Egyptian Informatics Journal 29 (2025) 100620

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full Length Article

IoT enabled data protection with substitution box for lightweight ciphers

K.B. Sarmila [a,*], S.V. Manisekaran [b]

[a] Department of Computer Science and Engineering, Sri Eshwar College of Engineering Coimbatore Tamil Nadu India
[b] Department of Information Technology, Anna University Regional Campus Coimbatore Tamil Nadu India

ARTICLE INFO

Keywords:
DAC
Constrained devices
Lightweight cryptography
Chaotic behavior
IoT

ABSTRACT

Rapid growth in communication and networking demands the protection of highly sensitive data in the system. The cryptographic techniques used in various traditional devices and cloud environments are not applicable to resource-constrained devices like sensors, industrial controllers, and RFID tags. A lightweight cryptographic design is required for securing the data revolving around constrained devices. Symmetric block cipher techniques shaped using substitution-permutation network (SPN) structure use the powerful component, the substitution box, which is the only component that contributes to non-linearity. In this paper, a modified 5-bit Dynamic Airy Chaotic (DAC) substitution box is proposed, which uses tent-logistic mapping for obtaining confusion property. This chaotic behavior is incorporated with an improved and crafted logical function. The substitution box exhibits high dynamic chaotic behavior and maintains the structure, balancing the composition of good security strength and resource utilization. The chaotic behavior and security resistance are evaluated based on the standard parameters. The DAC substitution box demonstrates improved security with 66% less memory footprint on an average gate count compared with standard 4- and 5-bit competitors. The solution was able to obtain equally good resistance against differential attacks and increased resistance against linear attacks with 40% less linear probability value in comparison with its competitors. With the increased bit length of 5, it is observed that DAC exhibits excellent flexibility with traditional block cipher techniques, thus simplifying the use of such a solution as a building block of cryptographic primitives.

1. Introduction

Lightweight ciphers are extensively used in securing data in resource-constrained applications. Devices involved in these applications communicate using the sensitive data revolving around the network. The number of vulnerabilities in various stages of data around the network is explained in [32], denoting the importance of securing data. The security requirements are mainly categorized into confidentiality, integrity, and availability. The symmetric key cryptographic method and classification as described in [1] are classified as a hash function for authentication, confidentiality, and forward secrecy are achieved using block and stream cipher. The process of data protection using the block cipher technique can be structured by adopting one of the six sub-structures shown in Fig. 1. Among the six sub-structures, the substitution technique used in the SPN structure is focused on in this work, with a discussion on previous works on the structuring of substitution boxes and the design and development of 5-bit substitution boxes and their dynamic chaotic behavior (DCB).

A significant challenge for a cryptographic algorithm designer is ensuring adequate security. Claude Shannon (1949) introduced modern cryptography, specifying that confusion and diffusion are the parameters for a good cryptographic structure. A good substitution box is a primitive cryptographic component involved in the block cipher technique, enabling non-linearity and strengthening the cryptographic algorithms, enabling parameter confusion in cryptographic algorithms. Various substitution box construction methods explained in [2] were constructed based on the substitution box used in the AES algorithm, which is a traditional cryptographic algorithm widely used in data security in cloud environments and on traditional devices. There are various approaches used in the substitution box construction, like the heuristic approach illustrated in [3], the Boolean function demonstrated in [4], the linear fractional transformation in [5], the algebraic techniques demonstrated in [6], and the analytical approach demonstrated in [7]. There are many substitution boxes constructed with different input lengths (ranging from 3 bits to 8 bits) based on the application. A 4-bit substitution box has been developed with 2^4 elements, represented

* Corresponding author.
E-mail address: sarmilakb@gmail.com (K.B. Sarmila).

https://doi.org/10.1016/j.eij.2025.100620
Received 5 March 2024; Received in revised form 8 July 2024; Accepted 28 January 2025
Available online 31 January 2025

in hexadecimal format. The random-like behavior of this substitution box is used in the Data Encryption Standard illustrated in [7]. Similarly, for an 8-bit substitution box, 2^8 elements are structured to form non-linearity, which is employed in the Advanced Standard Encryption (AES) cryptographic technique. Based on the length of the substitution box, the increased length strengthens the ciphers to be resistant against attacks. The 8-bit substitution box is more resistant compared to the 4-bit substitution box. Three innovative architectures for substitution boxes (S-boxes) in lightweight block ciphers were proposed in [8,17]. These architectures offer significant improvements, including a 66 % reduction in utilization of energy as well as a 36 % reduction in delay and power metrics.

1.1. Problem statement

Finding lightweight encryption methods with strong security and efficient performance has been difficult. Current S-box design methods fail to resist linear and differential cryptanalysis (LC and DC respectively). These problems cast doubt on lightweight encryption's security. The tent-logistic mapping method can increase the chaotic range of S-boxes, improving cryptographic strength [15]. In S-box design, essential characteristics, including computational performance cost and security strength, must be balanced [21]. Therefore, the task is to propose a new strategy that achieves the following goals:

- The suggested method must greatly strengthen S-boxes against linear and differential cryptanalysis to protect cryptographic algorithms from severe attacks.
- While improving security, the strategy should consider computing resources and performance overhead to implement lightweight encryption algorithms efficiently in resource-constrained contexts.
- The tent-logistics mapping method should be smoothly integrated into the S-box design to maximize chaotic range and security.
- A fine balance between security strength and performance cost should be struck, as over-security may make encryption unsuitable for real-world applications.

This problem statement requires a new S-box design method to bridge the gap between lightweight encryption and the growing demand for increased security in the face of advanced cryptographic attacks. The solution to this challenge could improve lightweight cryptography and application security in resource-constrained contexts.

1.2. Motivation

According to the documentation of Google Adiantum (Storage Encryption), which uses AES for achieving encryption, most Android devices adopt AES as it uses ARMv8, but to provide cost-efficiency the ARM Cortex-A7 is used in manufacturing, which requires a lightweight solution to provide the security of the data involved. In [33], the need for a lightweight solution to suit IoT devices is explained. Similarly, various IoT applications require this lightweight solution as they use resource-constrained devices. A few researchers adopted the chaotic mapping method in substitution box constructions and it was summarized by Goudarzi, et. Al., [15]. Evaluation of popular methods shows that to yield better tradeoff between overall performance and complexity, there is a need for the design and development of a lightweight weight solution with an effective substitution box. Dynamic chaotic sequences are used in cryptography to create secure encryption systems that can withstand attacks. Chaotic systems are desirable for cryptography because they are unpredictable and sensitive to initial conditions. Information security researchers study them because of their sensitivity to beginning conditions, nonlinearity, and complicated dynamics, which make them better than typical cryptographic methods.

Key reasons and benefits of dynamic chaotic sequences in cryptography:

- Chaotic systems produce pseudorandom sequences.
- The beginning conditions and governing equations of the chaotic system can be used to reproduce these deterministic sequences.
- They can generate encryption keys and nonces since they appear random to an observer without this information.
- Chaotic systems are very sensitive to initial conditions. A tiny starting state change can modify the sequence dramatically.
- Even a little change in cryptographic parameters produces a different encryption key, making it difficult for attackers to predict or duplicate the key.
- Chaotic sequence cryptographic systems are more resistant to attacks because they need advanced mathematical and computational methods to analyze and break them.

The proposed new 5-bit DAC substitution box is a Boolean decomposition using a crafted logical combination motivated by GIFT-based chaotic mapping suitable for application-specific integrated circuits (ASIC). The chaotic mapping method is incorporated into the construction of the substitution box. This method is involved due to its authentic parameters like randomness and sensitivity to changes, which improve the strength with increased confusion in the cipher. The increased confusion increases the time complexity of the attack, making it resistant to unforeseen security issues. The effectiveness of proposed substitution boxes based on their resistance to attacks and execution cost is demonstrated.

