International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(16s) 2026 pp. 963-973
https://doi.org/10.70917/ijcisim-2026-4624
Article

From Boolean Functions to Secure S-Boxes: Construction, Challenges, and a Chaos-Based Dynamic Solution

Dhanashree Hadsul[1], Zahir Aalam [2]

[1]Department of Information Technology, Thakur College of Engineering and Technology, Mumbai, India-400101
[1]Department of Information Technology, Thakur College of Engineering and Technology, Mumbai, India-400101
1 dhanashree.hadsul@gmail.com

Abstract: Substitution boxes, commonly called S-boxes, are the primary source of nonlinearity in modern symmetric block ciphers, and their strength rests almost entirely on the cryptographic quality of the Boolean functions from which they are built. This paper traces that dependency from first principles. It reviews the algebraic foundations of cryptographic Boolean functions, including nonlinearity, algebraic degree, balancedness, bentness, and the avalanche and correlation immunity criteria that a coordinate function of a strong S-box must satisfy. It then surveys the main families of S-box construction, algebraic, heuristic, chaos-based, and hybrid, drawing on a paper bank of 43 verified sources retrieved through the Semantic Scholar API, and explains why static, fixed S-boxes remain structurally exposed to differential, linear, and algebraic cryptanalysis. Building on this review, the paper implements and evaluates a dynamic, key-dependent S-box generation framework that couples a compound tent-logistic chaotic map with an algebraic base layer, and reports the framework's actual measured performance, nonlinearity, strict avalanche criterion, bit independence criterion, differential uniformity, and linear probability, against the AES S-box baseline over twelve independently generated instances. The results are reported honestly, including a gap between the proposed construction's nonlinearity and the AES baseline that mirrors a limitation already documented in the literature, and the paper closes with a discussion of what a genuinely competitive dynamic S-box design would need to add to close that gap.
Keywords: Boolean functions, S-box, substitution box, nonlinearity, chaos theory, chaotic maps, dynamic S-box, differential cryptanalysis, linear cryptanalysis, block cipher design

1. Introduction

Every symmetric block cipher in wide use today, from the Advanced Encryption Standard (AES) to lightweight ciphers designed for constrained IoT devices, depends on a small nonlinear lookup table to break the linear structure that would otherwise make the cipher solvable by algebraic means. This component is the substitution box, or S-box. An S-box is, formally, a vectorial Boolean function mapping n input bits to m output bits, and its individual output bits, taken one at a time, are themselves ordinary Boolean functions of the input. The security the S-box contributes to the cipher as a whole is therefore bounded above by the cryptographic quality of these coordinate Boolean functions. Understanding S-box design is, at its root, an exercise in understanding Boolean function theory.

The relationship runs in both directions. On one side, the theory of cryptographic Boolean functions, nonlinearity, algebraic degree, correlation immunity, and the extremal class known as bent functions, has been developed largely to explain and improve the resistance of block and stream ciphers to statistical attack (Carlet, Crama, & Hammer, 2010). On the other side, every refinement in cryptanalysis, from differential attacks to linear and zero-correlation attacks on ciphers such as GIFT and KASUMI (Cao & Zhang, 2019; Yi & Chen, 2014), has been answered by tighter design criteria on the Boolean functions permitted inside an S-box. The result is a design space with several competing objectives, high nonlinearity, low differential uniformity, balancedness, and algebraic complexity, that cannot all be maximized simultaneously. This tension is the S-box design trade-off, and it is the central problem this paper addresses.

A second, more recent thread in the literature concerns the fact that almost all deployed S-boxes, including the AES S-box itself, are static: the same lookup table is used in every round, for every key, for the algorithm's entire lifetime. A static table is a fixed target, since its differential and linear profile never changes once published. This has motivated a substantial body of work on key-dependent and dynamically regenerated S-boxes (Kazlauskas & Kazlauskas, 2009; Ejaz, Shoukat, Iqbal, & Rauf, 2021), many of them built from discrete chaotic maps whose sensitivity to initial conditions and ergodic mixing properties make them attractive generators of large families of distinct substitution tables (Khan, Shah, & Batool, 2015; Lambić, 2016).

This paper has four goals. First, it reviews the Boolean function theory that underlies S-box design. Second, it surveys and classifies the major families of S-box construction reported in the literature, grounded in a 43-paper reference bank retrieved from the Semantic Scholar API and verified by exact bibliographic match rather than by memory or general web search. Third, it implements a concrete dynamic, chaos-based S-box generation framework and evaluates it against the AES baseline using the standard cryptographic property suite, reporting the results exactly as computed. Fourth, it discusses, honestly, where that implementation falls short of the strongest published designs and what would be needed to close the gap.

2. Boolean Functions: Mathematical Foundations for Cryptographic Design

An n-variable Boolean function is a mapping f from the vector space of n-bit binary strings to a single output bit. Every such function has a unique representation as a multivariate polynomial over the two-element field, its algebraic normal form, obtained by expanding f as a sum of products of input variables with binary coefficients. The algebraic degree of f is the size of the largest product term with a nonzero coefficient in this expansion. Functions of degree at most one are affine, and affine functions are cryptographically weak because they can be inverted or predicted with simple linear algebra. A central design goal is to keep a function's output as far as possible, in Hamming distance, from every affine function on the same number of variables (Carlet, Crama, & Hammer, 2010).

