Enhancing Block Cipher Security: An Advanced Proposal for S-Box Design

Saad Abdullah

Mälardalen University, Västerås, Sweden

Correspondence:
Saad Abdullah: Saad.abdullah@mdu.se

Article Link: https://www.brainetwork.org/index.php/jcai/article/view/16

Volume 1, Issue 2, 2023

Funding
No

Citation: Abdullah, S. (2023). An advanced proposal of S-Boxes using block ciphers, *Journal of Computing and Artificial Intelligence, 1*(2), 28-39.

Conflict of Interest: Authors declared no Conflict of Interest

Acknowledgment: No administrative and technical support was taken for this research

Article History

Submitted: Sep 18, 2023
Last Revised: Oct 10, 2023
Accepted: Nov 28, 2023

An official Publication of
Beyond Research Advancement & Innovation Network, Islamabad, Pakistan

Enhancing Block Cipher Security: An Advanced Proposal for S-Box Design

Saad Abdullah*

Mälardalen University, Västerås, Sweden

Abstract

In this paper, we tend to intend towards skill a completely unique method used for planning cryptographically solid Substitution boxes persecution boxes polynomial representing. The projected CPM is skillful to draw the contribution system to a powerful 8 × 8 Substitution-box assembly the necessities of a bijective purpose. The employment of CPM keeps the ease of Substitution-boxes assembly technique and located reliable when put next with alternative existing S-box methods won't to make Substitution-boxes. Associate in nursing example planned Substitution-boxes is acquired that is systematically calculated by normal show principles as well as NL, bijection, BI, SAC, linear estimate possibility, and DU. The piece consequences are compared with some newly analyzed S-boxes to determine its crypto logical strength. The vital studies approve projected S-boxes making method is meaningfully originally real to get cryptographically secure s-box.

Keywords: s-boxes; cpm; block ciphers; cryptanalysis

Introduction

Modern technical inventions Associate in tending their fertile practice now reality must bring about in a massive development within the capacity of knowledge existence connected [1]. The complex environment of information strains designed for methods towards remain advanced then actions to protector after misappropriation. Previously program, an operator's information should remain altered popular such a kind no

* Corresponding Author: Saad.abdullah@mdu.se

meaningful to an assailant [2]. Bilaterally ciphers are between the leading wide recycled method to satisfy this resolve thanks to the open execution and existence the suppliers of abundant required science asset. Unique famous sort of ciphers makes use of s-box and p-box acts [3]. This sort of chunk cipher transmutes an enter block of information right obsessed by a worthless yield block with the aid of using the use of a symmetric key and unique wide variability of sequences. Normally, every spherical play sbox and pbox strategies at the enter block of information. A substitution technique changes an enter block through any other yield block the use of substitution box (S-box). AES such as an instance, is maximum typically jumble-sale symmetric block cipher. An S-Box is a significant element of latest block ciphers and produces a jumbled encryption text from the assumed message. A Substitution-Boxes existence the simplest NL basic of contemporary-day block ciphers, gives a complicated dating among the message and the cipher text [4]. This relative is known as misunderstanding. So on safety a block cipher presents is dependent at the mistake with inside the cipher text shaped through Substitution-Boxes. As an outcome, many researchers are designing unique S-box and comparing the electricity in their own Substitution-Boxes in opposition to a few standard benchmarks including bijective-ness, SAC, NL, BIC, linear and DP. In, some of houses had been advised to be existent in an S-container which will face up to diverse cryptanalytic attacks. An S-container keeping maximum of those houses presents extra safety [5].