The contributions to this solution are:

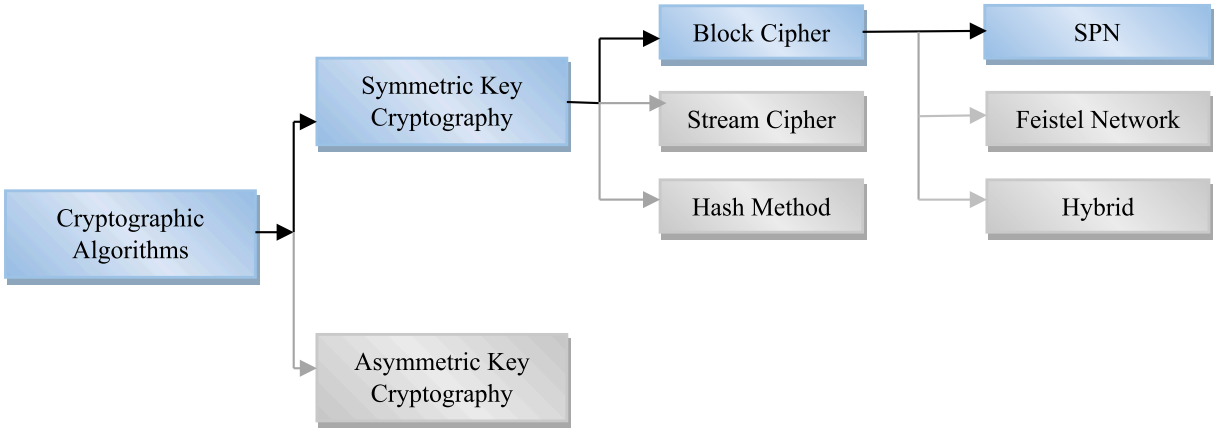

Fig. 1. Overview of structure-based classification techniques for cryptography.

(i) A comparison of various substitution box construction methods and their flexibility in application to block cipher techniques is discussed.
(ii) A new 5-bit substitution box with dynamic and chaotic behavior based on the cryptographic properties is structured.
(iii) The resistance is calculated based on the entropy analysis of the chaotic system, the avalanche property, boomerang uniformity, bit independence analysis, bijective property, differential probability, and linear probability, which are the traditional and most significant attacking techniques.

The paper is further designed with a comprehensive analysis of the characteristic features of various popular s-box based methodologies are discussed briefly in Section 2. In Section 3, the proposed functional block used in the new solution, a 5-bit DAC substitution structure is explained. Results and discussions based on the resilience property of the DAC system are provided and the performance analysis based on simulation results of the DAC system is presented in Section 4. In Section 5, the security analysis based on the complexity of the DAC system is discussed. In Section 6, the paper is concluded with suggestions for future directions.

2. Related works

Given the significance of substitution boxes in SPN networks, the architecture of substitution structures with robust cryptographic performance is the main objective of designing a cryptosystem. This section steps in with a discussion of various substitution box techniques proposed earlier with their advantages and limitations, followed by the design strategies adopted from the existing solutions to improve the balance between resource utilization and security strength.

Substitution box construction methods, as discussed in [1,9], follow various approaches to randomly transform the input bits to obtain a cipher. In general, the chaotic system is applied in the construction of a substitution box. There are various substitution boxes with varying input sizes, like 3, 4, 5, 6, and 8 (measured in bit units). Most of the cipher techniques using substitution and permutation networks choose 4-bit and 8-bit substitution boxes, which suit better for software

Table 1
Various lightweight encryption techniques with different substitution box lengths, advantages, and disadvantages.

Lightweight encryption techniques	Key length	Block size	S-box length	Advantages	Disadvantages
PRINT [27]	80/160	48/96	3-bit	• This technique occupies a very little memory footprint. • Less computational power is suitable for RFID tags.	• The 3-bit length of the substitution box with 2^3 possibilities. • It is easily victimized by attacks.
PYJAMASK – 96 [15]	128	96	3-bit	• This technique occupies a very little memory footprint • Less computational power is suitable for RFID tags.	• The 3-bit length of the substitution box with 2^3 possibilities. • It is easily victimized by attacks.
PYJAMASK – 128 [15]	128	128	4-bit	• This technique is a standard lightweight solution adopted by many other solutions. • Efficient in security with a smaller memory footprint and an increased count of rounds.	• It is vulnerable to differential attacks.
PRESENT [23]	80/128	64	4-bit	• This technique adopts the PRESENT strategy with a reduced number of rounds. • This replicates AES with reduced functionalities.	• It is more vulnerable to various cyberattacks. • Vulnerable in the 19th round.
RECTANGLE [24]	80/120	64	4-bit	• This uses 6 to 7 times less memory than AES and PRESENT. • Low critical path delay is used in designing these efficient blocks.	• Less secure against related key attacks. • 128-bit block sizes are more power-consuming than 64-bit block sizes.
PRINCE [11]	128	64	4-bit	• Hummingbird-2 is suitable for passive RFID tags as it consumes low power for implementation. • Produces message authentication code.	• Command decoding and processing a prerequisites for implementation. This additional processing is an overhead.
HUMMINGBIRD – 2 [25]	256	16	4-bit	• It is resistant to related key attacks. • Provides good software performance.	• The wire load model used in implementation occupies a high memory footprint.
LED [28]	80	64	4-bit	• Provides an extremely small footprint. • Resistant against known plaintext and key attacks.	• Analysis becomes difficult on increasing the key size to more than 64-bit.
KLEIN [26]	80	64	4-bit	• It consumes less power and memory area. • Ciphers are protected against known plaintext and key attacks. • Resistant against Biclique, MITM.	• Side-channel Attacks are not focused.
ANU-II [24]	80/128	64	4-bit	• It performs well balanced with software and hardware implementation.	• It exhibits low non-linearity. • Key schedules can be retrieved using a meet-in-middle attack.
TWINE [19]	80/128	64	4-bit	• This technique occupies very little memory footprint. • Less computational power, suitable for resource-constrained devices like RFID tags.	• The 3-bit length of the substitution box with 2^3 possibilities. • It is easily victimized by attacks.
FIDES [22]	80/96	160/ 192	5-bit	• Less memory footprint than Hummingbird-2 and Grain-128a. • Efficient throughput and latency	• Flexibility in block cipher implementation is difficult.
ASCON [18]	128	64	5-bit	• Resistant against implementation attacks, and side-channel attacks.	• Theoretically makes substitution boxes vulnerable to algebraic attacks.
DESL/DESXL [2 16]	184	64	6-bit	• More secure with key whitening features.	• Flexibility in block cipher implementation is difficult.
AES [20]	128/ 192/ 256	128	8-bit	• AES outperforms both versions of PRESENT by approximately 25%. Less energy consumption.	• More vulnerable to attacks.
ICEBERG [22]	128	64	8-bit	• It is a fast cipher technique.	• Requires high memory area, not suitable for low-powered devices.

implementations, as most of the cipher techniques use either 64-bit or 128-bit blocks. Table 1 lists various lightweight encryption algorithms using substitution and permutation network structures and the length of the substitution box considered.