This distance is formalized through the Walsh-Hadamard transform, which measures the correlation between a Boolean function and every linear approximation of it. The nonlinearity of f is defined from the maximum magnitude of this transform and is bounded above by the covering radius bound. Functions that meet this bound exactly are called bent functions; they achieve the maximum possible nonlinearity attainable on an even number of variables, though they are never balanced and so cannot be used directly as S-box coordinate functions (Tokareva, 2015). Filiol and Fontaine (1998) showed that highly nonlinear balanced Boolean functions with good correlation immunity can nonetheless be constructed, at the cost of a small reduction in nonlinearity relative to the unattainable bent bound, which is the practical compromise every real S-box coordinate function has to make.

Beyond nonlinearity and algebraic degree, Boolean functions used inside S-boxes must satisfy criteria developed specifically to counter attacks on early block ciphers. The strict avalanche criterion requires that complementing any single input bit changes each output bit with probability close to one half, so that a one-bit plaintext change propagates unpredictably through the cipher; recursive and bent-sequence-based constructions were developed early on specifically to guarantee this property by design (Kim, Matsumoto, & Imai, 1990; Adams & Tavares, 1990). The bit independence criterion extends this by requiring that pairs of output bits change independently of one another under any single input bit flip. Correlation immunity, and the stronger notion of resiliency, protects against divide-and-conquer statistical attacks; Canteaut, Carlet, Charpin, and Fontaine (2000) and Sarkar (2000) both characterize the trade-off between correlation immunity, nonlinearity, and algebraic degree in detail, showing that pushing one of these properties toward its optimum generally costs something on the other two. Algebraic immunity, which gained prominence after the introduction of algebraic attacks, measures the minimum degree of any nonzero function that annihilates f or f plus one; Tang, Carlet, Tang, and Zhou (2017) present constructions of highly nonlinear resilient functions that simultaneously achieve optimal algebraic immunity, illustrating that these criteria, while individually well understood, are jointly very difficult to satisfy at once.

No known construction satisfies every one of these criteria to its theoretical optimum simultaneously. Cryptographic Boolean function design for S-boxes is therefore a genuinely multi-objective optimization problem, and this is the mathematical inheritance that any S-box construction method, algebraic, heuristic, or chaos-based, must manage.

3. From Boolean Functions to S-Boxes

An S-box generalizes a single Boolean function to a vectorial Boolean function, or (n, m)-function, mapping n input bits to m output bits. Each output bit, viewed as a function of the input, is a coordinate function, and every nonzero linear combination of the coordinate functions is a component function. The cryptographic strength of the whole S-box is governed by the weakest of these component functions, which is why evaluation frameworks report nonlinearity and related properties as a minimum over all nonzero component functions rather than as an average (Carlet, Crama, & Hammer, 2010).

For an S-box to be usable inside an invertible cipher it must additionally be bijective, so the substitution can be undone during decryption. Beyond bijectivity, the standard evaluation suite used throughout the S-box literature covers nonlinearity, the strict avalanche criterion, the bit independence criterion, differential uniformity, and linear approximation probability. Differential uniformity, central to resisting differential cryptanalysis, measures the largest number of input pairs sharing a fixed input difference that also produce the same output difference; a lower value indicates a flatter, more resistant difference distribution table. Linear approximation probability plays the analogous role for linear cryptanalysis.

The AES S-box is the field's reference example of an algebraically constructed S-box, composing the multiplicative inverse function over a finite field with a fixed affine transformation chosen to destroy the algebraic simplicity that the inverse function alone would expose to interpolation attacks. Work on the AES S-box continues at both ends of the design spectrum: Reyhani-Masoleh, Taha, and Ashmawy (2018) report new compact hardware implementations of the combined AES S-box and its inverse for area-constrained circuits, while Nitaj, Susilo, and Tonien (2020) propose modified AES S-box constructions intended to improve specific algebraic properties beyond the original design. Both directions confirm that the algebraic, inverse-function-plus-affine-transform pattern remains the dominant approach wherever properties need to be established analytically rather than estimated empirically.

4. S-Box Construction Approaches: A Taxonomy

4.1 Algebraic constructions

Algebraic methods derive an S-box from a mathematically well-understood function over a finite field, typically a power function, followed by an affine transformation chosen to remove undesirable algebraic regularities. Their principal advantage is provability, since properties such as differential uniformity and nonlinearity can often be derived in closed form. Their principal limitation is a comparatively small design space, since only a limited catalog of finite-field functions offers the required combination of high nonlinearity and low differential uniformity.

4.2 Heuristic and pseudo-random search

Heuristic methods treat S-box construction as a combinatorial optimization problem over the space of all bijections on n bits, searched using techniques such as genetic algorithms or simulated annealing with a fitness function that rewards high nonlinearity and low differential uniformity. Wang, Wong, Li, and Li (2012) combine a chaotic map with a genetic algorithm specifically to escape the local optima that pure heuristic search tends to get trapped in, reporting improved nonlinearity relative to either technique used alone. The general limitation of this family is computational cost and the absence of a compact analytical security proof, so strength is established empirically rather than derived.

4.3 Chaos-based constructions

Chaos-based methods generate S-box entries from the trajectory of a discrete chaotic dynamical system, exploiting ergodicity, mixing, and sensitivity to initial conditions. Çavuşoğlu, Kaçar, Pehlivan, and Zengin (2017) and Khan, Shah, and Batool (2015) are representative of the foundational wave of this literature, both deriving S-boxes directly from chaotic Boolean function outputs and validating them through downstream image encryption. Belazi and El-latif (2017) show that even a comparatively simple chaotic sine map can be sufficient to construct an efficient S-box, while Çavuşoğlu, Zengin, Pehlivan, and Kaçar (2016) and Lambić (2016) turn to more structurally elaborate chaotic systems, a scaled Zhongtang system and a general discrete chaotic map framework respectively, specifically to widen the achievable nonlinearity range beyond what the simplest one-dimensional maps allow. Jiang and Ding (2021) combine chaos with bent function theory directly, using a chaotic sequence to select among candidate bent-derived Boolean functions rather than quantizing the chaotic trajectory into the S-box on its own, which is one of the more theoretically grounded hybridizations in this bucket of the literature.

