w}$.

X_i represents the ith bit of input set $X = [X_1, X_2, \ldots]$, Y_j indicates the jth bit of output $Y = [Y_1, Y_2, \ldots]$ and Z_k represents the k^{th} bit of the key. While performing linear cryptanalysis it is assumed that everything is known except key and requires following three steps.

i. Find linear approximation of nonlinear parts of the algorithm usually through S-boxes.
ii. Linear approximation is a method used to relate the plaintext bits, ciphertext bits and the bits of key. Pairing the linear approximation of S-boxes with other linear operations of encryption algorithm to compute linear approximation of entire encryption algorithm.
iii. Linear approximation works as a guide for which key to try first.

Differential cryptanalysis refers to a set of blueprints for tagging differences in a network of transformations, finding places where a cipher exhibits organized behavior, and using such attributes to recover the private key. Specifically, it is used in the study of block cipher to determine the result in the encrypted ciphertext in case of change in plaintext. It is important because a change in a specific pattern in encrypted text may signify weakness in the encryption scheme. This one is also known as chosen attack as the attacker has a choice to select input and corresponding output in an attempt to derive a key. In this cryptanalysis, a pair of inputs (X', X'') chosen by the attacker, to satisfy ΔX a corresponding ΔY value, occurs with high probability. The pair (ΔX, ΔY) referred to as a differential. Chaotic S-boxes are being used in the domain symmetric encryption algorithms. It is, therefore, by the use of chaos properties and Bent function; S-boxes are generated with high nonlinearity. In this technique, a set of bent functions is constructed as an output of an S-box to construct a high quality S-box. Randomness is an important index in a digital chaotic system. Lightweight S-boxes are required to ensure the security of IoT devices. Nonlinear 4 × 4 S-boxes are suited to internet of things (IoT) applications and the structure is developed in the Galois field $GF(2^4)$ *and* $GF(2^2)^2$. The field is realized by taking the multiplicative inversion followed by an affine transformation. The affine transmission is carried out in the Galois Field $GF(2^4)$. The constructed S-box with basic mathematical structure demonstrates 5% in the gate equivalent area. For 4-bit input, 4-bit Boolean function (BF) gives 1-bit output that is represented as a 16-bit output vector. Similarly, the truth table of a 16-bit Boolean function is represented by a 16-bit vector. The 4-bit sequential input produces 16 rows, each bit specifying the position at the same column and consists of bits and thereby four 4-bit input vectors are generated with the help of four 16-bit columns which are commonly used for all types of 4-bit Boolean function. So, 16 output bits created 2^{16} possibilities and the equivalent decimal varies between 0 to 2^{16}. Hence, for four 16-bit input vectors there are 2^{16} possible 16-bit output vectors. The 8-bit Boolean function provides 1-bit

output for 8-bit input and displays the output in the form of a 256-bit vector while the truth table is shown by 256-bit output vector using 8-bit Boolean function. The 8-bit sequential inputs contain 256 rows and provide an 8-bit input vector which is common for 8-bit Boolean function. Finally, we can say four valued 4-bit functions can be used to represent a 4-bit S-box.

2.3 Review of Boolean function and its algebraic form

Modern cryptosystems rely heavily on substitution boxes (S-boxes) and Boolean functions. If a function $f: GF(2^n) \rightarrow GF(2)$ receives n tuples as input and produces one of the two output bits $\{0, 1\}$ [10]. If a Boolean function takes 4-bit input $\{x_1, x_2, x_3, x_4\}$, produces 16 combinations of decimal values varying from 0 to 15 and for each combination of input, it will provide 1-bit output. This input-output relationship gives a 16-bit output vector against four 16-bit vectors, each one attached to 4-bit input as mentioned above. Boolean's function is a mapping from $(0, 1)^4$ *to* $(0, 1)^1$ and algebraically with 16 coefficients is denoted as

$$\begin{aligned} \mathrm{F(x)} = a^0 &+ \left(a^1.x^1 + a^2.x^2 + a^3.x^3 + a^4.x^4\right) \\ &+ \left(a^5.x^1.x^2 + a^6.x^1.x^3 + a^7.x^1.x^3. + a^8.x^2.x^3 + a^9.x^2.x^4 + a^{10}.x^3.x^4\right) \\ &+ \left(a^{11}.x^1.x^2.x^3 + a^{12}.x^1.x^2.x^4 + a^{13}.x^1.x^3.x^4 + a^{14}.x^2.x^3.x^4\right) + a^{15}.x^1.x^2.x^3.x^4 \ldots \end{aligned}$$

Where x belongs to 4-bit input $\{x_1, x_2, x_3x_4\}$ and denotes the hex value or decimal value, Boolean function assumes 1-bit output, '+' and '.' represents XOR and AND operations respectively.