Various encryption techniques with different substitution box designs and masking structures work well, with some challenges to be addressed. The structures involved in the 3-bit substitution box architecture are suitable for resource-constrained devices and provide a simple solution for small devices occupying low-circuit areas, but the technique remains vulnerable to attacks due to the small length substitution box. The 4-bit substitution box structure is highly used in lightweight cryptography with resistance towards traditional attacks and occupies less memory footprint but with low security. The 5-bit substitution box is more resistant to attacks than the 4-bit substitution box, but implementation is more flexible with even-numbered bit length. Both 6 and 8-bit substitution structures are highly resistant and provide good security compared to all other substitution structures. 8-bit substitution structure is widely used in the standard encryption technique, enabling integrity and non-linearity, but does not suit resource-constrained applications due to high resource utilization on computation. A comprehensive analysis is shown in Table 2, which offers a more elaborate rationale for selecting a 5-bit substitution box as opposed to the more prevalent 4-bit or 6-bit alternatives [15]. This justification is substantiated by theoretical arguments and the potential advantages that can be derived from this choice.

Table 2
Comparing the advantages of a 5-bit substitution box to those of more prevalent 4-bit and 6-bit variations [2,11,3,13,19,20,23–28].

Criteria for Bit Length Choice	4-Bit Substitution Box	5-Bit Substitution Box	6-Bit Substitution Box
Adaptability to block sizes	Limited adaptability to block sizes of different lengths.	Offers a balance between adaptability and security. Can be used with various block sizes, enhancing flexibility.	Less adaptable to block sizes outside the chosen 6-bit range.
Congruency with existing standards	Aligns well with existing standards that use multiples of 4 bits (e.g., byte alignment).	Moderately aligned with standards, slightly deviating from 4-bit multiples. May require slight adjustments in some cases.	Less congruent with existing standards, potentially necessitating more substantial modifications for integration.
Security strength	Provides basic security but may have limitations when facing advanced cryptographic attacks.	Strikes a balance between security and computational efficiency. Offers enhanced security strength than 4-bit S-boxes.	Offers a higher range of security but may come at the cost of increased complexity and computational overhead.
Resource utilization	Efficient in terms of resource usage due to smaller bit length.	Slightly higher resource usage than 4-bit S-boxes but remains efficient.	Potentially higher resource consumption due to larger bit length.
Resistance to cryptanalysis	May exhibit vulnerabilities in the face of certain cryptographic attacks, requiring additional security measures.	Enhances resistance to various cryptographic attacks, providing better overall security.	Offers strong resistance to some attacks but may introduce complexity that requires careful analysis.
Cryptographic primitives	Well-suited for simple cryptographic primitives but may lack the strength required for advanced ciphers.	Provides a versatile foundation for cryptographic primitives, allowing for a broader range of applications.	Offers room for more complex cryptographic primitives but may introduce computational overhead.
Implementation flexibility	Offers simplicity and ease of implementation, suitable for resource-constrained environments.	Balances security and implementation complexity, accommodating diverse hardware and software environments.	Provides flexibility for advanced cryptographic techniques but may be less straightforward to implement efficiently.

3. A new DAC system – proposed substitution box

The evaluation of popular methods discussed in section 2 shows that to yield a better trade-off between overall performance and complexity, there is a need for the design and development of a DAC substitution box (Dynamic Airy Chaotic S-Box). A comprehensive picture of the design convention of the DAC substitution box is discussed. This design is suitable for lightweight cryptographic techniques. The substitution box is structured with a 5-bit input being substituted with a unique 5-bit output. The structure of the substitution box is based on the dynamic chaotic sequence property with a Boolean function. There are various dynamic chaotic sequence approaches involved in non-linear mapping, they are logistic mapping, tent mapping, henon mapping, and quadratic mapping. The proposed solution uses tent-logistic chaotic mapping along with Boolean functions.

The proposed strategy follows two steps. The first step involves applying the chaotic sequence technique to obtain an intermediate substitution box. The second step, followed by the substitution of the result obtained in the previous step, uses the Boolean function to produce the output bits. The 5-bit input creates room for 2^n values in the substitution box. 'n' denotes the input vector length. The 5-bit substitution box can hold 32 unique values in the table for transformation.

3.1. Step 1- tent-logistic chaotic mapping

The chaotic mapping methods provide wilder behavior than continuous equations [10,12] his dynamic behavior imposes a higher rate of confusion, strengthening the cryptographic solution. The logistic map is a one-dimensional map with a mathematical function used to obtain highly chaotic behavior. The substitution box constructed based on a logistic map is defined by Equation (1)

$$s(n+1) = r^{*}s(n)^{*}(1-s(n)) \tag{1}$$

where 's' the control parameter ranging from 0 to 4. The system performance is chaotic if it is positive. Various ranges of parameters from 0 are experimented with Lyapunov exponent calculation. The Lyapunov exponent can be calculated by analytic or numeric approaches. In this paper, the analytic approach is demonstrated as in Equation (2)

$$m = \lim_{n\to\infty}\left(\frac{1}{n}\right)\ln[f(s(n))] \tag{2}$$

where 'm' denotes the Lyapunov exponent, $f(s(n))$ is the derivative of the substitution box at iteration. However, this analytic method is not feasible for larger systems. It is preferred in this case as it is used in the generation of a 5-bit substitution box. The chaotic behavior of the logistic map is illustrated in Fig. 2, using the bifurcation diagram. The complexity of the system increases only within 3.5 to 4, the state distribution is shown in Fig. 6a for $r = 3.9$. The chaotic behavior is obtained only for a few random values and within a shorter range. This characteristic makes this system unsuitable for cryptographic solutions as it provides a small key space.

Similarly, the tent map also exhibits randomness in a very short range from 0 to 2, and the methods exhibit a uniform distribution of

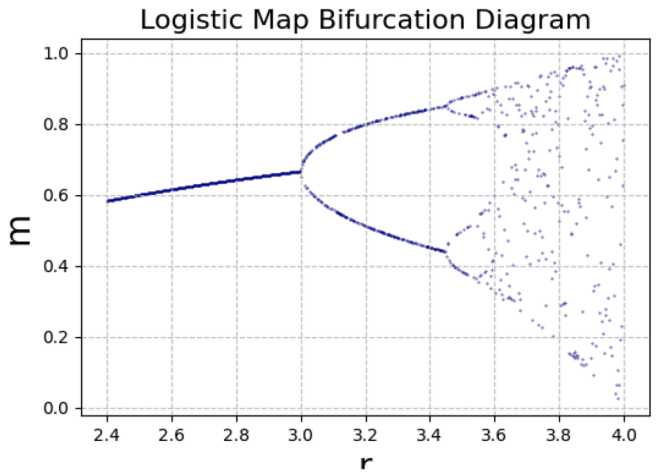

Fig. 2. Logistic map - bifurcation diagram for $r \in \{0, 4\}$, with 10000 iterations.

randomness. Thus, a hybrid method, the Tent-Logistic method is used with increased randomness and exhibits randomness from the range 0 to 9. Thus, providing a dynamic solution for substitution box construction.

3.2. Step 2 – composition of the logical function

The substitution box obtained as a result of step 1 is used as input for the Boolean function $bf(s)$. This gives the cryptographic system a stronger substitution box component. This function uses 3 NAND, 2 NOT, and 3 XOR gates to obtain the substitution box. The experimental setup used is explained in Section 4.

In Table 3, the 5-bit substitution box table is constructed based on a compound method of tent-logistic mapping, and a Boolean function is given. The illustration of the proposed solution and working procedure is described as follows:

To increase the resistance of a cryptographic solution, a confusion and diffusion strategy is used. To obtain this strength, chaotic mapping is used, as it is said to be deterministic. This method provides a robust substitution box. With a basic mathematical structure, complex chaotic behavior can still be obtained.

The 5-bit substitution box contains 32 values in the table, which satisfy the bijective property.