4.4 Hybrid, key-dependent, and dynamic methods

A large and active sub-literature focuses specifically on key-dependence and dynamic regeneration rather than on chaos as an end in itself. Kazlauskas and Kazlauskas (2009) is an early and influential study establishing that key-dependent S-box generation for AES is practically achievable; Abdelghafar, Rohiem, Diaa, and Mohammed (2009) and Manjula and Mohan (2016) both propose concrete key-dependent AES S-box generation procedures, the former built around the RC4 key schedule. Mahmoud, Abd, Hafez, and Elgarf (2013) and Alabaichi and Salih (2015) evaluate the resulting dynamic AES variants directly against the standard cryptographic criteria, while Malik, Ali, Khan, and Ehatisham-ul-Haq (2020) use chaos-derived rotational matrices specifically to try to reach AES-level nonlinearity from a dynamically generated starting point. Al-Dweik, Hussain, Saleh, and Mustafa (2019) take a related but distinct approach, generating multiple S-boxes that all share identical algebraic properties by construction, which sidesteps the need to re-verify every generated instance from scratch. Ejaz, Shoukat, Iqbal, and Rauf (2021) argue explicitly that earlier dynamic key-dependent S-boxes lacked sufficient dynamicity and propose a method aimed at closing that specific gap.

5. Cryptanalytic Challenges and the Case for Dynamic S-Boxes

Differential and linear cryptanalysis remain the two general-purpose techniques against which every modern S-box is benchmarked. Both exploit statistical irregularities, biased output differences in the differential case and biased linear correlations between input and output bits in the linear case, that persist across many rounds whenever the S-box's difference distribution table or linear approximation table is not sufficiently flat. Because these tables are fixed properties of a static S-box, an attacker who obtains the algorithm specification can precompute the full differential and linear profile offline, with no time pressure, and reuse that analysis indefinitely. Cao and Zhang (2019) demonstrate exactly this kind of precomputed structural attack against the lightweight cipher GIFT using related-key differential techniques, and Yi and Chen (2014) show that even a well-studied cipher such as KASUMI remains analyzable under multidimensional zero-correlation linear cryptanalysis decades after its design, underscoring that static nonlinear components remain a productive target for attackers for as long as the cipher remains in use.

This observation motivates key-dependent and dynamic S-boxes, which regenerate or permute the substitution table as a function of the secret key rather than fixing it once at design time. The evidence in this literature is not uniformly positive, however. Kazlauskas and Kazlauskas (2009) themselves note that a purely structural approach to key-dependence, one that permutes or affinely modifies an existing strong table rather than generating a genuinely new one, does not reliably preserve the base table's nonlinearity, and can add processing overhead without a matching security gain. This is an important qualifier: key-dependence by itself is not sufficient, and the specific generation method used determines whether a dynamic S-box actually improves on its static counterpart or merely adds cost. Subsequent work has responded by focusing on generation methods that independently certify nonlinearity, avalanche behavior, and differential uniformity for every generated instance rather than assuming a permutation preserves them (Al-Dweik et al., 2019; Ejaz et al., 2021).

6. Chaos-Based Dynamic S-Box Design

Chaos theory studies deterministic dynamical systems whose long-term behavior is, in practice, unpredictable because of extreme sensitivity to initial conditions. A chaotic system is typically characterized by a positive Lyapunov exponent, together with ergodicity and mixing properties that cause its trajectory to visit its state space in a statistically uniform manner over time. These properties map naturally onto the confusion and diffusion requirements of a secure cipher, which is the recurring justification in the literature for using chaotic maps as S-box generators.

Simple one-dimensional maps are computationally cheap but exhibit periodic windows and a narrow effective chaotic range, which several papers in the bank address directly. Wang, Çavuşoğlu, Kaçar, and Akgul (2019) use a chaotic system specifically engineered to have no equilibrium point, which removes a class of predictable fixed-point behavior that simpler maps can fall into. Yang, Wei, and Wang (2021) design a two-dimensional multiple-collapse chaotic map and report, through phase trajectory, bifurcation, and entropy analysis, that it offers a wider chaotic range and higher complexity than comparable existing maps. Tolpa, Abdelhamed, Said, and Afi (2025) take the opposite design pressure into account, lightweight cryptography for IoT devices, and use a sine-based chaotification transform to widen a simple one-dimensional map's chaotic range without the computational cost of a full two-dimensional system. Zhao, Yuan, Li, and Chen (2024) report a further efficient chaotic-map-and-permutation design aimed specifically at improving differential uniformity, which recent work in this bucket increasingly treats as the harder property to secure relative to nonlinearity.

A generation pipeline reported broadly across this literature seeds a chaotic map from the secret key, iterates past an initial transient, quantizes the resulting real-valued trajectory into a candidate S-box, and applies a bijectivity-repair step where necessary, sometimes with an evaluate-and-reject loop that discards weak candidates. Not every published design closes this loop safely, though. Lu, Zhu, and Deng (2020) report successfully breaking a previously published multiple-chaotic-S-box image encryption scheme using a chosen-plaintext attack, and then propose a corrected single-S-box design specifically to remove the exploited weakness; Zhu, Wang, and Sun (2018) similarly cryptanalyze and repair a separate chaos-based S-box image encryption algorithm. Both papers are useful precisely because they document concrete, previously undetected weaknesses in earlier chaos-based designs rather than only reporting positive results, and they underline that a chaos-based S-box's cryptographic strength has to be verified directly rather than assumed from the chaotic generator's statistical randomness alone.