Related Work

Now works, some of schemes and kit are followed intended for mixture of cryptographically strong Sbox. Projected a way to construct fountains of lively and resistant S-bins that can help even as modifying the block security. An S-field consuming extreme NL affords greater struggle in opposition to direct cryptanalysis. Advanced Encryption Standard employments extremely NL S-field in its numerous sequences for the encryption and decryption processes [6]. Proposed one-of-a-kind

improvements to the safety provided via way of means of AES via way of means of improving the Advanced Encryption Standard S-field in one-of-a-kind aspect. A block cipher consuming fixed S-field employments the unaffected S-field in every round. A static S-box lets in the attackers towards check out Substitution box capabilities, find out its flaws, and besides subsequently get a threat of cryptanalysis of the scrambled cipher text formed via way of means of the block cipher [7]. Owing to the constraints of static Sbox, a massive wide variety of investigators have discovered the thoughts for S-field layout together with randomness, dynamicity, and key-dependency. Typically, a key-established and active S-field improves the energy of the own block cipher. For example, used key-established S-bins and proposed techniques to provide huge amount of sturdy S-Boxes [8]. Authors planned key-established dynamic S-bins and examine display that planned S-boxes are cryptographically actual sturdy. Specified numerous incompetence like brought giving out time, etc. and found in key-established S-boxes. Writers planned improvements in AES via way of means of introducing key-established S-field. The SAC impact is unique of the several wished sites of today's cipher. This function of cipher requires that only bit amendment with inside the message or key ought to make large versions with inside the ensuing message [9]. Small price of SAC impact suggests a feebler block cipher, and subsequently the message produced via way of means of such cipher can be a sufferer of a cryptographically determination. Several easy techniques planned in may be used efficaciously toward analyze SAC and examine a specified S-Box for fullness and cryptographic energy [10]. Writers studied and different S-bins, appraised their avalanche impact, and decided that AES S-boxes have the most avalanche impact. Active Substitution planned via way of means of exhibit decent avalanche impact in comparison to the usual S-boxes. Further evaluation of the proposed and Substitution exhibits that Advanced Encryption Standard and novel ciphers are unbiased of every different and AES has greater effectiveness [11]. Chaos is a customary display with capabilities of compassion, uncertainty, unfolds range, periodicity. These

chaos landscapes mark chaotic structures as a preference for the growth of cutting-edge ciphers and lots of Writers have used chaos with inside the layout of Substitution box. Writers advised S-boxes primarily based totally on chaotic plot and examined those together with the opposite current S-field layout techniques. Examines revealed that the planned Sbox are sturdy in opposition to one of kind assaults and subsequently advise their utilization in cutting-edge block ciphers [12]. Advanced shape of chaos known as hyper chaotic is denser than the chaos in opposition to cryptanalysis hard work because of its active difficulties. Using its energy, writers planned some of S-boxes primarily based totally on hyper chaotic standards even as every S-field may be very powerful manner the capabilities like SAC, BIC. A device is wanted to significantly examine an S-field and test its safety in opposition to a few general standards [13]. The writers of have advanced an application to assess the cryptographic overall act of any S-box. In this weekly, a green method to assemble S-bins has been advised. The planned technique is a pioneering one and various from the techniques provided with inside the fiction as we've got endorsed a CPM and discovered it aimed at the layout of strong S-Boxes. Subsequently the development of an S-Box, its performance evaluation consumes stayed executed to assess its cryptographic energy [14]. An assessment by different currently planned Substitution evokes approximately its energy. The logical effects inspire using the planned Substitution-Box in innovative block ciphers. The agency of the reduction of the weekly is by way of monitors. Segment proposals the layout of the proposed S-Box. Act evaluation of the proposed S-Box in opposition to cryptographic sites is discussed in Piece and an assessment is complete with a few these days designed S-boxes. Section4completes the studies paper with assumptions [15].

Planned S-Box Design

Best of the symmetric block encryptions usage unique before additional Substitution box for swap drive towards carry now the important error. An S-box delivers the misunderstanding ability among the plaintext and the

cipher text finished a NL representing [16]. The scholars need widely traveled such NL mappings to idea Substitution boxs having diverse cryptographic benefit. Yet, the procedure of Substitution structure by these methods is very compound and incompetent.