Declare the following parameters for the tent-logistic chaotic method:

r_tent = 1.8 // Tent map parameter

r_logistic = 3.9 // Logistic map parameter

seed_tent = 0.1 //Initial value for the tent map (seed)

seed_logistic = 0.5 //Initial value for the logistic map (seed)

where r is a regulating parameter with a r_logistic range from 0 to 4 and a r_tent range from 0 to 2. The control parameters correspond to the chaotic behavior.

3.2.1. The tent-logistic map is calculated as in equations (3), 4, and 5

$$s(n+1) = \begin{cases} f_1(s(n)), s(n) \le 0.5 \\ f_2(s(n)), s(n) > 0.5 \end{cases} \tag{3}$$

$$f_1(s) = r_{\text{logistic}} * \frac{9-r}{9} * s * (1-s) + r_{\text{tent}} * \frac{r}{9} * s \tag{4}$$

$$f_2(s) = r_{\text{logistic}} * \frac{9-r}{9} * s * (1-s) + r_{\text{tent}} * \frac{r}{9} * (1-s) \tag{5}$$

where r denotes the regulating parameter of the tent-logistic method, which ranges from 0 to 9, the system works as a logistic method if $r = 0$ and the tent method works if $r = 9$.

The mapping value 's' must be different from the input value 'm' ($m \neq s$).

The chaotic sequence obtained is applied to the Boolean function to obtain the substitution value,

$$c(n) \rightarrow bf(c) \rightarrow c(n+1) \tag{6}$$

where $c(n)$ denotes the chaotic sequence as a result of step 3.2.6, $bf(c)$ is the Boolean function, and is the substitution value

In the implementation of the above steps, the substitution box is constructed with an improved Strict Avalanche Criterion with a very minimum modification in input, producing massive revisions in the output. Similar to [1], with the 5-bit implementation, in the proposed DAC system, 31! random substitution boxes are possible. Whereas with 4-bit implementation, only 16! substitution boxes are possible, but with an increased number of randomness, the DAC system is comparatively stronger towards security.

The Boolean function used in the proposed S-box design satisfies the following criteria:

- Boolean function is non-linear to withstand LC, which seeks linear relationships between input and output bits.
- Minimal changes in input bits cause huge changes in output bits. Thus, the avalanche effect improves S-box diffusion.
- This balanced Boolean function reduces bias by ensuring that its output has about equal numbers of 1 s and 0 s.
- S-boxes have high algebraic complexity, making it hard to represent their output as a low-degree polynomial of the input bits.
- The Boolean function is resistant to differential cryptanalysis, which compares plaintext pairings and their ciphertexts.
- The function is resistant to known cryptographic attacks and has well-studied cryptographic features.

3.3. Cryptographic properties of DAC – substitution box

The proposed DAC solution satisfies the following cryptographic properties making it more suitable for the IoT environment and resistant against various attacks.

3.3.1. Stability

A Boolean function working with an n-bit ('n' denotes the length of the substitution box) structure denoted by is said to be stable if the result of the function contains a balance of 0's and 1's. A linear function $bf : \{0,1\}^n \rightarrow \{0,1\}$ selected for an input 'm', where $m \in f_2^n$, and $c \in f_2^n$,

$$f_m(c) = m_1c_1 \oplus m_2c_2 \ldots \oplus m_nc_n \tag{7}$$

Equation (7) m_ic_i denotes the bitwise AND of the bit and denotes bitwise XOR. Walsh coefficient is denoted as in equation (8),

$$W_f(c) = \sum_{m=f_2^n} (-1)^{f(m) \oplus m.c} \tag{8}$$

3.3.1.1. Non-linearity property. The Boolean function *bf,* defined as the

Table 3
5-bit Dynamic Airy Chaotic (DAC) Substitution box.

IP	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(IP)	30	24	9	27	28	26	4	22	2	15	29	5	13	8	25	3
IP	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
S(IP)	11	10	16	31	0	20	14	21	1	12	18	6	23	19	17	7

least possible hamming gap between an affine function is known as non-linearity. NL_{bf} denotes non-linearity of the function as given in equation (9)

$$NL_{bf} = \min(d(bf, g)), \forall g \in A_f \tag{9}$$

the Boolean function can be rewritten as equation (10), using the highest value of the Walsh coefficient, denoted by *WT* (Walsh-Hadamard Transform).

$$NL_{bf} = \frac{1}{2}[2^n - \max(WT(bf))] \tag{10}$$

3.3.1.2. Bijective property. A substitution box is considered bijective if each input vector is mapped with distinct resultant vectors. A Boolean function *f* of a substitution box is bijective if it is mapped in a one-to-one structure.

3.3.1.3. Bit Independency Criterion of substitution box (BIC). According to the Bit Independency Criterion, the change in any k^{th} bit in the input should impact the j^{th} bit of the resultant vector without any dependency. The resultant vector must be statically independent of each other.

3.3.1.4. Strict avalanche Criterion characteristics of substitution box (SAC). The strict avalanche effect is a pivotal characteristic of any cryptographic substitution box. This property is defined as the probability of changes in the resultant vector on flipping one bit, that is bit of an input. To have a strong substitution box resistant against attacks, the probability of changes in output must be at least 0.5. The probability of SAC is denoted by $p(i, r)$ in equation (11)

$$p(i, r) = 0.5, \forall i \to 0 : n, r \to 0 : n \tag{11}$$

3.3.1.5. Linear probability of continuous similarity. The Continuous similarity probability is also termed a linear approximation. Linear approximation is the minimum amount of similarity between the input and output vectors, with robust confusion and diffusion effects. The resistance of the substitution box is measured using the linear approximation probability, the lower value in the linear approximation table indicates high non-linearity and highly resistant against linear cryptanalysis. Linear approximation probability (LAP) is calculated by

$$LAP = \max\left[\frac{\#\{m \in X | m.\Delta m = S(m).\Delta c\}}{2^n} - \frac{1}{2}\right], \Delta c \neq 0 \tag{12}$$

In equation (12), m and c denote the input vector and the resultant vector respectively, and 'm' is the input vector with all possible inputs. $\Delta m$and Δc represent the noise added to the input channel or input difference and the noise added to the output channel or output difference. The resultant LAP value in the table decides the security of data. A probability value close to zero indicates high resistance to attacks.

3.3.1.6. Difference feasibility. The difference probability of a substitution box is the differential uniformity as defined as,

$$DDT = \max\left[\frac{\#\{ip \in X | S(ip) \oplus S(ip \oplus \Delta ip) = \Delta c\}}{2^n}\right], \Delta ip \neq 0 \tag{13}$$

In equation (13), X is the set of the different probable input values, and a number of bits are given by 'IP'. The substitution box attains non-linearity with high resistance to attack with the lowest value in DDT.

4. Results and discussions

The 5-bit DAC substitution box is implemented in ASIC using Hardware Description Language, Verilog, in Quartus Prime Version 22.1std.1 SC Lite Edition. Device model EP4CE10E22C8 has a computational time of 6.225 ns including 4.475 ns logic, 1.750 ns route, 71.9 % logic, and 28.1 % route.

The implementation cost of the substitution box is estimated as in [2]. The operations NAND, NOR, and NOT are denoted by N operations, and XOR, and XNOR are denoted by X operations. The DAC substitution box uses 5 N + 3X operations, which use 10 units (10 pins used out of 92). A comparison of the gate equivalence of various 4 and 5-bit substitution structures is compared with the gate area occupied in implementing the proposed DAC substitution box illustrated in Table 4.

4.1. Resilience property of a 5-bit DAC substitution box

The resilience properties of traditional and previous solutions in substitution box construction are discussed. The probability of using the odd-sized substitution boxes is comparatively low compared to 4-bit, 6-bit, and 8-bit substitution structures. An even-sized substitution box is preferred due to its congruency in input blocks. The DAC substitution box with 5-bit is also more adaptable to all the input block sizes.