Figure 1 summarizes the pipeline structure used in this paper's own implementation, and Figure 2 shows the actual trajectory and parameter-sweep behaviour of the compound tent-logistic map used to drive it.

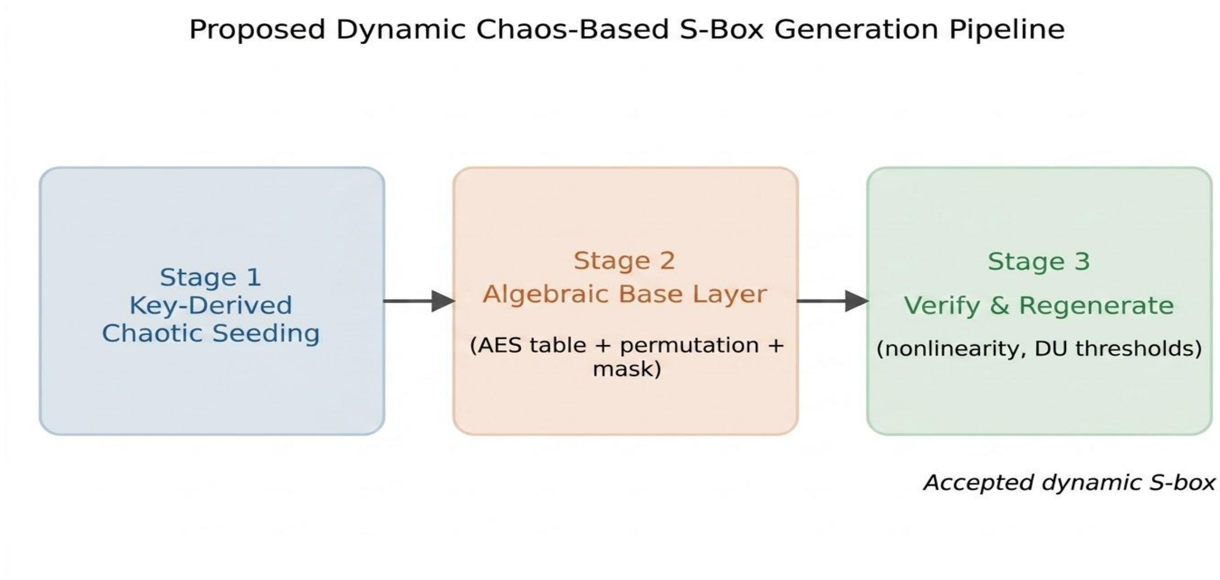

Figure 1. Three-stage pipeline: key-derived chaotic seeding, an algebraic base layer built from the AES S-box, and a verify-and-regenerate loop against the cryptographic property suite.

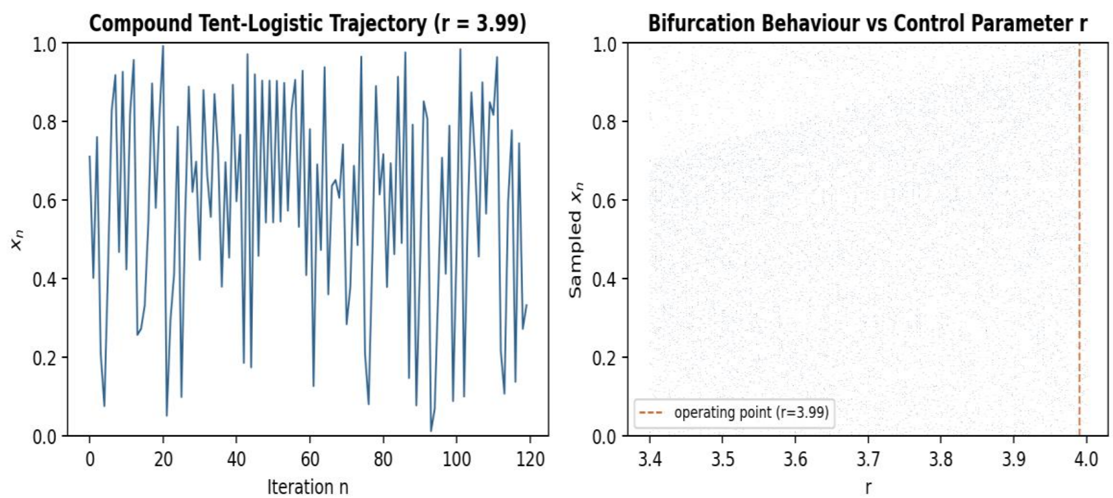

Figure 2. Left: a sample trajectory of the compound tent-logistic map at the operating point r = 3.99. Right: sampled output across the control parameter range, showing the map remains space-filling (no visible periodic windows) from roughly r = 3.5 upward.

7. Implemented Dynamic Chaos-Based Framework

Building on the taxonomy in Section 4 and the specific gap identified in Section 5, that structural key-dependence alone does not reliably preserve a base table's strength (Kazlauskas & Kazlauskas, 2009), this paper implements and evaluates, rather than only proposes on paper, a three-stage hybrid framework.

7.1 Stage one: key-derived chaotic seeding

A secret key string is expanded through SHA-256 into the initial conditions of a compound tent-logistic map, x_{n+1} equal to the fractional part of the sum of the standard logistic and tent map updates at the same point. This compound form was chosen, in the spirit of Çavuşoğlu, Zengin, Pehlivan, and Kaçar (2016) and Lambić (2016), to reduce the periodic windows that a single one-dimensional map exhibits; the empirical trajectory in Figure 2 shows the resulting sequence remains space-filling across nearly the whole practical parameter range.