For example, if n = 2 and $GF(2^n) \rightarrow GF(2)$ mapping is given as below

$$f(x, y, z) = x \,.\, y \oplus z$$

Thus, a single input bit results in a single output bit in a Boolean function, but an S-box is made up of multiple Boolean functions with distinct outputs.

2.4 Review of advanced encryption standard

Advanced Encryption Standard (AES) has variable rounds and the number of rounds depends on the length the of key. Each round comprises 4 functions: Sub-Bytes, Shift Rows, Mix Columns and Add round key. Here is a working scenario of AES

2.4.1 AES encryption process

This encryption process is organized into following four sub-processes:

A. Byte Substitution

The 16 input bytes are replaced by searching up an AES S-box. The end result is a matrix of size 4 × 4.

B. Shift Row

In this phase each row of the matrix is shifted cyclically to the left. The result is a new matrix of the same size and same values but on different positions.

III. Mix Columns

In this round, a special mathematical function takes four bytes from one column as input and returns four completely new bytes that replace the original column.

IV. Add Round Key

The matrix's 16 bytes are now treated as blocks of 128 bits and are XORed with the round key's 128 bits. If this is the final round, the output will be the ciphertext.

Moreover, the decryption process is also organized into four sub-process as discussed in the encryption process but in reverse order. Encryption and decryption process is illustrated in the following Fig. 3.

3 Performance evaluation criteria

An S-box is the only nonlinear component of block cipher and it should be resistant to various linear and differential attacks. S-box is considered to be secure if it generally achieves number

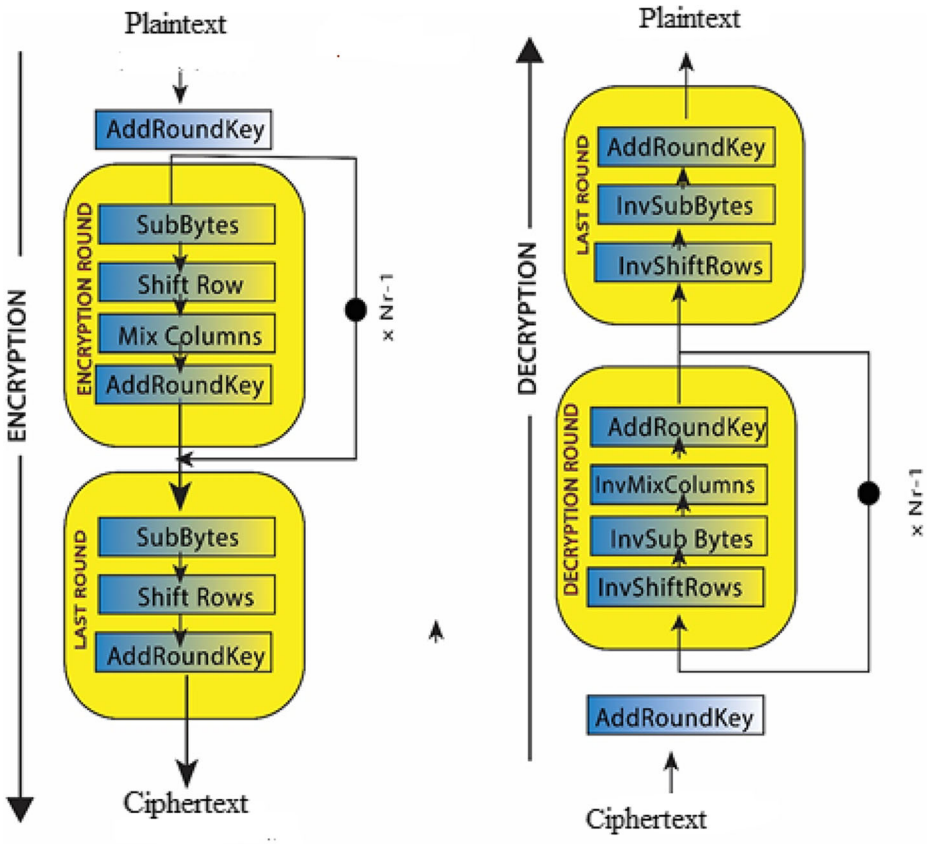

Fig. 3 AES Encryption and Decryption Stages

of criteria, such as nonlinearity, strict avalanche criteria, bijection, bit independence criterion, input/output XOR distribution and maximum linear probability.