As in [15], the 32-bit blocks are divided into six 5-bit blocks and the remaining two bits. The MSB and LSB in the input are flipped from 0 to 1 or 1 to 0 respectively to improve the SAC property. Similarly, all the n-bit input can be split into 5*m blocks the remaining bits are flipped as shown in Fig. 3.

4.2. Analysis of the chaotic behavior of the DAC substitution box

The complexity of the DAC system is analyzed using entropy approximation analysis. The greater value of the entropy approximation value indicates the increased complexity of the system [14]. The DAC system uses the compound method of the Tent-Logistic Mapping method to produce chaotic behavior and obtain non-linearity. The performance of the Tent-Logistic map is compared with the Tent map and Logistic map methods, as shown in Fig. 4. Thus, the proposed chaotic behavior in the DAC substitution box exhibits good chaotic behavior.

Fig. 5 illustrates the chaotic behavior of the DAC substitution box implemented with the Logistic mapping method, Tent mapping method, and Tent-Logistic mapping method in Fig. 4a, b, and c, respectively. A small change in seed value has produced output with major changes, as shown in Fig. 4c. The illustrations are performed for 50 iterations. The values used in the calculation are given in Section 3 illustration 3.2.

Table 5 presents a comparative analysis of the Dynamic Airy Chaotic (DAC) substitution box compared to other widely used substitution boxes, focusing on aspects of security, resource utilization, and performance. A tabular representation is employed to facilitate the comparison.

A tabular representation illustrating comprehensive outcomes of the DAC's performance across multiple measures in comparison to conventional approaches, Table 6.

5. Security analysis of DAC the substitution box

The resistance capability of the 5-bit DAC substitution box is demonstrated in this section. The following are parameters involved in measuring the strength and robustness of the proposed substitution structure. They are nonlinearity, bijective property, bit independence property, avalanche property, linear and differential probability. The comparison of these parameters with other lightweight cryptographic

Table 4
Observations of the memory footprint of various lightweight cryptographic algorithms.

Lightweight Algorithm	Bit Length	Gate Count
DAC (Proposed)	**5 x 5**	**11.25 GE**
Vishal A. Thakor, et. Al. [1]	5 x 5	12.54 GE
PRESENT [23]	4 x 4	22.5 GE
SKINNY [25]	4 x 4	12 GE
Hummingbird-2 [25]	4 x 4	20 GE
RECTANGLE [24]	4 x 4	18 GE

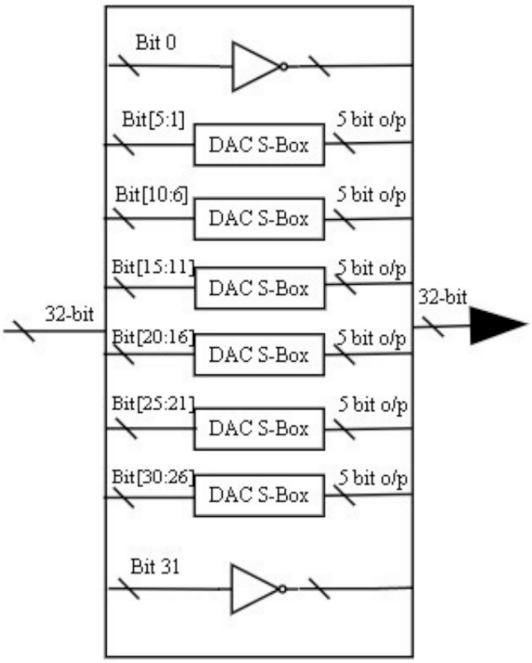

Fig. 3. Resilience of a 5-bit DAC system for a 32-bit block cipher technique.

algorithms is illustrated.

5.1. Bijective property of DAC

The Dynamic Airy Chaotic (DAC) substitution box is a 5x5 substitution box that is said to be bijective. The bijective property is derived using the Hamming weight (H_w) using equation (14). Hamming weight refers to several non-zero elements in a bit sequence. The count of '1s' in the string is demonstrated using

$$H_w\left(\sum_{i=1}^{n} b_i f_i\right) = 2^{n-1} \tag{14}$$

where, $b_i \in \{0,1\}$ and $b_i \neq 0$. f_i is the Boolean function that satisfies the bijective property with a count of 0′s and 1′s. Also, the DAC substitution box produces 32 distinct values from 0 to 31 as a result.

5.2. Avalanche property of DAC

It is a pivotal property of a cryptographic substitution box. A minimum variance in the input produces a massive revision in the result is known as the avalanche effect. A cryptographic solution is said to satisfy this property if at least one-half of the resultant bits flip each time for a change in one bit. As in [8], SAC is defined by considering the 5-bit input denoted by M producing a 5-bit output denoted by using the substitution function $S, M_i = S(N_i)$ $where \leqslant\leqslant 5$. A change in M (i.e., M_j) results with The dependency probability P_j is calculated by performing $N_j \oplus N$ and dividing the output by 2^n. A 5x5 probability matrix is constructed for a function, $f : z_2^m \rightarrow z_2^n$ and the matrix $a \in z_2^m$, where $a \neq 0$ using $f(x) \oplus f(x \oplus a)$. The DAC substitution box results in an average of 0.52 as the avalanche probability. The SAC criteria are satisfied if the probability is a minimum of 0.5 (50 % of change). Thus, the DAC substitution box is said to satisfy SAC.

5.3. DAC – nonlinearity property

The Boolean function $bf : z_2^n \rightarrow z_n$ used in structuring DAC to exhibit nonlinearity property, which is defined as,

$$N_{bf}(f) = \min_{\alpha \in A_n} d(bf, \alpha) \tag{15}$$

were, *alphais* an integrity of all affine functions. The nonlinearity of an affine function is zero. Thus, if a Boolean function is not affine, then the nonlinearity will be greater than zero $(N_{bf} > 0)$. The greater the hamming distance value the solution is said to be highly nonlinear. The hamming distance H_d is calculated as the difference between the corresponding input and output pairs. The hamming distance of each pair in the DAC substitution box is shown in Table 7. According to Table 7, the minimum is 1 and the maximum is 5. Thus, the average H_d is 2.5625, satisfying the nonlinearity characteristics.

5.4. Linear cryptanalysis of the DAC substitution box

In linear probability and differential cryptanalysis, as discussed in Section 3.6; the probability bias is calculated. A larger probability value denotes a higher chance of being compromised. For the DAC substitution box, the highest value is 8. Thus, the average linear approximation probability is 0.125, which is closer to zero. The comparison of the probability value of the DAC method with other solutions is given in Table 8.

5.5. Differential cryptanalysis of the DAC substitution box

Differential cryptanalysis is an attack based on the difference distribution table constructed for a substitution box. The difference distribution probability is calculated as given in Section 3.3.6 using Equation (13). The maximum probability of differential cryptanalysis of the DAC substitution box is 8. The probability value is 0.25 given by 8 / 2^n, and n is the bit count (5 bits in the DAC solution). The comparison of differential cryptanalysis of DAC with other substitution boxes is in Table 8. Thus, the lower probability value makes the DAC system stronger against differential attacks.

5.6. DAC – BIC

The bit independence criterion (BIC), is defined as the change in an i^{th} bit in the input that will reflect the revision in output bits, m and n, elements where $\in (1, 2, \cdots, 5) and m \neq n$. Thus, the output bits of the Boolean function must satisfy the SAC property and show high nonlinearity. Nonlinearity by $f_m \oplus f_n$. The substitution box with a BIC and avalanche value close to 0.5 is said to be highly resistant to attacks. The DAC-BIC and DAC-SAC probabilities calculated for the DAC substitution structure are 0.52. Thus, satisfying the bit independence criterion makes it strong in security.

