THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 1 (2024)
https://doi.org/ 10.62019/abbdm.v4i1.127.

An innovative design of substitution-box using Trigonometric-Multiplicative Functions Using Square Root Arguments: A Data-driven study

Syed Atir Raza*, Sadia Abbas Shah, Abdul Wahab, Maham Fatima

Chronicle

Article history

Received: February 23, 2024
Received in the revised format: March 13, 2024
Accepted: March 18, 2024
Available online: March 19, 2024

Syed Atir Raza is currently affiliated with the Department of Computer Science and Information Technology, University of Lahore, Lahore Pakistan.
Email: atir.raza@cs.uol.edu.pk

Sadia Abbas Shah is currently affiliated with the School of Computer Science, Minhaj University Lahore, Pakistan.
Email: sadiaabbas.cs@mul.edu.pk

Abdul Wahab and Maham Fatima are currently affiliated with the Department of Software Engineering, University of Lahore, Lahore Pakistan.
Email: abdul.wahab@se.uol.edu.pk
Email: maham.fatima@se.uol.edu.pk

***Corresponding Author:**

Abstract

In the evolving landscape of digital technology, the imperative for robust data security mechanisms has escalated, given the increasing sophistication of cyber threats. This abstract delineates a study focused on enhancing cryptographic defenses through the innovation of a Substitution box (S-Box), which is pivotal in the architecture of modern encryption algorithms. The proposed S-Box, deriving its foundation from chaotic maps integrated with trigonometric-multiplicative functions, represents a novel approach in cryptographic design, utilizing square root arguments to instigate dynamic characteristics. The evaluation of the proposed S-Box was methodically conducted using a comprehensive set of cryptographic benchmarks including Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), Linear Approximation Probability (LP), and Differential Approximation Probability (DP), to ascertain its defensive robustness against cryptanalytic attacks. The comparative analysis delineated in this study reveals that the cryptographic strength of the proposed S-Box transcends that of other contemporaneously designed S-Boxes thereby underscoring its potential applicability in real-world security scenarios. The findings of this research not only contribute to the theoretical underpinnings of cryptographic security but also have practical implications in the development of more secure digital environments fortifying data against unauthorized access and ensuring the integrity of confidential information in digital communications.

Keywords: Cryptographic Security, S-Box Optimization, Cyber Resilience, Encryption Algorithms.

INTRODUCTION

In our rapidly advancing world, technology continues to reshape our lives, introducing new tools and methods to streamline tasks and enhance efficiency. Each day heralds fresh innovations, but with progress comes a dual edge (Anitha, Nirmala, Ramesh, Tamilselvi, & Ramkumar, 2022)(Akkad, Wills, & Rezazadeh, 2023). Today's cutting-edge gadgets and systems, driven by the latest technology, generate an unprecedented volume of data (Anitha et al., 2022)(Akkad et al., 2023). Data communication serves as the essential conduit for information exchange and transmission among devices and networks. This pivotal role extends across diverse realms including business, education, entertainment, and beyond(Anitha et al., 2022). However, the surge in data also brings about heightened security concerns. Attackers, driven by motives ranging from financial

gain to personal curiosity or political interests, employ various tactics like hacking, phishing, malware, and social engineering to illicitly access sensitive information, underscoring the critical importance of robust cyber security measures(Mua'ad, Aldebei, & Alqadi, 2022)(Hofheinz & Kiltz, 2023). Safeguarding data from potential threats is paramount for both individuals and organizations. Heightened awareness and proactive measures are essential in mitigating the risks of data breaches and theft(E. A. Adeniyi, Falola, Maashi, Aljebreen, & Bharany, 2022)(Boobalan, Gunasekar, Thirumoorthy, & Senthil, 2023). Cryptography emerges as a powerful solution for data security, employing mathematical techniques to encrypt data, rendering it accessible to only those with the correct decryption key(E. A. Adeniyi et al., 2022). This ensures that the sensitive information remains impervious to interception and unauthorized access, bolstering data privacy and overall security. Additionally, cryptography serves as a means to verify data integrity, confirming its authenticity and ensuring it remains untampered during the transmission. Notable symmetric ciphers stand out for their efficiency and resource conservation compared to asymmetric counter parts., categorized into stream ciphers and block ciphers(A. E. Adeniyi et al., 2023)(Y. Zheng, Gao, & Wang, 2023).

To protect sensitive data, measures and protections that render it unreadable to potential attackers during transmission must be used(Sharma & Kawatra, 2022). Ciphers, roughly classified as stream ciphers and block ciphers, are used to accomplish this transformation(Kaur, Singh, Kaur, & Lee, 2022). Although slower than block ciphers, stream ciphers process data one bit or byte at a time(Qassir, Gaata, & Sadiq, 2022; Valea, Da Silva, Flottes, Di Natale, & Rouzeyre, 2019). They are useful in systems with limited computational resources, where efficiency is sacrificed (Atawneh, Layla, & Abutaha, 2020; Jassim & Farhan, 2021). Block ciphers, on the other hand, work on specified blocks of bits and are widely used in information security applications. AES, DES, Blowfish, RC2, RC5, and IDEA are well-known symmetric ciphers thanks to their simple implementation and easy deployment(Atawneh et al., 2020; Jassim & Farhan, 2021). Block ciphers use permutation and substitution procedures to convert plaintext (PT) into a cryptic arrangement known as ciphertext (CT), confusing potential attackers and strengthening data security. Permutation involves shifting data bits or bytes, whereas substitution includes replacing plaintext pieces with non-related counterparts(Hu & Zhao, 2019)(Rana, Mondal, & Kamruzzaman, 2023). To aid this critical step, prominent block ciphers use one or more substitution boxes (S-boxes) (Bhagat, Kumar, Gupta, & Chaube, 2023). An S-box is a critical component in current block ciphers, helping to generate elaborate ciphertext from plaintext(Heys, 2020)(Hamza & Kumar, 2020). Candid disorientation is a basic approach used to induce uncertainty within the S-box, generating a complex interaction between the plaintext and the resulting ciphertext.