A. *Nonlinearity*

An S-box is a nonlinear component and nonlinearity can be defined as a distance between the Boolean function and the set of all affine functions. S-box has a nonlinear mapping between ciphertext and plaintext as linear mapping is easily understandable by hackers or crackers to get the plaintext from ciphertext. In other words, nonlinearity refers to the change in number of bits in the truth table to reach the nearest affine function. Higher nonlinearity assures that S-box is more immune against linear attacks. The nonlinearity of S-box or upper bound can be calculated as follows [18]

$$NL_f = 2^{n-1} - \frac{1}{2} \max_{\alpha \in F_2^n} |W_{f(\alpha)}| \tag{14}$$

AES S-box has nonlinearity is 112. However, for $GF(2^8)$, the optimal value of nonlinearity is 120 and best known value of nonlinearity found in literature is 114.5 [14]. Nonlinearity comparison of S-boxes, yielded by various methods found in literature given in Table 3.

B. *Bit Independent Criterion*

The output bit independent criterion (BIC) is another desirable parameter to ensure the quality of S-box which was first introduced by Webster and Tavares [64]. BIC refers to the change of one bit in plaintext or key for a given set of values (avalanche vector), all the pairwise output values of respective set (vector) should be independent. The avalanche vector V^{ei} has two co-efficient components X^{th} *and* Y^{th} which are used to measure the bit independent criterion of overall pairs (P, P_i) of avalanche vector which differ only in bit i $P_i = (P \oplus ei)$.

Table 3 Nonlinearity of well-known S-boxes

S-box Construction	Nonlinearity
AES [12]	112
Gray [62]	112
APA [11]	112
Lu [36]	92
Skipjack [28]	102
Xyi [65]	98
Prime [23]	94
Zahid [70]	112
Arshad [7]	110
Arshad [6]	106
Tang [61]	109
Ahmad [1]	112
Sarfraz [54]	110
Gao [19]	108
Zahid [71]	112
Lambic [33]	108
Peng [42]	102
Liu [35]	110
Alzaidi [5]	110
Tang [60]	108

$$BIC^{ei}(d_j, d_k) = |corr(d_j^{ei} + d_k^{ei})| \quad (15)$$

BIC should be in the range of 0 and 1. In the best case it is equal to zero while in the worst case it is equal to 1.

C. *Strict Avalanche Criterion:*

In cryptography, avalanche effect is the desirable condition for block ciphers. Strict avalanche refers to the change of a single bit in plaintext or key results in a change of 50% of output bits. In the case of high-quality S-box, this slight change in input should cause a drastic change in ciphertext. If an error occurs in encrypted data on a wireless channel, the decryption process at the destination results in 50% original message to be an error due to SAC effect. In other words, the probability to switch each bit of input S-box should be one half changes in output S-box. The SAC score of some existing S-boxes presented in literature given in Table 4.

D. *Linear and Differential Probability*

In cryptosystem, a user tries to muddle plaintext into ciphertext in such a way that it becomes more meaningless for the invaders. Linear attack is one of the most widely used attacks on cipher blocks. In Nonlinear Transformed S-box, ideally, nonlinear transformation should have differential uniformity. There should be a unique mapping between input differential Δx_i and output differential y_i, while ensuring the uniform probability for each i. The differential uniformity for S-box is defined as

$$DP(\Delta x \rightarrow \Delta y) = \left[\frac{\#\{x \in X / S(x) \oplus (x + \Delta x) = \Delta y\}}{2^m}\right] \quad (16)$$

4 Comparative study of S-box

A quality S-box should satisfy a number of criteria which are discussed in detail in Section 4. In order to determine the performance and security of S-box some mandatory properties should be analyzed as shown in Table V. Niemiec and Machowski proposed the simulator in order to analyze the algebraic properties of S-box [39]. However, all properties cannot be

Table 4 SAC Score of well-known S-boxes

S-box	SAC Score
AES [12]	.5058
Gray [62]	0.5058
APA [11]	0.4987
Skipjack [28]	0.4980
Xyi [65]	0.5048
Prime [23]	0.5012
Zahid [71]	0.502
Lambić [32]	0.506
Farah [15]	0.501

analyzed by using this tool. Only a certain number of criteria can be evaluated which are nonlinearity, strict avalanche criterion, completeness, low XOR table, balanced and diffusion order. In order to assess the several properties of S-box a comparative analysis is presented in detail.

As a result, the analysis has found that some of the properties are very important in order to resist algebraic attacks including linear, differential and statistical etc. A detailed analysis is also discussed in [1] as given in Table 5. In the domain of cryptography, the nonlinearity property of S-box is analyzed which makes the S-box protected from linear cryptanalysis. High nonlinearity shows stronger resistance to linear attacks. Based on the previous study, there exists no specific method to evaluate the S-box quality or security while another study shows that only two properties are enough to judge the strength of S-box. These properties are strict avalanche criterion and robustness. In short, most of the researchers analyze the S-box properties based on their perception and common usage. Therefore, benchmark methodology will contribute to protecting S-box from algebraic attacks. The Niemiec and Machowski and Wang et al. [39, 63] simulators are used in order to analyze the algebraic properties of S-boxes Fig. 4.