Cryptographic features and chaos-based transformations protect the DAC [25] Substitution Box from differential and linear cryptanalysis. Here's how DAC resists various attacks in detail:

- DAC has strong non-linearity due to chaotic transformations of input data. Chaotic maps like Logistic or Tent maps make replacement nonlinear.
- The DAC S-box exhibits a significant avalanche impact. Even a single-bit input change causes large and unpredictable output alterations. This characteristic improves the diffusion property and makes the S-box resistant to linear cryptanalysis by dispersing input bit changes throughout the output.
- Chaotic systems like DAC have complicated dynamics, making their behavior sophisticated and challenging to understand theoretically. This intricacy makes linear or differential S-box analysis and breaking more difficult for cryptanalysts.
- To assure security, DAC's design and parameters were tested against cryptographic criteria such as the SAC and Propagation Criterion. The S-box's diffusion and confusion qualities are essential for differential and linear cryptanalysis resistance.

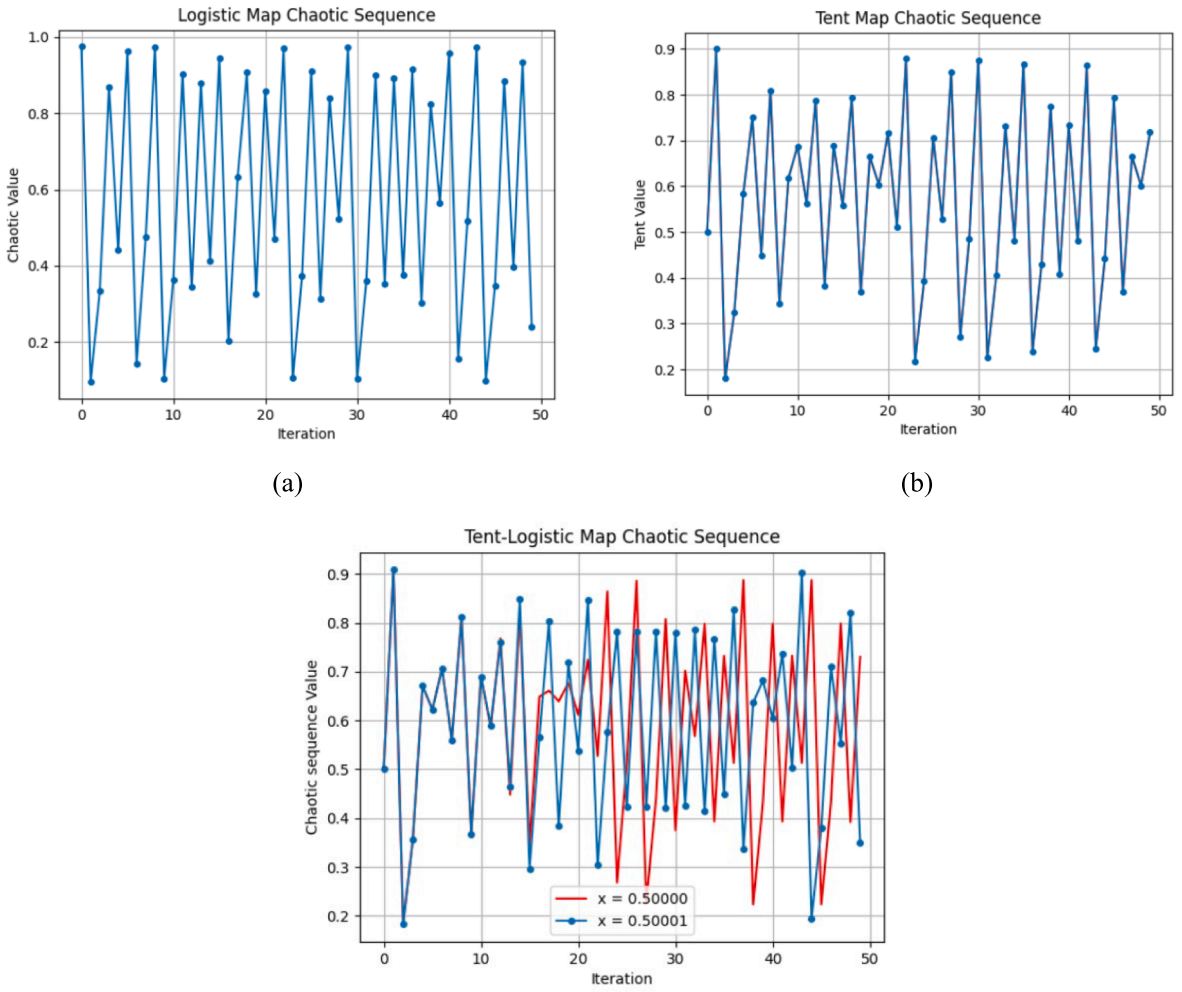

Fig. 4. Chaotic sequence behavior of the first 50 iterations (a) Logistic Map with control parameter r = 3.9, initial seed, x = 0.5, (b) Tent Map with r = 1.8 and x = 0.1 (c) Logistic-Tent map r = 8 and comparison with two different initial value of x is given (demonstrated using Matplotlib Python compiler).

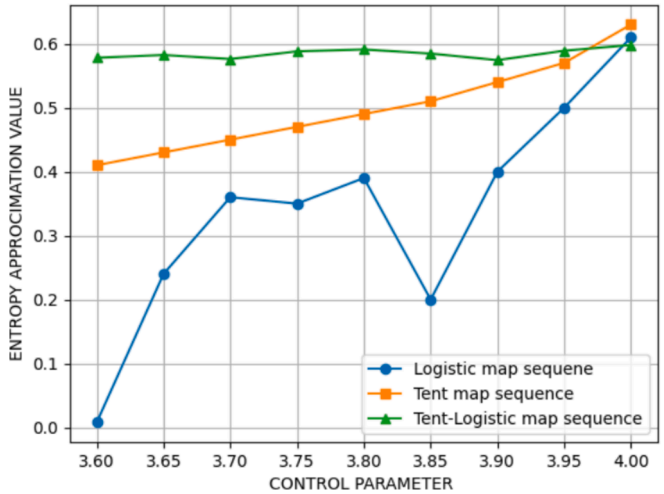

Fig. 5. Entropy approximation values generated by different chaotic map sequences.

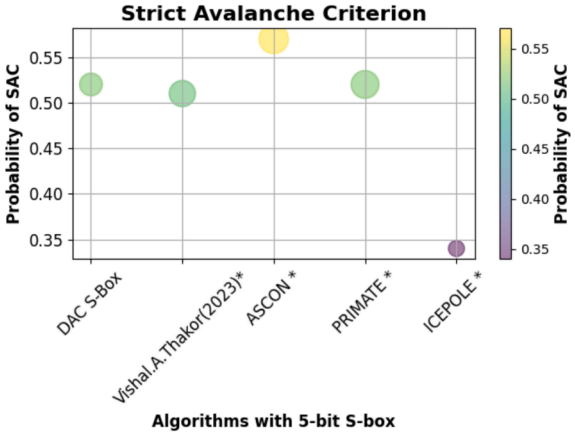

Fig. 6. Comparison of SAC.

- The Airy map in DAC offers smooth and continuous transformations. This continuity resists cryptographic function discontinuity or discrete behavior assaults.

A comprehensive table is presented in Table 9, offering an in-depth

Table 5
Comparing security, resource utilization, and performance of the DAC substitution box to other typical substitution boxes.