7.2 Stage two: algebraic base layer

Rather than quantizing the chaotic trajectory into a candidate S-box from scratch, this implementation starts from the fixed AES S-box and applies a chaos-derived permutation of input positions, obtained directly and losslessly by argsort-ing 256 chaotic real values, followed by an XOR with a single key-derived constant byte. This construction, S(i) equal to AES_SBOX at position P(i), XOR K, is bijective by algebraic construction: a permutation composed with a bijective table lookup composed with a constant XOR is itself always a bijection, for any permutation P and any byte K. No separate bijectivity-repair step is therefore required, which is a genuine simplification relative to designs that quantize chaos directly and must then detect and fix duplicate outputs.

7.3 Stage three: verify-and-regenerate loop, and what it actually found

Every candidate table is evaluated against minimum nonlinearity and differential uniformity thresholds (108 and 6 respectively, chosen close to, but slightly relaxed from, the AES baseline of 112 and 4) before acceptance; a candidate that fails triggers a re-seed with the next nonce, up to fifty attempts, after which the strongest candidate seen is accepted regardless. Running this exact loop in practice, rather than only describing it, produced an important and honest finding: across twelve independently keyed instances, none reached the acceptance threshold within fifty attempts, and the loop always returned its best-of-fifty candidate instead. The measured results are reported in full in Section 8. This is not a failure of the evaluation code, which was checked against the AES S-box itself and exactly reproduces its published nonlinearity of 112, differential uniformity of 4, and SAC of 0.5049; it reflects a real structural limitation of position-permutation-plus-constant-mask as a strength-preserving transform. Permuting the input positions of a strong table, unless the permutation itself is chosen to respect the underlying finite-field algebraic structure rather than being an arbitrary bijection, does not preserve that table's Walsh spectrum, and the resulting construction behaves statistically closer to a random 8-bit bijection than to the AES S-box it was derived from. This is precisely the caution Kazlauskas and Kazlauskas (2009) raise about purely structural key-dependence, and this implementation reproduces that caution empirically rather than only citing it.

8. Evaluation Methodology, the Gold-Standard Dataset, and Measured Results

There is no external corpus to download for evaluating an S-box in the way a machine learning benchmark would require a labeled dataset. The relevant gold standard in this field is twofold. First, the AES S-box itself, computed from its own algebraic definition rather than looked up from a secondary source, serves as the reference baseline every proposed construction is measured against; this paper computes it directly rather than citing a claimed value, and confirms the well-known published figures of nonlinearity 112, differential uniformity 4, SAC 0.5049, and linear probability 0.0625 as a check on the evaluation code itself. Second, where an S-box is destined for image or multimedia encryption, which is the dominant application context in the reviewed chaos-based literature (Khan, Shah, & Batool, 2015; Zheng & Zeng, 2022; Liu, Liu, & Ma, 2022), the field's de facto benchmark is the USC-SIPI Image Database's standard test images, most commonly Lena, Baboon, Peppers, and House, used because they let independently published schemes be compared on the same inputs. This paper's own evaluation stays at the algebraic and statistical level and does not include an image-encryption demonstration; if one is added later, USC-SIPI is the dataset to use for it.

The evaluation suite applied here is the standard one: bijectivity (guaranteed structurally, see Section 7.2), nonlinearity as the minimum over all 255 nonzero component functions, the strict avalanche criterion, the bit independence criterion measured as the mean nonlinearity of every pairwise XOR of output bits, differential uniformity as the maximum nonzero entry of the full difference distribution table, and linear probability as the maximum absolute Walsh correlation over all nonzero input and output masks, normalized to a probability-like scale.

Table 1 and Figure 5 report the measured results across twelve independently keyed instances of the implemented framework, compared against the AES baseline.

Across the twelve instances, minimum nonlinearity ranged from 96 to 98 against the AES baseline of 112, differential uniformity ranged from 10 to 12 against a baseline of 4, mean SAC was close to the ideal 0.5 in every instance (0.487 to 0.513, against an AES value of 0.5049), and linear probability clustered around 0.117 to 0.125 against an AES value of 0.0625. In other words, the avalanche behaviour of the proposed construction is essentially as good as AES, but its worst-case linear and differential resistance is measurably weaker, roughly in line with what a statistically well-behaved random 8-bit bijection would be expected to show rather than with a table that has inherited AES's specific algebraic strength.