4.1 Challenges in S-box construction

Since 2001, AES has been a worldwide standard encryption algorithm and S-box is one of its important nonlinear components, but this component is fixed throughout the algorithm. Due to its fixation, cryptanalysts attempted to take advantage of this flaw. In fact, the S-box is a heart of cryptosystem and its basic function is to create confusion between key and ciphertext. So, here are five biggest challenges confronting the future of S-box:

Table 5 Experimental results of cryptographic features of well-known S-boxes

S-box	Nonlinearity			SAC	BIC-NL	BIC-SAC	DP	LP
	MaxVal	MinVal	AvrVal	AvrVal	AvrVal	AvrVal	MaxVal	MaxVal
Razaq [52]	116	112	113.75	0.5017	104.00	.5018	12	0.1328
Razaq [50]	112	110	111.25	0.5029	110.78	0.5007	6	0.0781
Zhu [73]	108	102	105.75	0.5021	104.14	0.5050	10	0.1328
Zahid [72]	112	110	111.75	0.5029	103.74	0.5005	10	0.125
Zahid [67]	108	106	107.00	0.4968	103.50	0.5039	10	0.1562
Razaq [47]	108	104	106.75	0.5031	103.64	0.5073	12	0.1328
Razaq [51]	110	106	108.25	0.4985	103.00	0.5057	10	0.1406
Razaq [49]	112	112	112.00	0.5014	112.00	0.5030	4	0.0625
Zahid [68]	110	104	107.5	0.4980	103.50	0.5005	10	0.125
Razaq [48]	112	112	112.00	0.5056	112.00	0.5192	4	0.625
Alghafis [2]	105	97	102.87	0.5192	102.67	0.4787	54	0.1679
Zahid [66]	108	104	106.75	0.5070	103.92	0.4997	14	0.125
Jiang [26]	108	104	106.75	0.4975	103.57	0.5022	10	0.1328
Shahzad [57]	112	108	110.50	0.5031	109.21	0.5018	6	0.0859
Razaq [45]	110	101	106.75	0.5031	103.57	0.5005	10	0.1289
Hua [21]	108	102	105.25	0.5351	103.25	0.5087	–	0.1406
Javeed [25]	110	106	107.50	0.4997	104.64	0.5048	12	0.1406
Hematpour [20]	109	102	105.25	0.4960	104.53	0.5045	–	0.1328
Nizam Chew [40]	112	112	112.00	0.4980	112.00	0.4981	4	0.0625
Artuğer [8]	112	110	111.75	0.4968	104.00	0.5016	12	0.125

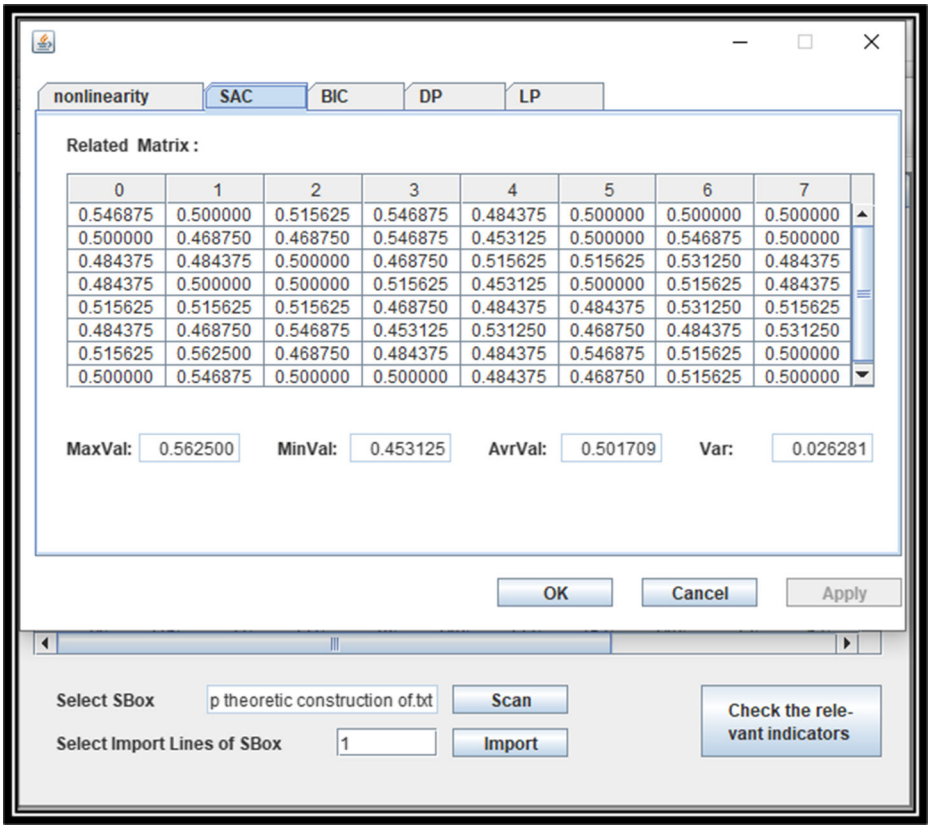

Fig. 4 Analysis of Razaq et al. S-box [52]