The robustness of the cipher is directly related to the level of confusion introduced in the ciphertext, emphasizing the importance of this technique in guaranteeing robust data security(Chen et al., 2022)(Mahboob et al., 2022). The cryptographic robustness of the S-cryptographic box itself determines the efficacy of a block cipher employing an S-box(Khompysh, Kapalova, Algazy, Dyusenbayev, & Sakan, 2022). Extensive study has been conducted to generate high-quality S-boxes and evaluate their strength against known criteria such as nonlinearity, bijection, SAC(Khompysh et al., 2022), BIC, linear and differential probability(Y. Zheng et al., 2023). The dilemma of potential data security compromise in modern cryptographic systems underscores a significant challenge within

the realm of cybersecurity (Y. Zheng et al., 2023). At the heart of this issue is the vulnerability of modern ciphers to increasingly sophisticated cryptographic attacks(A. E. Adeniyi et al., 2023)(Y. Zheng et al., 2023). As the digital landscape evolves, so does the arsenal of tools available to cybercriminals, enabling them to exploit weaknesses in cryptographic algorithms, particularly the Substitution box (S-Box), a core component in cipher design. These vulnerabilities can lead to the decryption of sensitive information, thereby granting unauthorized access and compromising data integrity. The complexity of the problem is further exacerbated by the dynamic nature of cyber threats, which continuously adapt to countermeasures, necessitating a proactive and innovative approach to cipher design. Consequently, the development of an advanced S-Box, such as the one proposed in this study, is crucial. It aims to enhance the robustness of encryption methods, ensuring they remain several steps ahead of potential breaches. This proactive stance in cryptographic research is essential for establishing a secure digital environment, where data protection is paramount against the backdrop of an ever-evolving technological and threat landscape. Thus, addressing the issue of data security compromise in modern ciphers is not only a matter of enhancing current encryption methods but also a strategic imperative to safeguard digital information in the foreseeable future.

MOTIVATION

In the rapidly advancing digital era, where technological innovation outpaces cybersecurity measures, the motivation for the proposed S-Box is anchored in the critical need for enhanced data security. As cyber threats evolve in complexity and sophistication, traditional encryption methods are increasingly challenged, necessitating advanced cryptographic solutions to safeguard sensitive information. The proposed S-Box, engineered with chaotic maps and trigonometric-multiplicative functions, is a response to this exigency. It is designed to fortify encryption algorithms against the ingenuity of modern cyber-attacks, ensuring robust data protection in an ever-changing technological landscape. This initiative reflects a proactive approach to cybersecurity, aiming to stay ahead of potential vulnerabilities and secure digital assets against the backdrop of rapid technological evolution.

CONTRIBUTION

In this paper a novel S-box has been introduced named as Trigonometric-multiplicative Function with Square Root Argument. This essential component is critical in improving the cryptographic strength of block ciphers. The suggested S-box exhibits a thorough comprehension of cryptographic principles and demonstrates the author's proficiency in creating secure systems. This contribution is not only notable, but it also paves the way for future study and innovation in the field of information security. The results given here show promise for applications requiring comprehensive data protection in a variety of fields. S-Boxes, or substitution boxes play a crucial role in modern cryptographic systems by introducing non-linearity and confusion, enhancing the security of data encryption. In real-world applications, S-Boxes are extensively used in various scenarios such as secure communication protocols, financial transactions, digital signatures, and authentication mechanisms. For example, in secure communication, S-Boxes help encrypt sensitive data transmitted over networks, ensuring confidentiality and preventing unauthorized access. In financial transactions, S-Boxes are employed to encrypt transaction details, protecting

financial information from cyber threats and fraud. Additionally, S-Boxes are integrated into digital signatures and authentication systems to verify the authenticity of messages and users, safeguarding against identity theft and unauthorized access. Overall, S-Boxes are fundamental components of cryptographic protocols, providing essential security measures in a wide range of real-world applications where data confidentiality and integrity are paramount.

2 Proposed Approach For S-Box

The substitution box, which is used in symmetric block ciphers such as AES and DES, is a non-linear function that is critical for improving cipher security against differential and linear cryptanalysis. It is built by picking specific-length integers or binary strings for both the input and output areas, which strengthens the cipher's resilience against attacks. This smart S-box implementation strengthens the overall encryption process, offering strong data protection. The construction of s box involved the following steps

- Chaotic Map Design
- S-box Development
- Final S box generation

Chaotic Map Design

For the novel S-box construction we have merge the linear equation with the trigonometric functions and then passed square root argument. The novel aspects of chaotic maps stem from their intricate, non-linear dynamics, which are pivotal for generating cryptographic keys with high unpredictability. When integrated into S-Box design, chaotic maps bolster data encryption by introducing complex transformations that thwart statistical attacks, thus ensuring robust security measures in contemporary cryptographic systems. These innovative approaches leverage the inherent chaos of chaotic maps to enhance the resilience of cryptographic algorithms against various threats and vulnerabilities, contributing significantly to the advancement of information security. We have named this approach as "Trigonometric-Multiplicative Function With Square Root Argument". The chaotic map is generalized as:

$$X_n = \begin{cases} Sin(\pi - Xn) \\ \\ Cot\sqrt{(1 + Xn)} \end{cases} \quad (1)$$