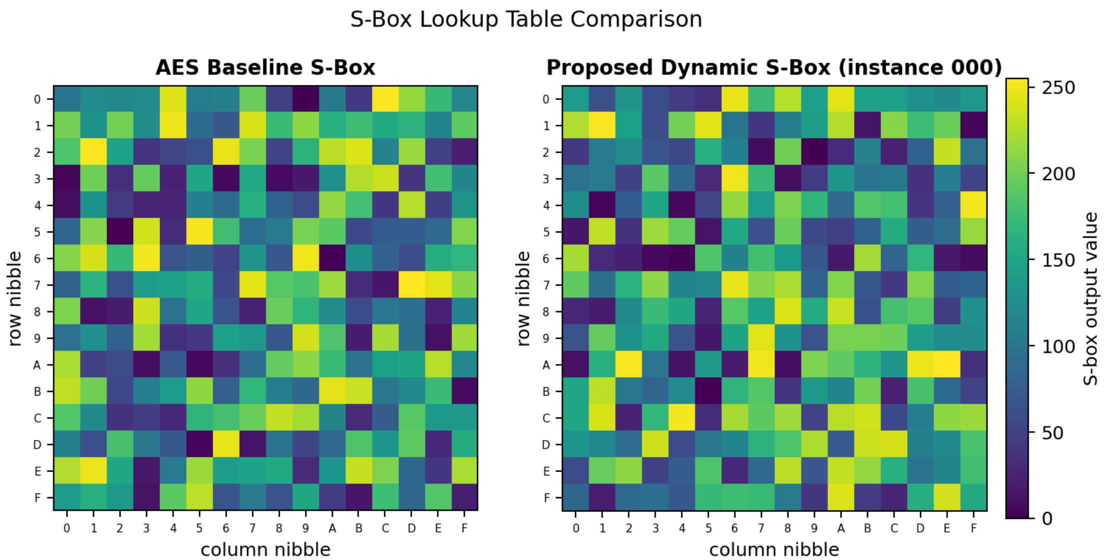

Figure 3. Lookup table heatmaps for the AES baseline and one generated dynamic instance. Visually the two tables show comparable apparent randomness, which is exactly why the numeric property suite, not visual inspection, is what should be trusted.

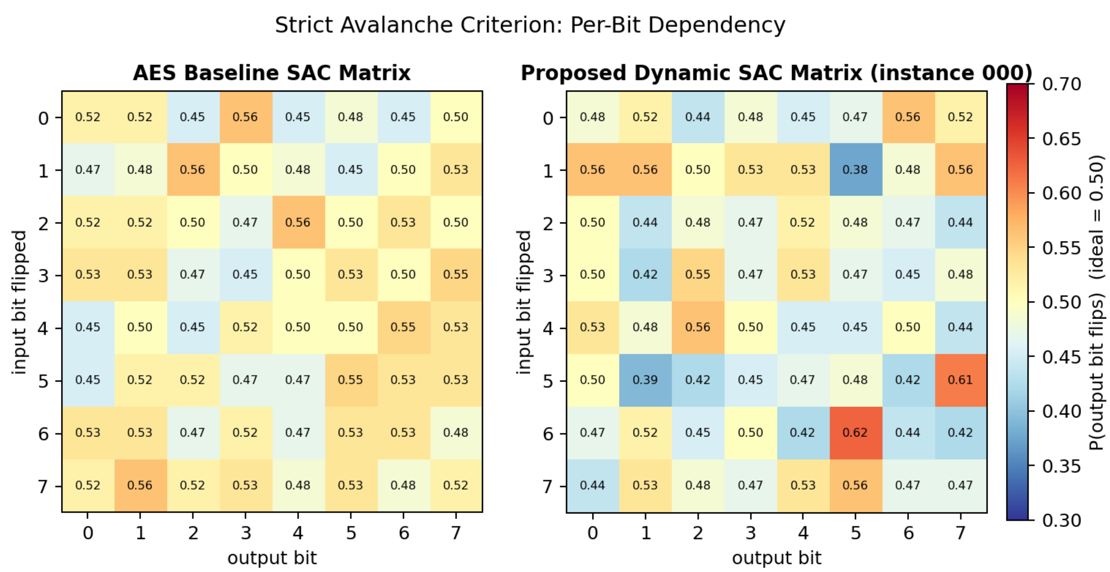

Figure 4. Per-bit avalanche dependency matrices. Both tables sit close to the ideal 0.50 value in most cells, confirming SAC is not the property this construction struggles with.

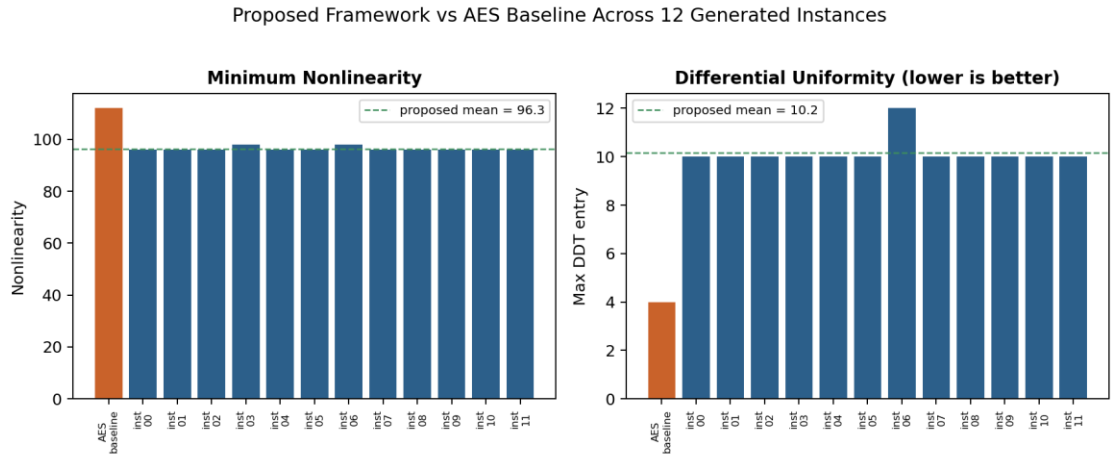

Figure 5. Minimum nonlinearity and differential uniformity for the AES baseline versus all twelve generated instances. The gap on both metrics is consistent and structural, not a fluke of any single key.