1) Currently used AES S-box is fixed so the major challenge is the construction of dynamic S-boxes which can be employed to replace static AES S-boxes. Fix mapping makes it relatively easy for an invader to decipher the original plaintext from the ciphertext. Hence, there is always a need to build robust S-boxes with a larger number of input bits that can resist several linear and differential attacks.
2) Many linear, trigonometric, heuristic evolution, spatiotemporal chaotic dynamics and chaotic map based S-box construction techniques are discussed in literature to produce robust S-boxes but the hardest challenge is to consider the critical properties which we consider important for the analysis and strength of S-box. The reason is clear that some algebraic properties have minor contributions and even vary case to case [44] but some have major contributions in the development of a good S-box. Fibonacci numbers and prime factors are also used to increase the security of S-box and presented the detailed analysis of S-box properties in [37]. Such nonlinear transformations to construct resistant S-boxes should be explored by researchers recurrently.
3) Another major issue is designing and selection of tools for the analysis of cryptographic properties of S-box as the existing tools do not have enough features to analyze all properties. Hence, we believe that development of new tools for the analysis of cryptographic properties will help cryptographers in better examining the behavior of S-boxes and researchers will be able to execute desired attributes of an entire S-box.

4) Researchers have investigated for a long time to construct various S-boxes and most of these S-box construction methodologies are random S-box generation. Security of random S-box is acceptable because of using different techniques in the development process and it is more immune against major cryptanalysis attacks. The problem is that randomness requires high computational complexity and it has no fixed points of reconstruction procedure [34]. So, instead of random construction, we should prefer to adopt complex mathematical structures for better resistance against algebraic attacks. For example, Hussain et al. [38] presented linear fractional transformation based S-box construction.
5) Sometimes S-boxes are generated manually or through simple mathematical operation but this type of construction is suitable for small S-boxes and even though this method could be lossy and uncompact for the construction of large S-boxes. Particularly, initial configuration must be improved by using novel approaches as discussed in Section 2.1.

5 Conclusion

In connection with the digital transactions, most of the new and interesting S-box security analytics are reviewed in this study. An S-box is the sole nonlinear component of most of the cryptographic algorithms that provides a complicated connection between plaintext and ciphertext and makes the digital transaction secure. Finally, we have conducted linear and differential analysis to see if the discussed S-box construction methodology has good statistical features which help in the resistance of algebraic attacks on digital communication. A comparison of the new and existing S-boxes reveals that the linear fractional transformation-based S-boxes are more robust in order to secure digital transactions and can be used in significant ciphers. However, some mathematical based construction techniques are better in terms of performance criteria but some are worse in the context of reliability and lower nonlinearity like chaos-based construction methods. Such S-boxes should be used with caution. For example, if we replace the Rijndael S-box in AES with some chaos-based S-box with overall lower nonlinearity, the resulting cipher will be weaker in terms of resistance to algebraic attacks. We have also compared the results of well-known S-boxes which are constructed from linear, differential transformations and with some permutations. The result shows that linear fractional transformation-based S-boxes are better than fractional order chaotic systems. Furthermore, all the discussed techniques enhance the security of digital transactions by introducing strong S-boxes instead of fixed one component of block ciphers. Furthermore, all of the discussed S-boxes have successfully cleared the standard security tests [53] as recommended by National Institute of Standard and Technology for secure digital communication.

References

1. Ahmad M, Khaja IA, Baz A, Alhakami H, Alhakami W (2020) Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications. IEEE Access 8:116132–116147. https://doi.org/10.1109/ACCESS.2020.3004449
2. Alghafis A, Munir N, Khan M (2021) An encryption scheme based on chaotic Rabinovich-Fabrikant system and S8 confusion component. Multimed Tools Appl 80:7967–7985. https://doi.org/10.1007/s11042-020-10142-x