Algorithm for the proposed s box is as

Algorithm for Initial S box

Step 1: Start
Step 2:
Initialize the Xn and range

Xn = 0.0
Range = 1.0
A<2<3
Initilize the array of 256
Size = 256, S[0]*size
Initialize Loc,Where Loc=0;

Step 3: Stop Condition
While Loc != 256:
Check Xn<0.5:
If Xn<0.5:
Xn= sin(pi – Xn)
else:
Xn = cot(math.sqrt(1+Xn)
Step 4:
Calculate V
V = int (Xn/1*10)Mod 256
If F[V]==0;
S[Loc]=V, F[V]=1 , Loc += 1
Stop

Bifurcation

In block ciphers, bifurcation refers to the process of separating the input space into two separate subsets, which influences the transformation of plaintext to ciphertext. This method improves cryptographic security by increasing the complexity of the encryption process. The S-box creates a higher degree of confusion by bifurcation, making it more resistant to cryptanalytic attacks. As evidenced by recent improvements in information security protocols, this critical idea serves a critical role in increasing the overall security of cryptographic systems(Y. Zheng et al., 2023). The bifurcation diagram of the proposed s box is shown in figure 1.

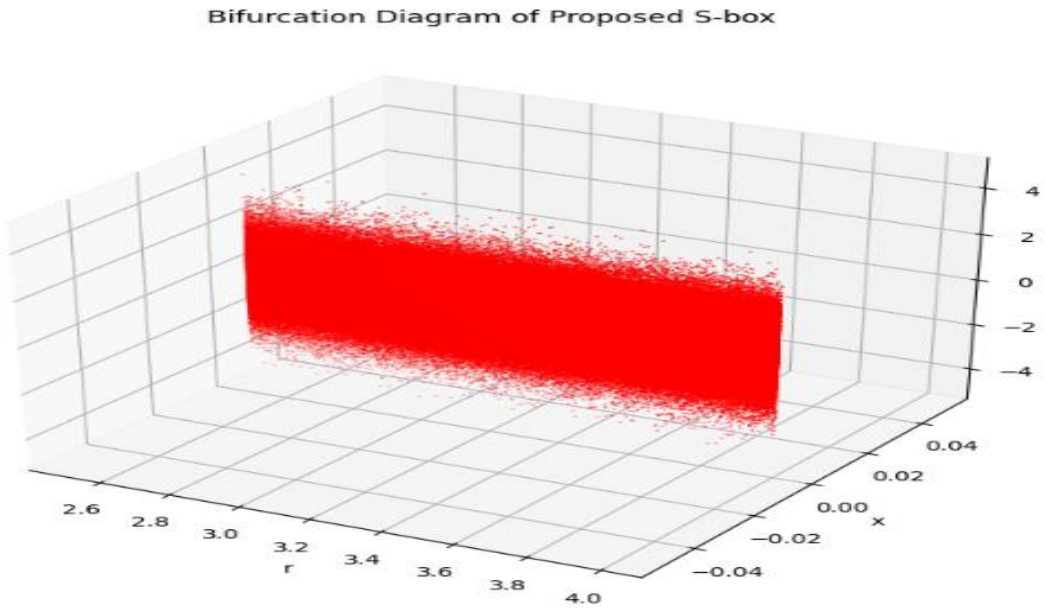

Figure 1.
Bifurcation diagram for our S-box

Lyapunov Exponent

The Lyapunov Exponent assesses a dynamic system's sensitivity to initial conditions. It analyzes how minor changes in input affect output in the setting of S-boxes, showing the extent of chaos or unpredictability. A higher Lyapunov Exponent indicates increased

complexity, which can improve cryptographic security by making it more tough for the attackers to predict the S-box's behavior(Atawneh et al., 2020; Jassim & Farhan, 2021). This metric can be used to assess the robustness of cryptographic algorithms that use S-boxes. It is calculated as shown in equation 2.

$$\lim_{t\to\infty}\frac{1}{t}\sum_{i=0}^{t-1} Log\frac{df}{dx}\ |x = xi\ | \qquad (2)$$

The Lyapunov exponent for the proposed S-box is as:

$$F'(Xn) = Log\frac{df}{dx}\sin(\pi - Xn) * Cot\left(\sqrt{1-xn}\right) \qquad (3)$$

The Lyapunov exponent for the proposed S-box is illustrated in figure 2.