Substitution Box	Security	Resource Utilization	Performance
Dynamic Airy Chaotic (DAC)	– Highly non-linear, offering resistance to linear and differential cryptanalysis.	– Requires additional computational resources for chaotic map calculations.	– May exhibit slower encryption/ decryption speeds due to chaotic map evaluations.
S-Box in AES [20]	– Secure against known cryptographic attacks, widely analyzed and trusted.	– Hardware and Software implementation is proficient.	– Provides a trade-off between security and efficiency in widely used ciphers like AES.
S-Box in DES [2]	– Somewhat outdated and vulnerable to modern attacks like differential cryptanalysis.	– Efficient resource utilization due to simpler bitwise operations.	– Less secure compared to modern ciphers, leading to reduced overall security.
SubBytes in Serpent [29]	– Provides a high level of security with complex operations, secure against to linear and differential attacks.	– May require more resources compared to some other S-boxes.	– Serpent is known for its security, but it may be slower in software implementations.
SubBytes in Twofish [30]	– Designed for security and resistance to various cryptographic attacks.	– Typically, more efficient in terms of resource utilization.	– Provides a trade-off between security and efficiency.
SubBytes in Camellia [31]	– Designed with security in mind, offering resistance to known attacks.	– Resource-efficient, designed for hardware acceleration.	– Generally, provides good performance with strong security features.

Table 6
DAC's performance compared to conventional approaches.

Performance Metric	DAC Substitution Box	Traditional 4-bit Substitution Box	Traditional 6-bit Substitution Box
Bit Nonlinearity (AIN)	High	Average to High	High
Differential Probability	Low	Average to Low	Low
Avalanche Effect	Strong	Average to Strong	Average to Strong
Cryptanalysis Resistance	Strong	Average	Strong
Implementation Complexity	Average	Low	High
Resource Utilization	Average	Low	High
Latency and Throughput	Acceptable	Low	Average
Adaptability to Block Sizes	High	Limited	Limited
Security Strength	High	Average	High
Power Consumption (if applicable)	Low to Average	Low to Average	High

examination of the computational, memory, and additional overheads associated with the proposed DAC system in comparison to currently available alternatives. Particular emphasis is placed on evaluating the efficiency of "lightweight" designs.

Table 7
Hamming Distance (H_d) for DAC substitution box.

Input	Result	DAC- H_d	Input	Result	DAC $-H_d$
00,000	11,110	4	10,001	01,010	4
00,001	11,000	3	10,010	10,000	1
00,010	01,001	3	10,011	11,111	2
00,011	11,011	2	10,100	00,000	2
00,100	11,100	2	10,101	10,100	1
00,101	11,010	5	10,110	01,110	2
00,110	00,100	1	10,111	10,101	1
00,111	10,110	2	11,000	00,001	3
01,000	00,010	2	11,001	01,100	3
01,001	01,111	2	11,010	10,010	1
01,010	11,101	4	11,011	00,110	4
01,011	00,101	3	11,100	10,111	3
01,100	01,101	1	11,101	10,011	3
01,101	01,000	2	11,110	10,001	4
01,110	11,001	4	11,111	00,111	2
01,111	00,011	2	10,001	01,010	4

Table 8
Security analysis of various 5-bit substitution structures.

5-bit Substitution Box	Non – Linearity	SAC	Linear Probability	Differential Probability	BIC
DAC	2.5625	0.52	0.125	0.25	0.52
Vishal A. Thakor, et. Al.	2.675	0.51	0.25	0.25	0.53
ASCON	2.5	0.57	0.25	0.25	0.58
PRIMATE	2.5	0.52	0.375	0.0625	0.54
ICEPOLE	1.531	0.34	0.25	0.25	0.44

6. Conclusion

The substitution box, is a crucial element that imparts necessary nonlinearity to encryption algorithms based on substitution and permutation networks (SPNs). The lightweight cryptographic systems necessitate the careful consideration of S-box designs that effectively balance factors such as cost, performance, and security strength. The present study investigates different designs of S-boxes, with lengths ranging from 3 to 8 bits, and assesses their appropriateness for devices with limited resources. As evidenced by the chart supplied, the utilization of 3- and 4-bit S-boxes has been prevalent in limited situations. The proposal of the Dynamic Airy Chaotic (DAC) substitution box has emerged as a solution to address the requirement for heightened security while considering limited resource restrictions. DAC architecture incorporates a 5-bit length, providing enhanced adaptability across a range of block sizes. The utilization of the Tent-Logistic technique in DAC construction effectively broadens the range of chaos and promotes chaotic behavior. Furthermore, the incorporation of Boolean functions strengthens the substitution box. The suggested DAC substitution box demonstrates its robustness, stability, and resistance characteristics through cryptographic strength evaluations conducted using common benchmarks. The DAC substitution box has the potential to be integrated into comprehensive lightweight block cipher algorithms. The efficiency of such integrations can be assessed and compared to pre-existing systems while considering external variables such as power usage. The utilization of the DAC-based technique presents a promising opportunity to bolster the security of lightweight cryptographic solutions in safeguarding contemporary resource-limited gadgets and applications. In the future, this DAC-based technique can further be applied to different structures of a lightweight block cipher.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence

Table 9
Comparison of the proposed DAC system's computational, memory, and other overheads to those of existing solutions.

Overhead Comparison	Proposed DAC System	Existing Solutions
Computation Overhead	– Moderate computational overhead due to the dynamic chaotic sequence generation and Boolean function application.	– Generally lower computational overhead in lightweight designs to ensure efficient performance on resource-constrained devices.
Memory Overhead	– Reasonable memory usage for storing chaotic map parameters, Boolean functions, and intermediate data.	– Efficient memory usage, prioritizing minimal memory footprint in lightweight cryptographic solutions.
Power Consumption	– This may have a slightly higher power consumption compared to basic 4-bit substitution boxes due to increased complexity.	– Designed to minimize power consumption in lightweight solutions, often operating within tight energy budgets.
Algorithm Size	– Larger algorithm size compared to minimalistic designs to accommodate the DAC S-box and associated components.	– Compact algorithm size is a key consideration in lightweight cryptography to conserve device storage.
Latency and Throughput	– May introduce slight latency in encryption/ decryption due to chaotic sequence generation but can maintain acceptable throughput.	– Prioritizes low latency and efficient throughput to support real-time applications in lightweight scenarios.
Implementation Flexibility	– Offers flexibility in terms of bit length and adaptability to various block sizes, enhancing versatility.	– Prioritizes simplicity and ease of implementation in constrained environments.
Security Strength	– Provides robust security against advanced cryptographic attacks, justifying the trade-off in overheads.	– Balances security strength with overhead constraints to maintain the desired level of protection.

the work reported in this paper.

References

[1] Thakor VA, Razzaque MA, Darji AD, Patel AR. A novel 5-bit S-box design for lightweight cryptography algorithms. J. Inform. Security Appl. 2023;73. https://doi.org/10.1016/j.jisa.2023.103444.

[2] Panchami V, Mathews MM. A substitution box for lightweight ciphers to secure the internet of things. J. King Saud Univ. – Computer Inf. Sci. 2023;35(4):75–89. https://doi.org/10.1016/j.jksuci.2023.03.004.

[3] Beaulieu R, Treatman-Clark S, Shors D, Weeks B, J. Smith and L. Wingers. 2015. The SIMON and SPECK lightweight block ciphers. 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA. 1-6. doi: 10.1145/2744769.2747946.

[4] Jamal SS, Anees A, Ahmad M, Khan MF, Hussain I. Construction of cryptographic s-boxes based on mobius transformation and chaotic tent-sine system. IEEE Access 2019;7:173273–85. https://doi.org/10.1109/ACCESS.2019.2956385.