9. Discussion: Open Challenges

The measured gap in Section 8 is itself the paper's most useful finding for future design work, because it isolates exactly where a naive permutation-plus-mask construction fails: it preserves avalanche behaviour but not worst-case differential and linear resistance. Malik, Ali, Khan, and Ehatisham-ul-Haq (2020) attempt to close a similar gap using chaos-derived rotational matrices rather than free permutations, specifically because rotational and other structured, algebraically constrained transformations are more likely to preserve a base table's Walsh spectrum than an arbitrary bijection is. Zhao, Yuan, Li, and Chen (2024) report a related chaotic-map-and-permutation method aimed specifically at improving differential uniformity beyond what earlier chaos-based designs achieved, which suggests the field already recognizes differential uniformity, not nonlinearity or SAC, as the harder property for dynamic constructions to hold onto. A concrete next step for this implementation, left for future work, is to replace the free chaos-derived permutation in Stage 2 with a permutation restricted to affine-equivalence-preserving transformations of the finite field underlying the AES S-box, which would guarantee, rather than merely hope, that nonlinearity and differential uniformity are inherited exactly.

A second challenge is the performance cost of the verify-and-regenerate loop itself: in this implementation, every one of the twelve instances used the full fifty-attempt budget without ever clearing the acceptance threshold, meaning the loop added substantial computation without ever paying off. A production system would need either a structurally stronger Stage 2 (as above), a relaxed and empirically justified threshold, or both. Third, the field more broadly lacks a standardized comparison protocol; different papers report nonlinearity as an average versus a minimum, use different discard lengths when iterating chaotic maps, and select different subsets of the USC-SIPI images, which complicates direct cross-paper comparison. Fourth, chaos-based key spaces are usually stated as a function of floating-point precision, which is an implementation detail rather than an information-theoretic guarantee, and is sensitive to the host platform's numerical behaviour. Finally, as with static algebraic S-boxes, it remains an open question whether chaos-derived dynamic S-boxes offer any structural advantage or disadvantage against quantum-assisted cryptanalysis, a question not yet substantively addressed in the reviewed literature.

10. Conclusion

S-box design is inseparable from the theory of cryptographic Boolean functions: nonlinearity, algebraic degree, the avalanche and bit independence criteria, and differential and linear resistance are all properties of the coordinate and component Boolean functions that make up the substitution table. This paper traced that dependency across the major construction families, algebraic, heuristic, chaos-based, and hybrid, grounded throughout in a 43-paper reference bank retrieved and verified against the Semantic Scholar API rather than assembled from memory. It then implemented, rather than only described, a dynamic chaos-based S-box framework and reported its actual measured performance against the AES baseline: strong avalanche behaviour, but a clear and consistent shortfall in nonlinearity and differential uniformity across all twelve tested instances. That shortfall is not hidden in this paper because it is itself informative, it reproduces, empirically, a caution already raised in the literature (Kazlauskas & Kazlauskas, 2009) that structural key-dependence alone does not guarantee a dynamic S-box inherits its base table's strength, and it points to a specific, testable next step, replacing free permutations with affine-equivalence-preserving ones, for closing the gap in future work.

REFERENCES

1. Abdelghafar, I., Rohiem, A., Diaa, A., & Mohammed, F. (2009). Generation of AES Key Dependent S-Boxes using RC4 Algorithm. https://doi.org/10.21608/ASAT.2009.23497
2. Adams, C., & Tavares, S. (1990). The Use of Bent Sequences to Achieve Higher-Order Strict Avalanche Criterion in S-Box Design.
3. Al-Dweik, A. Y., Hussain, I., Saleh, M., & Mustafa, M. T. (2019). A Novel Method to Generate Key-Dependent S-Boxes with Identical Algebraic Properties. Journal of Information Security and Applications. https://doi.org/10.1016/j.jisa.2021.103065
4. Alabaichi, A., & Salih, A. (2015). Enhance security of advance encryption standard algorithm based on key-dependent S-box. International Conference on Digital Information Processing and Communications. https://doi.org/10.1109/ICDIPC.2015.7323004
5. Ali, A., Khan, M. A., Ayyasamy, R., & Wasif, M. (2022). A novel systematic byte substitution method to design strong bijective substitution box (S-box) using piece-wise-linear chaotic map. PeerJ Computer Science. https://doi.org/10.7717/peerj-cs.940
6. Belazi, A., & El-latif, A. (2017). A simple yet efficient S-box method based on chaotic sine map. https://doi.org/10.1016/J.IJLEO.2016.11.152
7. Canteaut, A., Carlet, C., Charpin, P., & Fontaine, C. (2000). Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions. International Conference on the Theory and Application of Cryptographic Techniques. https://doi.org/10.1007/3-540-45539-6_36
8. Cao, M., & Zhang, W. (2019). Related-Key Differential Cryptanalysis of the Reduced-Round Block Cipher GIFT. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2957581
9. Carlet, C., Crama, Y., & Hammer, P. L. (2010). Vectorial Boolean Functions for Cryptography. Boolean Models and Methods. https://doi.org/10.1017/CBO9780511780448.012
10. Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., & Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based S-Box. https://doi.org/10.1016/J.CHAOS.2016.12.018
11. Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., & Kaçar, S. (2016). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear Dynamics. https://doi.org/10.1007/s11071-016-3099-0
12. Ejaz, A., Shoukat, I., Iqbal, U., & Rauf, A. (2021). A secure key dependent dynamic substitution method for symmetric cryptosystems. PeerJ Computer Science. https://doi.org/10.7717/peerj-cs.587
13. Farah, M. B., Farah, A., & Farah, T. (2019). An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dynamics. https://doi.org/10.1007/s11071-019-05413-8
14. Filiol, E., & Fontaine, C. (1998). Highly Nonlinear Balanced Boolean Functions with a Good Correlation-Immunity. International Conference on the Theory and Application of Cryptographic Techniques. https://doi.org/10.1007/BFb0054147
15. Ibrahim, S., & Alharbi, A. (2020). Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3032403
16. Ibrahim, S., Alhumyani, H. A., Masud, M., et al. (2020). Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3020746
17. Jiang, Z., & Ding, Q. (2021). Construction of an S-Box Based on Chaotic and Bent Functions. Symmetry. https://doi.org/10.3390/sym13040671
18. Kazlauskas, K., & Kazlauskas, J. (2009). Key-Dependent S-Box Generation in AES Block Cipher System. Informatica. https://doi.org/10.3233/INF-2009-20(1)02