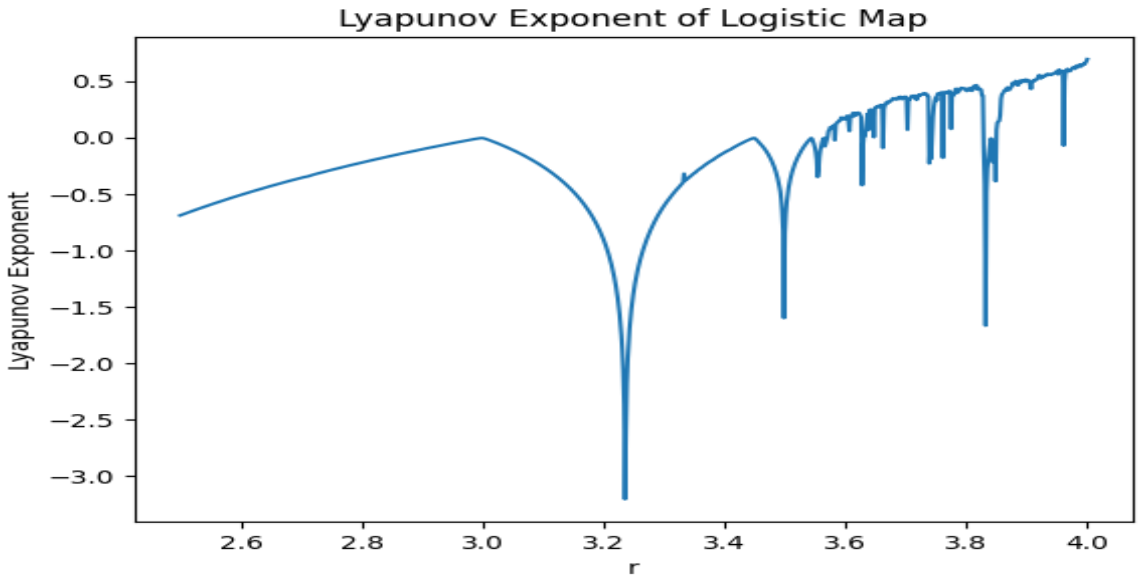

Figure 2.
Lyapunov Exponent for our S-box
The flowchart of the proposed S-box is as:

Novel Trignometric-Mulitplicative Function Method For Final S-box

The proposed chaotic map has been given a proposed chaotic map formula as given in the equation 1 to increase the robustness of the proposed S-box. The formula for final S box is given in equation 4. final look by making some amendments in the

$$X_n = (\sin(\pi - Xn) * \cot\left(\sqrt{(1+Xn)}\right) * H^2 MOD256 \qquad (4)$$

The construction of S box is shown in algorithm 2. In which we have use a Trigonometric-Multiplicative Function With Square Root Argument by taking H with a fixed value of large prime numbers in order to get an improved final S-box with high non-linearity. The unique aspect of this methodology lies in its integration of trigonometric functions with multiplicative operations, where square root arguments are employed to induce chaos in the S-Box design. This novel combination facilitates the generation of highly

unpredictable and complex patterns, essential for thwarting cryptographic attacks. Unlike conventional methods, which often rely on linear or simpler nonlinear processes, the proposed technique leverages the inherent complexity of trigonometric functions and their interactions with multiplicative elements to produce a dynamic, robust S-Box. This innovation not only increases the cipher's resistance to attacks but also ensures a higher level of security in encrypted communications, showcasing a significant leap forward in the field of cryptography. The working is also illustrated in flowchart as shown in figure 4.