3. Alhadawi HS, Majid MA, Lambić D, Ahmad M (2021) A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm. Multimed Tools Appl 80:7333–7350. https://doi.org/10.1007/s11042-020-10048-8
4. Alshammari BM, Guesmi R, Guesmi T, Alsaif H, Alzamil A (2021) Implementing a symmetric lightweight cryptosystem in highly constrained iot devices by using a chaotic s-box. Symmetry (Basel) 13:1–20. https://doi.org/10.3390/sym13010129
5. Alzaidi AA, Ahmad M, Doja MN, Solami EA, Beg MMS (2018) A new 1D chaotic map and β-hill climbing for generating substitution-boxes. IEEE Access 6:55405–55418. https://doi.org/10.1109/ACCESS.2018.2871557
6. Arshad B (2021) A novel method for designing substitution boxes based on Mobius group. https://doi.org/10.21203/rs.3.rs-173305/v1
7. Arshad B, Siddiqui N, Hussain Z, Ehatisham-ul-Haq M (2022) A novel scheme for designing secure substitution boxes (S-boxes) based on Mobius group and finite field. Wirel Pers Commun 124:3527–3548. https://doi.org/10.1007/s11277-022-09524-1
8. Artuğer F, Özkaynak F (2022) SBOX-CGA: substitution box generator based on chaos and genetic algorithm. Neural Comput & Applic 34:20203–20211. https://doi.org/10.1007/s00521-022-07589-4
9. Bin Roslan MF, Seman K, Ab Halim AH, Syam Mohd Sayuti MNA (2019) Substitution Box Design Based from Symmetric Group Composition J Phys Conf Ser 1366. https://doi.org/10.1088/1742-6596/1366/1/012001
10. Carlet C (2013) Vectorial Boolean functions for cryptography. Boolean Model Methods Math Comput Sci Eng 398–470. https://doi.org/10.1017/cbo9780511780448.012
11. Cui L, Cao Y (2007) A new S-box structure named affine-power-affine. Int J Innov Comput Inf Control 3:751–759
12. Daemen J, Rijmen V (2002) The Design of Rijndael
13. Dawood OA, Khalaf M, Mohammed FM, Almulla HK (2020) Design a compact non-linear S-box with multiple-affine transformations. In: Communications in Computer and Information Science. Springer, pp. 439–452
14. Dimitrov MM (2020) On the Design of Chaos-Based S-boxes. IEEE Access 8:117173–117181. https://doi.org/10.1109/ACCESS.2020.3004526
15. Farah MAB, Farah A, Farah T (2020) An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dyn 99:3041–3064. https://doi.org/10.1007/s11071-019-05413-8
16. Farwa S, Shah T, Idrees L (2016) A highly nonlinear S-box based on a fractional linear transformation Springerplus 5. https://doi.org/10.1186/s40064-016-3298-7
17. Ferguson N, Schneier B, Kohno T, Niels Ferguson BS (2010) Cryptography Engineering: Design Principles and Practical Applications, Chapter 9.4: The Generator
18. Gao S, Ma W, Zhu J (2012) Nonlinearity Profile Test for an S-Box
19. Gao W, Idrees B, Zafar S, Rashid T (2020) Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF(2 8)). IEEE Access 8:136736–136749. https://doi.org/10.1109/ACCESS.2020.3010615
20. Hematpour N, Ahadpour S, Behnia S (2021) Presence of dynamics of quantum dots in the digital signature using DNA alphabet and chaotic S-box. Multimed Tools Appl 80:10509–10531. https://doi.org/10.1007/s11042-020-10059-5
21. Hua Z, Li J, Chen Y, Yi S (2021) Design and application of an S-box using complete Latin square. Nonlinear Dyn 104:807–825. https://doi.org/10.1007/s11071-021-06308-3
22. Hussain Alkhaldi A, Hussain I, Gondal MA (2015) A novel design for the construction of safe S-boxes based on TD ERC sequence. Alexandria Eng J 54:65–69. https://doi.org/10.1016/j.aej.2015.01.003
23. Hussain I, Shah T, Mahmood H et al (2011) Some analysis of S-box based on residue of prime number. Proc Pakistan Acad Sci 48:111–115
24. Ivanov G, Nikolov N, Nikova S (2016) Cryptographically strong S-boxes generated by modified immune algorithm. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics) 9540:31–42. https://doi.org/10.1007/978-3-319-29172-7_3
25. Javeed A, Shah T, Attaullah (2020) Design of an S-box using Rabinovich-Fabrikant system of differential equations perceiving third order nonlinearity. Multimed Tools Appl 79:6649–6660. https://doi.org/10.1007/s11042-019-08393-4
26. Jiang Z, Ding Q (2021) Construction of an s-box based on chaotic and bent functions Symmetry (Basel) 13. https://doi.org/10.3390/sym13040671
27. Johnson B (1997) Break the code: cryptography for beginners
28. Kim J, Phan RCW (2009) Advanced differential-style cryptanalysis of the NSA's skipjack block cipher. Cryptologia 33:246–270. https://doi.org/10.1080/01611190802653228