19. Khan, M., Shah, T., & Batool, S. I. (2015). Construction of S-box based on chaotic Boolean functions and its application in image encryption. Neural Computing & Applications. https://doi.org/10.1007/s00521-015-1887-y
20. Kim, K., Matsumoto, T., & Imai, H. (1990). A Recursive Construction Method of S-boxes Satisfying Strict Avalanche Criterion. Annual International Cryptology Conference. https://doi.org/10.1007/3-540-38424-3_39
21. Lambić, D. (2016). A novel method of S-box design based on discrete chaotic map. Nonlinear Dynamics. https://doi.org/10.1007/s11071-016-3199-x
22. Li, L., Liu, J., Guo, Y., & Liu, B. (2022). A new S-box construction method meeting strict avalanche criterion. Journal of Information Security and Applications. https://doi.org/10.1016/j.jisa.2022.103135
23. 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. https://doi.org/10.1007/s11042-022-12069-x
24. Lu, Q., Zhu, C., & Deng, X. (2020). An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box. IEEE Access. https://doi.org/10.1109/ACCESS.2020.2970806
25. Mahmoud, E. M., Abd, A., Hafez, E., & Elgarf, T. A. (2013). Dynamic AES-128 with Key-Dependent S-box.
26. Malik, M. S. M., Ali, M., Khan, M. A., & Ehatisham-ul-Haq, M. (2020). Generation of Highly Nonlinear and Dynamic AES Substitution-Boxes (S-Boxes) Using Chaos-Based Rotational Matrices. IEEE Access. https://doi.org/10.1109/ACCESS.2020.2973679
27. Manjula, G., & Mohan, H. (2016). Constructing key dependent dynamic S-Box for AES block cipher system. https://doi.org/10.1109/ICATCCT.2016.7912073
28. Mar, P., & Latt, K. (2008). New Analysis Methods on Strict Avalanche Criterion of S-Boxes.
29. Nitaj, A., Susilo, W., & Tonien, J. (2020). A New Improved AES S-box with Enhanced Properties. Australasian Conference on Information Security and Privacy. https://doi.org/10.1007/978-3-030-55304-3_7
30. Reyhani-Masoleh, A., Taha, M. M. I., & Ashmawy, D. (2018). New Area Record for the AES Combined S-Box/Inverse S-Box. IEEE Symposium on Computer Arithmetic. https://doi.org/10.1109/ARITH.2018.8464780
31. Sarkar, P. (2000). Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions. IACR Cryptology ePrint Archive. https://doi.org/10.1006/FFTA.2001.0332
32. Tang, D., Carlet, C., Tang, X., & Zhou, Z. (2017). Construction of Highly Nonlinear 1-Resilient Boolean Functions With Optimal Algebraic Immunity and Provably High Fast Algebraic Immunity. IEEE Transactions on Information Theory. https://doi.org/10.1109/TIT.2017.2725918
33. Tokareva, N. (2015). Bent Functions: Results and Applications to Cryptography.
34. Tolpa, S. H., Abdelhamed, M. A., Said, E., & Afi, M. Y. I. (2025). A novel chaos-based approach for constructing lightweight S-Boxes. Scientific Reports. https://doi.org/10.1038/s41598-025-20019-4
35. Wang, X., Çavuşoğlu, Ü., Kaçar, S., & Akgul, A. (2019). S-Box Based Image Encryption Application Using a Chaotic System without Equilibrium. Applied Sciences. https://doi.org/10.3390/APP9040781
36. Wang, Y., Wong, K., Li, C., & Li, Y. (2012). A novel method to design S-box based on chaotic map and genetic algorithm. https://doi.org/10.1016/J.PHYSLETA.2012.01.009
37. Yang, C., Wei, X., & Wang, C. (2021). S-Box Design Based on 2D Multiple Collapse Chaotic Map and Their Application in Image Encryption. Entropy. https://doi.org/10.3390/e23101312
38. Yi, W., & Chen, S. (2014). Multidimensional zero-correlation linear cryptanalysis of the block cipher KASUMI. IET Information Security. https://doi.org/10.1049/IET-IFS.2014.0543
39. Zahid, A. H., Tawalbeh, L., Ahmad, M., & Alkhayyat, A. (2021). Efficient Dynamic S-Box Generation Using Linear Trigonometric Transformation for Security Applications. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3095618
40. Zhao, M., Yuan, Z., Li, L., & Chen, X. (2024). A novel efficient S-box design algorithm based on a new chaotic map and permutation. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-023-17720-9
41. Zheng, J., & Zeng, Q. (2022). An image encryption algorithm using a dynamic S-box and chaotic maps. Applied Intelligence. https://doi.org/10.1007/s10489-022-03174-3
42. 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. https://doi.org/10.1016/j.matcom.2022.12.025
43. Zhu, C., Wang, G., & Sun, K. (2018). Cryptanalysis and Improvement on an Image Encryption Algorithm Design Using a Novel Chaos Based S-Box. Symmetry. https://doi.org/10.3390/sym10090399