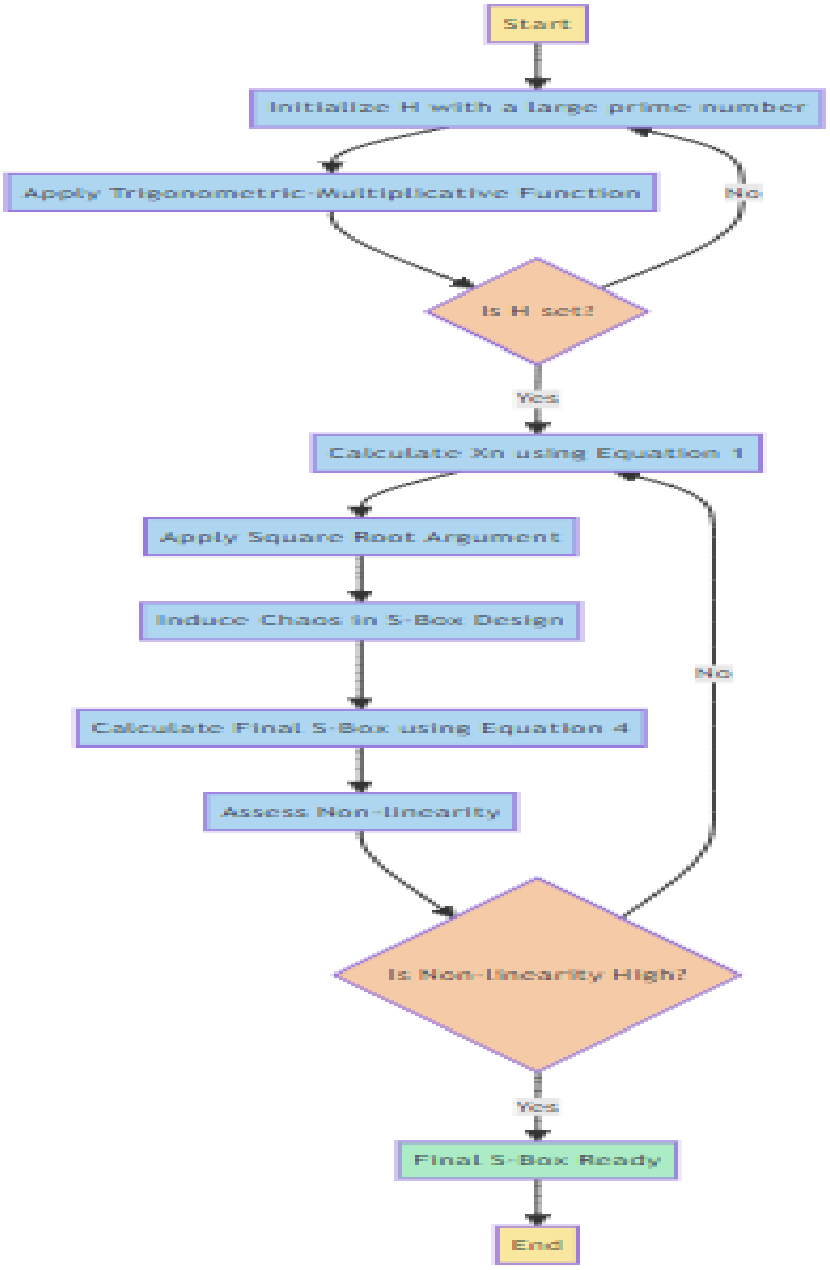

Figure 3.
Flowchart for Final S box

Algorithm for Final S box Generation

Step 1: Start
Step 2:
Initialize Xn and Range
Xn = 0.0
range = 1.0, F = 71059 , G = 71058
Initialize array of size 256
size = 256
S = [0] * size
Initialize Loc
Loc = 0
Step 3:
Stop condition
while Loc != 256:
  Check Xn < 0.5
  if Xn < 0.5:
    Xn = sin(pi-Xn) MOD256
  else:
    Xn = Cot(Sqrt(1+Xn))*H*H Mod256
Step 4:
Calculate V
  V = int(XnMoD256)

  Check if F[V] is equal to 0
  if F[V] == 0:
    S[Loc] = V
    F[V] = 1
    Loc += 1
Stop

Security Analysis of our S-box

The design of new S-boxes is a significant research contribution in the realm of data and information security. After designing an S-box, it is analyzed to determine its capabilities and strength against various attacks (Linear and Differential).

Evaluation of an S-box depends on the following predefined criteria.

- Non-Linearity of S box
- Fixed Points in S box
- Strict Avalanche effect (SAC) of S box
- Bit Independency Criterion of S box
- Linear Approximation Probability of S box
- Differential Approximation Probability (DP)

Non-Linearity

Nonlinearity is a critical parameter in assessing the performance of an S-box, as it measures the S-box's ability to resist linear and differential cryptanalysis attacks. These attacks attempt to exploit linear approximations of the S-box function to deduce key information. A high nonlinearity score indicates that the S-box effectively scrambles the input data, making it more difficult for attackers to establish linear relationships and

predict outcomes. Our proposed S-box boasts a nonlinearity of 128, signifying its strong capability to obfuscate the relationship between input and output, thus enhancing the overall security of the cryptographic system. This high level of nonlinearity is indicative of the S-box's robustness against cryptanalytic attacks, confirming its efficacy in secure encryption practices.

Table 1.
Non-Linearity Values of our S box

Boolean Function	R1	R2	R3	R4	R5	R6	R7	R8
Nonlinearity	128	128	116	128	128	128	116	128

Table 2.
Nonlinearity Comparison With Recent S-Boxes

S box	**Minimum**	**Maximum**	**Average**
Proposed	108	128	128.5
(Lu, Zhu, & Deng, 2020)	104	110	106.3
(Riaz & Siddiqui, 2020)	104	108	105.2
(Ibrahim et al., 2020)	104	110	108.0
(H. Zhu, Tong, Wang, & Ma, 2020)	106	108	106.8
(Lambić, 2020)	106	108	106.0
(Manzoor, Zahid, & Hassan, 2022)	108	112	110.0
(Jiang & Ding, 2021)	104	108	106.75
(Lambić, 2014)	112	114	112.25
(Zahid et al., 2021)	112	110	111.50
(Shafique, 2020)	104	110	107.0
(Ali & Ali, 2022)	104	108	108.2
(J. Zheng & Zeng, 2022)	108	100	104
(Liu, Liu, & Ma, 2022)	110	108	105
(Hematpour, Ahadpour, Sourkhani, & Sani, 2022)	96	108	102.2
(S. Zhu, Deng, Zhang, & Zhu, 2023)	104	110	106.0

Fixed Points

A fixed point in a substitution box (S-Box) occurs when an input value remains unchanged after encryption, meaning the output is identical to the input. In cryptographic terms, this is a vulnerability. If attackers capture cipher text and identify such fixed points, they can exploit this predictability to decipher or infer the original data, undermining the encryption's security. Therefore, the absence of fixed points in an S-Box is crucial to prevent such security breaches. In the context of the suggested S-Box, rigorous testing was conducted specifically to detect any fixed points, and the results confirmed their absence. This outcome is vital for the cryptographic robustness of the S-Box, ensuring that it provides a high level of security by eliminating predictable points that could be targeted by attackers to compromise the encrypted data(Atawneh et al., 2020; Jassim & Farhan, 2021).

Strict Avalanche Criterion

Tavares and Webster invented the Strict Avalanche Criterion (SAC). If a single input bit of a cryptographic function is changed, at least half of the output bits must likewise change, according to the criterion. A dependence matrix can be used to calculate the SAC value of an S-Box. The SAC dependency matrix of the proposed S-box is specified in Table

3. The recommended number for improved cryptographic uncertainty is 0.5 however our S-box is giving 0.52 which is near to ideal value. Figure 3 is comparing the SAC values of different S-Boxes to the proposed S-Box's SAC values. The chart clearly shows that the suggested S-Box's SAC Offset value is, which is extremely minimal, proving its suitability for usage in security-related applications.