29. Kleist VF (2005) The code book: the science of secrecy from ancient Egypt to quantum cryptography [book review]
30. Kumar GS, Premalatha K (2021) Securing private information by data perturbation using statistical transformation with three dimensional shearing[formula presented]. Appl soft Comput 112. https://doi.org/10.1016/j.asoc.2021.107819
31. Lambić D (2017) A novel method of S-box design based on discrete chaotic map. Nonlinear Dyn 87:2407–2413. https://doi.org/10.1007/s11071-016-3199-x
32. Lambić D (2017) A novel method of S-box design based on discrete chaotic map. Nonlinear Dyn 87:2407–2413. https://doi.org/10.1007/s11071-016-3199-x
33. Lambić D (2018) S-box design method based on improved one-dimensional discrete chaotic map. J Inf Telecommun 1–11. https://doi.org/10.1080/24751839.2018.1434723
34. Lambić D, Živković M (2013) Comparison of random S-box generation methods. Publ l'Institut Math 93:109–115. https://doi.org/10.2298/PIM1307109L
35. Liu L, Zhang Y, Wang X (2018) A novel method for constructing the S-box based on spatiotemporal chaotic dynamics Appl Sci 8. https://doi.org/10.3390/app8122650
36. Lu Q, Zhu C, Wang G (2019) A novel S-Box design algorithm based on a new compound chaotic system Entropy 21. https://doi.org/10.3390/e21101004
37. Mohamed K, Hani Hj Mohd Ali F, Ariffin S et al (2018) An improved AES S-box based on Fibonacci numbers and prime factor. Int J Netw Secur 20:1206. https://doi.org/10.6633/IJNS.201811
38. Mroczkowski P (2009) Generating pseudorandom S-boxes – a method of improving the security of cryptosystems based on block ciphers. J Telecommun Inf Technol nr 2:74–79
39. Niemiec M, MacHowski L (2012) A new symmetric block cipher based on key-dependent S-boxes. Int Congr ultra mod Telecommun control Syst work 474–478. https://doi.org/10.1109/ICUMT.2012.6459712
40. Nizam Chew LC, Ismail ES (2020) S-box construction based on linear fractional transformation and permutation function Symmetry (Basel) 12. https://doi.org/10.3390/SYM12050826
41. Paar C, Pelzi J, Preneel B (2010) Understanding Crytography: a textbook for students and practitioners
42. Peng J, Jin S, Lei L, Jia R (2012) A novel method for designing dynamical key-dependent S-boxes based on hyperchaotic system. Int J Adv Comput Technol 4:282–289. https://doi.org/10.4156/ijact.vol4.issue18.33
43. Piper F, Murphy S (2002) Team-Fly cryptography: a very short introduction by Fred Piper and Sean Murphy Oxford University press © 2002 (142
44. Radhakrishnan SV, Subramanian S (2013) An analytical approach to s-box generation. Comput Electr Eng 39:1006–1015. https://doi.org/10.1016/j.compeleceng.2012.11.019
45. Ramzan M, Shah T, Hazzazi MM, Aljaedi A, Alharbi AR (2021) Construction of S-boxes using different maps over elliptic curves for image encryption. IEEE Access 9:157106–157123. https://doi.org/10.1109/ACCESS.2021.3128177
46. Rashidi B (2021) Lightweight 8-bit S-box and combined S-box/S-box−1 for cryptographic applications. Int J Circuit Theory Appl 49:2348–2362. https://doi.org/10.1002/cta.3041
47. Razaq A, Yousaf A, Shuaib U, Siddiqui N., Ullah A., Waheed A. (2017) A novel construction of substitution box involving Coset diagram and a bijective map. Secur Commun Networks 2017 https://doi.org/10.1155/2017/5101934
48. Razaq A, Al-Olayan HA, Ullah A, et al (2018) A Novel Technique for the Construction of Safe Substitution Boxes Based on Cyclic and Symmetric Groups Secur Commun Networks 2018. https://doi.org/10.1155/2018/4987021
49. Razaq A, Alolaiyan H, Ahmad M, Yousaf MA, Shuaib U, Aslam W, Alawida M (2020) A novel method for generation of strong substitution-boxes based on Coset graphs and symmetric groups. IEEE Access 8:75473–75490. https://doi.org/10.1109/ACCESS.2020.2989676
50. Razaq A, Ullah A, Alolaiyan H, Yousaf A (2021) A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers. Wirel Pers Commun 116:3165–3190. https://doi.org/10.1007/s11277-020-07841-x
51. Razaq A, Iqra AM et al (2021) A novel finite rings based algebraic scheme of evolving secure S-boxes for images encryption. Multimed Tools Appl 80:20191–20215. https://doi.org/10.1007/s11042-021-10587-8
52. Razaq A, Akhter S, Yousaf A, Shuaib U, Ahmad M (2022) A group theoretic construction of highly nonlinear substitution box and its applications in image encryption. Multimed Tools Appl 81:4163–4184. https://doi.org/10.1007/s11042-021-11635-z
53. Rukhin A, Soto J, Nechvatal J (2010) A statistical test suite for random and pseudorandom number generators for cryptographic applications. Nist spec Publ 22:1/1–G/1
54. Sarfraz M, Hussain I, Ali F Construction of S-Box Based on Mobius Transformation and Increasing Its Confusion Creating Ability through Invertible Function. Int J Comput Sci Inf Secur 14(2):187
55. Sathish Kumar G, Premalatha K, Aravindhraj N et al (2019) Secured cryptosystem using blowfish and RSA algorithm for the data in public cloud. Int J Recent Technol Eng 7:45–49