[5] Jamal SS, Attaullah T, Shah AH, AlKhaldi, Tufail MN. Construction of new substitution boxes using linear fractional transformation and enhanced chaos. Chinese J Phys 2019;60:564–72. https://doi.org/10.1016/j.cjph.2019.05.038.

[6] Hussain I, Anees A, T.A. Al-Maadeed, and M.T. Mustafa. 2019. Construction of S-box based on chaotic map and algebraic structures. Symmetry. 2019. 11(3):351. doi: 10.3390/sym11030351.

[7] Sakthi Vignesh Radhakrishnan, Subramanian S. 2012. An analytical approach to s-box generation. International Conference on Communication and Signal Processing, Chennai, India. 1-5, doi: 10.1109/ICCSP.2012.6207752.

[8] Ruby, Mishra., Manish, Okade., Kamalakanta, Mahapatra. (2022). FPGA-based High Throughput Substitution Box Architectures for Lightweight Block Ciphers. doi: 10.1109/PKIA56009.2022.9952325.

[9] Sherine Jenny R, Sudhakar R, Karthikpriya M. Design of compact S box for resource-constrained applications. J Phys Conf Ser 2020;1767. https://doi.org/10.1088/1742-6596/1767/1/012059.

[10] Alshammari BM, Guesmi R, T. Guesmi, H. Alsaif, and A. Alzamil. 2021. Implementing a Symmetric Lightweight Cryptosystem in Highly Constrained IoT Devices by Using a Chaotic S-Box. Symmetry. 2021; 13(1):129. doi: 10.3390/sym13010129.

[11] Lu Q, Zhu C, Wang G. 2019. A Novel S-Box Design Algorithm Based on a New Compound Chaotic System. Entropy. 2019. 21(10):1004. doi: 10.3390/e21101004.

[12] Aruna S, Usha G. S-DAC: A Novel Dynamic Substitution box using a hybrid chaotic system and Deoxyribonucleic Acid (DNA) coding for counterfeiting Side-Channel Attacks. Pers Ubiquit Comput 2021. https://doi.org/10.1007/S00779-021-01579-4.

[13] Chengrui Z, Junxin C, Dongming C, Wei W, Yushu Z, Yinwen Zu. Exploiting substitution box for cryptanalyzing image encryption schemes with DNA coding and nonlinear dynamics. IEEE Trans Multimedia 2023. https://doi.org/10.1109/tmm.2023.3276504.

[14] Xiaojun T, Xudong L, Jing L, Miao Z, Zhu W. A novel lightweight block encryption algorithm based on combined chaotic S-box. Int J Bifurcation Chaos 2021. https://doi.org/10.1142/S0218127421501522.

[15] Goudarzi D, Jean J, Kölbl S, Peyrin T, Rivain M, Sasaki Y, et al. Pyjamask: block cipher and authenticated encryption with highly efficient masked implementation. IACR Trans Symmetric Cryptol 2020;2020(S1):31–59. https://doi.org/10.13154/tosc.v2020.iS1.31-59.

[16] Nilima S, Alind, Alind, Nitin, Arora. Randomization technique for designing of substitution box in data encryption standard algorithm. Int J Mathem Sci Comp 2019. https://doi.org/10.5815/IJMSC.2019.03.03.

[17] Naveed A, Azam, Umar, Hayat, Maria, Ayub. A substitution box generator, its analysis, and applications in image encryption. Signal Process 2021. https://doi.org/10.1016/J.SIGPRO.2021.108144.

[18] Dobraunig C, Eichlseder M, Mendel F, et al. ASCON v1.2: lightweight authenticated encryption and hashing. J Cryptol 2021;34(33). https://doi.org/10.1007/s00145-021-09398-9.

[19] Suzuki T, Minematsu K, Sumio Morioka, and Eita Kobayashi. 2011. TWINE: A Lightweight, Versatile Block Cipher. ECRYPT Workshop on Lightweight Cryptography.

[20] Tiessen T, Knudsen LR, S. Kölbl, and M.M. Lauridsen. 2015. Security of the AES with a Secret S-Box. Fast Software Encryption. FSE 2015. Lecture Notes in Computer Science. 9054. doi: 10.1007/978-3-662-48116-5_9.

[21] Webster AF, Tavares SE. On the design of S-boxes. Advances in Cryptology — CRYPTO '85 Proceedings. Lect Notes Comput Sci 1986;218. https://doi.org/10.1007/3-540-39799-X_41.

[22] Bilgin B, Bogdanov A, Knežević M, F. Mendel, and Q. Wang. 2013. Fides: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware. Cryptographic Hardware and Embedded Systems - CHES 2013. Lecture Notes in Computer Science book series. 8086. doi: 10.1007/978-3-642-40349-1_9.

[23] Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJB, et al. PRESENT: An Ultra-Lightweight Block Cipher. Heidelberg: Springer; 2007. p. 450–66. 10.1007/978-3-540-74735-2_31, 4727.

[24] Dahiphale V, Bansod G, Patil J. 2017. ANU-II: A fast and efficient lightweight encryption design for security in IoT. International Conference on Big Data, IoT and Data Science (BID), Pune, India. 130-137. doi: 10.1109/BID.2017.8336586.

[25] Engels D, Saarinen MJO, P. Schweitzer, E.M. Smith. 2012. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm. RFID. Security and Privacy. RFIDSec 2011. Lecture Notes in Computer Science. 7055. doi: 10.1007/978-3-642-25286-0_2.

[26] Gong Z, S. Nikova, Y.W. Law. 2012. KLEIN: A New Family of Lightweight Block Ciphers. RFIDSec 2011. Springer, Heidelberg. 7055: 1–18. doi:10.1007/978-3-642-25286-0_1.

[27] Knudsen L, Leander G, Poschmann A, Robshaw MJB. PRINTCIPHER: A block cipher for IC-Printing. Cryptographic Hardware and Embedded Systems, CHES 2010. Lect Notes Comput Sci 2010;6225:16–32. https://doi.org/10.1007/978-3-642-15031-9_2.

[28] Guo J, Peyrin T, A. Poschmann, and M.J.B. Robshaw. 2011. The led block cipher. Cryptographic Hardware and Embedded Systems – CHES 2011. 6917(8): 326–341. doi:10.1007/978-3-642-23951-9_22.

[29] Kabilan K, Saketh M, Nagarajan KK. Implementation of SERPENT cryptographic algorithm for secured data transmission. In: 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS); 2017. https://doi.org/10.1109/ICIIECS.2017.8275863.

[30] Gulsezim D et al. 2019. Two Factor Authentication using Twofish Encryption and Visual Cryptography Algorithms for Secure Data Communication. 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain. pp. 405-411, doi: 10.1109/IOTSMS48152.2019.8939261.

[31] Aoki K. et al. 2001. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. In: Stinson, D.R., Tavares, S. (eds) Selected Areas in Cryptography. SAC 2000. Lecture Notes in Computer Science, vol 2012. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44983-3_4.

[32] Wenkai Li, Jiuyang Bu, Xiaoqi Li, Hongli Peng, Yuanzheng Niu, Yuqing Zhang. A survey of DeFi security: Challenges and opportunities. 2022. J King Saud Univ – Computer Inf Sci, 34 (10), Part B, pp. 10378-10404. https://doi.org/10.1016/j.jksuci.2022.10.028.

[33] Han D, Zhou H, Weng TH, et al. LMCA: a lightweight anomaly network traffic detection model integrating adjusted mobilenet and coordinate attention mechanism for IoT. Telecommun Syst 2023;84:549–64. https://doi.org/10.1007/s11235-023-01059-5.