0.4688	0.4844	0.5156	0.5625	0.4688	0.4688	0.4531	0.5313
0.5000	0.5156	0.5313	0.5313	0.5625	0.4844	0.4844	0.5156
0.4688	0.4844	0.5938	0.4688	0.5313	0.4688	0.5313	0.5313
0.4531	0.5313	0.4688	0.5313	0.4844	0.5000	0.4688	0.5000
0.5000	0.5313	0.4531	0.5156	0.5625	0.4844	0.5313	0.5000
0.5000	0.5469	0.4531	0.5313	0.4688	0.4375	0.5313	0.4844
0.4219	0.4688	0.4688	0.4688	0.5625	0.4844	0.5000	0.5000
0.5000	0.5000	0.5156	0.4844	0.4688	0.4219	0.5469	0.5313

Figure 4.
SAC MATRIX FOR PROPOSED S-BOX

Bit Independency Criterion

The Bit Independence Criterion (BIC), a concept introduced by Tavares and Webster. serves as a vital metric for gauging an S-Box's efficacy. This criterion emphasizes the need for output bits to change independently in response to modifications in the input bits, ensuring that each bit contributes uniquely to the overall security. In essence, BIC assesses the S-Box's ability to maintain unpredictability and resist certain forms of cryptanalysis. The performance of our proposed S-Box under this criterion is noteworthy, as evidenced by its BIC-Nonlinearity (BIC-NL) score of 107.56768, detailed in Table 4. This table not only presents the BIC-NL scores but also facilitates a comparative analysis with the SAC (Strict Avalanche Criterion) and BIC-NL values of other S-Boxes, underlining the robustness and superior performance of our proposed S-Box in maintaining bit independence and cryptographic strength.

Table 4.
Comparison of SAC and BIC values or proposed S box

S box	SAC	SAC offset	BIC NL
Proposed	0.5256	0.005	107.56
(Lu et al., 2020)	0.507	0.007	103.9
(Riaz & Siddiqui, 2020)	0.5000	0.000	104.2
(Ibrahim et al., 2020)	0..4977	0.002	104.1
(H. Zhu et al., 2020)	0.5101	0.010	106.25
(Lambić, 2020)	0.4990	0.001	104.29
(Jiang & Ding, 2021)	0.4995	0.001	104.57
(Lambić, 2014)	0.5034	0.003	103.8
(Zahid et al., 2021)	0.506	0.006	104.2
(Shafique, 2020)	0.4978	0.002	104.21
(Manzoor et al., 2022)	0.5042	0.004	110.6
(Ali & Ali, 2022)	0.498	0.000	104.0
(J. Zheng & Zeng, 2022)	0.598	0.006	103.3
(Liu et al., 2022)	0.510	0.003	104.67
(Hematpour et al., 2022)	0.50	0.006	106.57
(S. Zhu et al., 2023)	0.507	0.001	103.91

Differential Approximation Linear Probability

In 1990, Shamir and Biham introduced the differential cryptanalysis as a novel method for attacking the Data Encryption Standard (DES)(Biham & Shamir, 1991). All ciphers utilizing DES-style substitution and permutation techniques are vulnerable to this attack. To assess the strength of an S-Box against this attack, Differential Uniformity (DU) and Differential Probability (DP) values are employed.

$$DU = Max\ \Delta g\ \neq 0, \Delta y\ \ [\#\{g\ \in N | S(g) \oplus \mathrm{S}(\mathrm{g} \oplus \Delta \mathrm{g}) = \Delta y\}] \quad (5)$$

Where N donates all possible inputs.

Table 5 presents the Differential Uniformity (DU) outcomes for the specified S-Box, where the proposed S-Box demonstrates a DU value of 0.029, indicating its superior resistance to cryptanalysis attacks. Table 6 provides a comparative analysis of Differential Probability (DP) values among various S-Boxes.

Linear Approximation Probability

Matsui developed linear cryptanalysis in 1993 as a theoretical technique to attacking the Data Encryption Standard (DES). This is a cryptanalysis technique that applies to symmetric-key block ciphers and provides a linear approximation for each cipher. The Advanced Encryption Standard (AES) was developed by the National Institute of Standards and Technology (NIST) with the purpose of preventing linear and other related attacks. An S-Box with a low linear probability (LP) value is resistant to linear cryptanalysis assaults, while one with a high value is not.

The suggested S-Box has a very low LP value, demonstrating its efficiency against linear attacks. Table 5 shows a comparison of LP values across several S-Boxes.

Table 5.
LP and DP values Comparison of Different S boxes

S-Box	LP	DP
Proposed	0.135	0.0296
(Lu et al., 2020)	0.133	0.039
(Riaz & Siddiqui, 2020)	0.132	0.039
(Ibrahim et al., 2020)	0.132	0.046
(H. Zhu et al., 2020)	0.105	0.030
(Lambić, 2020)	0.125	0.039
(Jiang & Ding, 2021)	0.117	0.039
(Lambić, 2014)	0.133	0.039
(Zahid et al., 2021)	0.125	0.039
(Shafique, 2020)	0.133	0.039
(Manzoor et al., 2022)	0.085	0.039
(Ali & Ali, 2022)	0.133	0.039
(J. Zheng & Zeng, 2022)	0.132	0.0469
(Liu et al., 2022)	0.106	0.030
(Hematpour et al., 2022)	0.115	0.039
(S. Zhu et al., 2023)	0.130	0.039

Efficiency Analysis of our proposed S box

In order to observe the computational efficiency of the proposed S-box technique, a simulation was conducted using python google colabs on a Windows 10 system with a 8GB RAM and an Intel Core i7 7th generation CPU. The proposed method's computational

efficiency was evaluated for both the initial and final S-boxes. The creation of the final S-box relies on a novel and innovative approach to enhance the cryptographic strength of an initially generated S-box. The time complexity of 1000 different initial S-boxes was measured to determine the time required to generate the final S-box using various parameter values.