56. Shah T, Qamar A, Hussain I (2013) Substitution box on maximal cyclic subgroup of units of a galois ring. Zeitschrift fur Naturforsch - Sect A J Phys Sci 68:567–572. https://doi.org/10.5560/ZNA.2013-0021
57. Shahzad I, Mushtaq Q (2019) Razaq a (2019) construction of new S-box using action of quotient of the modular group for multimedia security. Secur Commun Networks 2019:1–13. https://doi.org/10.1155/2019/2847801
58. Si Y, Liu H, Zhao M (2023) Constructing keyed strong S-box with higher nonlinearity based on 2D hyper chaotic map and algebraic operation. Integration 88:269–277. https://doi.org/10.1016/j.vlsi.2022.10.011
59. Sohal AS, Sandhu R, Sood SK, Chang V (2018) A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput Secur 74:340–354. https://doi.org/10.1016/j.cose.2017.08.016
60. Tang G, Liao X (2005) A method for designing dynamical S-boxes based on discretized chaotic map. Chaos, Solitons Fractals 23:1901–1909. https://doi.org/10.1016/j.chaos.2004.07.033
61. Tang G, Liao X, Chen Y (2005) A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons Fractals 23:413–419. https://doi.org/10.1016/j.chaos.2004.04.023
62. Tran MT, Bui DK, Duong AD (2008) Gray S-box for advanced encryption standard. Proc - 2008 Int Conf Comput Intell Secur CIS 2008(1):253–258. https://doi.org/10.1109/CIS.2008.205
63. Wang Y, Xie Q, Wu Y, Du B (2009) A software for S-box performance analysis and test. In: proceedings - 2009 international conference on electronic commerce and business intelligence, ECBI 2009. Pp 125–128
64. Webster AF, Tavares SE (1986) On the Design of S-Boxes. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics) 218 LNCS:523–534. https://doi.org/10.1007/3-540-39799-X_41
65. Yi X, Cheng SX, You XH, Lam KY (1997) Method for obtaining cryptographically strong 8×8 S-boxes. Conf Rec / IEEE Glob Telecommun Conf 2:689–693. https://doi.org/10.1109/glocom.1997.638418
66. Zahid AH, Arshad MJ (2019) An innovative design of substitution-boxes using cubic polynomial mapping. Symmetry (Basel) 11. https://doi.org/10.3390/sym11030437
67. Zahid AH, Arshad MJ, Ahmad M (2019) A novel construction of efficient substitution-boxes using cubic fractional transformation. Entropy 21:1–13. https://doi.org/10.3390/e21030245
68. Zahid AH, Al-Solami E, Ahmad M (2020) A novel modular approach based substitution-box design for image encryption. IEEE Access 8:150326–150340. https://doi.org/10.1109/ACCESS.2020.3016401
69. Zahid AH, Tawalbeh L, Ahmad M et al (2021) Efficient dynamic S-box generation using linear trigonometric transformation for security applications. IEEE Access 9:98460–98475. https://doi.org/10.1109/ACCESS.2021.3095618
70. Zahid AH, Ahmad M, Alkhayyat A, Arshad MJ, Shaban MMU, Soliman NF, Algarni AD (2021) Construction of optimized dynamic S-boxes based on a cubic modular transform and the sine function. IEEE Access 9:131273–131285. https://doi.org/10.1109/ACCESS.2021.3113338
71. Zahid AH, Rashid H, Shaban MMU, Ahmad S, Ahmed E, Amjad MT, Baig MAT, Arshad MJ, Tariq MN, Tariq MW, Zafar MA, Basit A (2021) Dynamic S-box design using a Novel Square polynomial transformation and permutation. IEEE Access 9:82390–82401. https://doi.org/10.1109/ACCESS.2021.3086717
72. Zahid AH, Iliyasu AM, Ahmad M, Shaban MMU, Arshad MJ, Alhadawi HS, el-Latif AAA (2021) A novel construction of dynamic S-box with high nonlinearity using heuristic evolution. IEEE Access 9:67797–67812. https://doi.org/10.1109/ACCESS.2021.3077194
73. Zhu D, Tong X, Zhang M, Wang Z (2020) A new s-box generation method and advanced design based on combined chaotic system. Symmetry (Basel) 12:1–17. https://doi.org/10.3390/sym12122087