Table 6.
Differential uniformity Analysis of Our S box

6	6	6	8	6	6	8	6	6	6	8	4	6	6	6	4
6	8	6	8	6	6	6	6	8	8	6	6	8	6	6	8
6	14	6	6	6	8	6	6	8	6	6	8	8	6	6	6
6	6	6	8	6	6	6	8	8	6	8	8	6	8	8	8
6	8	6	6	6	6	8	6	8	8	6	6	6	8	6	8
6	8	6	6	6	6	6	6	8	8	6	8	12	8	6	6
8	6	6	6	8	6	8	6	12	8	8	14	6	6	8	14
8	6	6	6	6	6	6	6	8	6	6	6	6	6	6	6
6	6	6	6	6	8	6	6	6	8	6	6	6	8	8	8
6	8	6	8	6	6	8	6	6	6	6	6	6	6	8	6
8	6	8	6	6	8	8	6	8	8	6	6	8	8	6	8
8	6	8	6	6	8	8	6	6	6	6	8	6	8	6	10
6	6	6	6	6	6	6	6	6	6	6	4	8	8	6	6
8	6	6	6	6	8	6	10	6	8	6	6	12	8	8	6
6	6	6	8	8	6	8	6	6	4	6	6	6	6	6	6

Table 7.
Proposed S-Box

118	215	16	86	187	33	153	93	121	45	196	27	135	108	83	113
48	169	111	106	92	123	42	176	62	188	22	1	8	29	88	157
203	13	63	131	190	25	20	57	84	149	12	11	9	10	58	145
119	64	71	143	35	95	170	36	204	102	105	126	34	67	192	214
37	205	65	142	189	14	23	56	107	197	77	81	19	90	150	124
120	61	104	191	68	207	39	83	122	46	80	171	40	87	85	146
162	165	51	79	203	30	136	78	182	60	18	69	55	89	100	21
45	184	24	208	66	82	17	114	26	169	70	72	74	76	73	75
59	181	49	15	70	31	128	97	28	170	142	50	225	195	111	52
37	207	88	47	115	205	125	94	187	192	103	173	32	121	41	208
53	178	96	116	141	38	99	209	174	180	44	210	91	139	209	138
98	54	28	195	130	86	43	76	175	124	16	19	17	133	69	39
82	182	59	131	25	198	22	52	72	46	78	149	123	199	63	129
183	12	33	140	75	84	62	147	37	137	58	13	40	172	31	55
30	132	112	101	48	151	79	50	120	86	151	47	188	80	135	109
67	146	68	117	103	121	158	74	114	159	27	60	152	160	154	155

CONCLUSION

This paper presents a new approach for constructing a dynamic substitution box (S-box) that depends on the encryption key. The approach uses an innovative chaotic map generated using a trigonometric-multiplicative function with square root arguments, both

of which are dynamic and introduced for the first time. The values of the parameters used in these processes are determined by the encryption key, and a slight modification in the parameter values generates a new S-Box. Our subsequent exploration and comparison show that the proposed chaotic map has high chaotic complexity. We evaluate the cryptographic strength of the designed S-Box using standard criteria and compare its performance with other substitution boxes based on chaotic maps. Our results demonstrate that the proposed S-Box is suitable for cryptographic applications.

LIMITATIONS

While our innovative design of a substitution box using Trigonometric-Multiplicative Functions with Square Root Arguments demonstrates promising results, several limitations warrant consideration. Firstly, the computational complexity of the proposed algorithm may increase with larger key sizes or input data, potentially impacting performance in resource-constrained environments. Secondly, the security analysis primarily focuses on traditional cryptographic metrics, and further evaluation against advanced attacks like machine learning-based techniques could provide deeper insights into its robustness. Additionally, the scalability of our approach concerning integration into larger cryptographic frameworks and compatibility with diverse platforms requires thorough investigation.

FUTURE WORK

Future research endeavors will focus on addressing the identified limitations and expanding the scope of our innovative S-Box design. This includes optimizing the algorithm for improved computational efficiency without compromising security, exploring alternative chaotic map formulations for enhanced non-linearity, and conducting comprehensive evaluations against advanced cryptanalysis methods. Moreover, extending the application of our S-Box design to different cryptographic protocols and evaluating its performance in real-world scenarios will be pivotal. Collaborative efforts with experts in machine learning and artificial intelligence will also be pursued to assess its resilience against evolving cyber threats and enhance its applicability in next-generation cryptographic systems.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally to the creation of this work.

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

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Adeniyi, A. E., Abiodun, K. M., Awotunde, J. B., Olagunju, M., Ojo, O. S., & Edet, N. P. (2023). Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach. *Multimedia Tools and Applications*, 1–15.

Adeniyi, E. A., Falola, P. B., Maashi, M. S., Aljebreen, M., & Bharany, S. (2022). Secure sensitive data sharing using RSA and ElGamal cryptographic algorithms with hash functions. *Information*, *13*(10), 442.

Akkad, A., Wills, G., & Rezazadeh, A. (2023). An information security model for an IoT-enabled Smart Grid in the Saudi energy sector. *Computers and Electrical Engineering*, *105*, 108491.

Ali, T. S., & Ali, R. (2022). A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box. *Multimedia Tools and Applications*, *81*(15), 20585–20609.

Anitha, G., Nirmala, P., Ramesh, S., Tamilselvi, M., & Ramkumar, G. (2022). A Novel Data Communication with Security Enhancement using Threat Management Scheme over Wireless Mobile Networks. *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, 1–6. IEEE.

Atawneh, B., Layla, A.-H., & Abutaha, M. (2020). Power consumption of a chaos-based stream cipher algorithm. *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, 1–4. IEEE.

Bhagat, V., Kumar, S., Gupta, S. K., & Chaube, M. K. (2023). Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. *Concurrency and Computation: Practice and Experience*, *35*(1), e7425.

Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, *4*, 3–72.

Boobalan, P., Gunasekar, K., Thirumoorthy, P., & Senthil, J. (2023). An Introduction to Deepfakes on Cryptographic Image Security. In *Handbook of Research on Advanced Practical Approaches to Deepfake Detection and Applications* (pp. 72–81). IGI Global.

Chen, S., Fan, Y., Sun, L., Fu, Y., Zhou, H., Li, Y., … Guo, C. (2022). SAND: an AND-RX Feistel lightweight block cipher supporting S-box-based security evaluations. *Designs, Codes and Cryptography*, 1–44.

Hamza, A., & Kumar, B. (2020). A review paper on DES, AES, RSA encryption standards. *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, 333–338. IEEE.

Hematpour, N., Ahadpour, S., Sourkhani, I. G., & Sani, R. H. (2022). A new steganographic algorithm based on coupled chaotic maps and a new chaotic S-box. *Multimedia Tools and Applications*, *81*(27), 39753–39784.

Heys, H. M. (2020). A Tutorial on the Implementation of Block Ciphers: Software and Hardware Applications. *Cryptology EPrint Archive*.

Hofheinz, D., & Kiltz, E. (2023). Scalable Cryptography. In *Algorithms for Big Data: DFG Priority Program 1736* (pp. 169–178). Springer.

Hu, X., & Zhao, Y. (2019). Block ciphers classification based on random forest. *Journal of Physics: Conference Series*, *1168*(3), 32015. IOP Publishing.

Ibrahim, S., Alhumyani, H., Masud, M., Alshamrani, S. S., Cheikhrouhou, O., Muhammad, G., … Abbas, A. M. (2020). Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps. *Ieee Access*, *8*, 160433–160449.

Jassim, S. A., & Farhan, A. K. (2021). A survey on stream ciphers for constrained environments. *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, 228–233. IEEE.

Jiang, Z., & Ding, Q. (2021). Construction of an S-box based on chaotic and bent functions.

Symmetry, *13*(4), 671.
Kaur, S., Singh, S., Kaur, M., & Lee, H.-N. (2022). A systematic review of computational image steganography approaches. *Archives of Computational Methods in Engineering*, 1–23.
Khompysh, A., Kapalova, N., Algazy, K., Dyusenbayev, D., & Sakan, K. (2022). Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information. *Cogent Engineering*, *9*(1), 2080623.
Lambić, D. (2014). A novel method of S-box design based on chaotic map and composition method. *Chaos, Solitons & Fractals*, *58*, 16–21.
Lambić, D. (2020). A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. *Nonlinear Dynamics*, *100*(1), 699–711.
Liu, H., Liu, J., & Ma, C. (2022). Constructing dynamic strong S-Box using 3D chaotic map and application to image encryption. *Multimedia Tools and Applications*, 1–16.
Lu, Q., Zhu, C., & Deng, X. (2020). An efficient image encryption scheme based on the LSS chaotic map and single S-box. *IEEE Access*, *8*, 25664–25678.
Mahboob, A., Asif, M., Siddique, I., Saleem, A., Nadeem, M., Grzelczyk, D., & Awrejcewicz, J. (2022). A novel construction of substitution box based on polynomial mapped and finite field with image encryption application. *IEEE Access*, *10*, 119244–119258.
Manzoor, A., Zahid, A. H., & Hassan, M. T. (2022). A new dynamic substitution box for data security using an innovative chaotic map. *IEEE Access*, *10*, 74164–74174.
Mua'ad, M., Aldebei, K., & Alqadi, Z. A. (2022). Simple, efficient, highly secure, and multiple purposed method on data cryptography. *Traitement Du Signal*, *39*(1), 173–178.
Qassir, S. A., Gaata, M. T., & Sadiq, A. T. (2022). Modern and Lightweight Component-based Symmetric Cipher Algorithms. *ARO-THE SCIENTIFIC JOURNAL OF KOYA UNIVERSITY*, *10*(2), 152–168.
Rana, S., Mondal, M., & Kamruzzaman, J. (2023). RBFK cipher: a randomized butterfly architecture-based lightweight block cipher for IoT devices in the edge computing environment. *Cybersecurity*, *6*(1), 1–19.
Riaz, F., & Siddiqui, N. (2020). Design of an efficient cryptographic substitution box by using improved chaotic range with the golden ratio. *International Journal of Computer Science and Information Security (IJCSIS)*, *18*(1), 89–94.
Shafique, A. (2020). A new algorithm for the construction of substitution box by using chaotic map. *The European Physical Journal Plus*, *135*(2), 194.
Valea, E., Da Silva, M., Flottes, M.-L., Di Natale, G., & Rouzeyre, B. (2019). Stream vs block ciphers for scan encryption. *Microelectronics Journal*, *86*, 65–76.
Zheng, J., & Zeng, Q. (2022). An image encryption algorithm using a dynamic S-box and chaotic maps. *Applied Intelligence*, *52*(13), 15703–15717.
Zheng, Y., Gao, J., & Wang, B. (2023). New Quantum Search Model on Symmetric Ciphers and Its Applications. *Cryptology EPrint Archive*.
Zhu, H., Tong, X., Wang, Z., & Ma, J. (2020). A novel method of dynamic S-box design based on combined chaotic map and fitness function. *Multimedia Tools and Applications*, *79*, 12329–12347.
Zhu, S., Deng, X., Zhang, W., & Zhu, C. (2023). Secure image encryption scheme based on a new robust chaotic map and strong S-box. *Mathematics and Computers in Simulation*.