We existing a actual modest and well-organized

$$c(t) = [a * t^3 + b](MOD(2^n + 1)) \quad t \in N. \quad (1)$$

Where N= {0, 1… 2n -1}

a = 69, and b = 100.

When T= 135, C(t) calculates to 256 $\notin$ N. Design 16×16 S-box in Table 1.

Table 1

Planned Substitution-Box.

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

Results and Discussions

Now this piece, we examine our new method then offered S-box assumed in Table1for largely well-known average Substitution boxes performance scales towards size its cryptographic power[17].

A. Bijectiveness

Used aimed at binary groups x and y, a function f: x ⟶ y is bijective only if it is 1to1 and onto instantaneously. 1to1 charting needs that apiece part of usual x is similar with objective one part of group y [18]. Onto charting

necessitates that apiece part of group y has different pre-image in group x. CPM function C: N ⟶ N is bijective by way of it yields separate production figures for separate input figures having image(C) = N and pre-image(C) = N, where N = {0, 1, . . . , 254, 255}.

B. Strict Avalanche Criterion (SAC)

The SAC standard is an imperious article for slightly cryptographic S-box which defines that uncertainty a solo little is altered in the input, this alteration would change partial of the yielding whiles. An S-box requiring a figure of SAC nearer to 0.5 has fair inconsistency [19]. Dependence medium given that the SAC figures of projected S-box are given in Table2. It is patent from Table2 that the regular Strict Avalanche Criterion significance of the S-Box is equivalent to 0.5. This Strict Avalanche Criterion assessment is a sign that the planned S-box pleases Strict Avalanche Criterion stuff in a reputable way.

Table 2

Dependence matrix SAC figures.

0.500	0.469	0.500	0.516	0.547	0.453	0.563	0.469
0.531	0.578	0.453	0.500	0.453	0.484	0.531	0.531
0.531	0.484	0.547	0.531	0.594	0.469	0.516	0.484
0.469	0.531	0.500	0.516	0.453	0.547	0.531	0.516
0.438	0.531	0.406	0.500	0.500	0.453	0.547	0.484
0.563	0.500	0.453	0.500	0.531	0.453	0.468	0.547
0.563	0.516	0.531	0.547	0.469	0.422	0.531	0.531
0.547	0.563	0.438	0.578	0.516	0.516	0.516	0.500

C. *Non-Linearity*

If a Substitution box is designed in a way that introduces linear correlation between the plaintext and the ciphertext, it becomes vulnerable to linear cryptanalysis attacks, allowing adversaries to recover the original plaintext [20].

The Nonlinearity (NL) values of our Substitution box range from 104 to 108, with an average of 106.8. These NL values indicate the resistance of the Substitution box against linear attacks [21]. The NL values of all 8 fundamental Boolean functions are also presented in Table 3.

Table 3

NLs of essential Boolean purposes of planned Substitution box

Boolean Function	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
Nonlinearity	106	104	106	108	108	106	108	108

In Table 4, we make an evaluation of planned Substitution box and other modern S-boxes with respect to NL metric.

Table 4

Changed S-boxes and the individual NL figures.

S-box Method	Minimum	Maximum	Average
[17]	98	108	102.5
[28]	96	110	104.3
[30]	102	108	105.3
[38]	102	108	105.3
[43]	102	108	104.5
[44]	104	110	106
[48]	98	108	104
[54]	98	108	104
[55]	102	106	104
[56]	102	108	105.3
[57]	100	110	105.5
[58]	104	106	105.3
[59]	100	108	105.7
[60]	100	108	104.8
[61]	94	104	99.5
[62]	96	108	103.5
[63]	100	106	103.3
[64]	84	106	100
[65]	100	108	104.5
Proposed	104	108	106.8

D. Bit Independence Criterion (BIC)

According to this criterion, enhancing a response bit p should not impose any constraints on the output bits q and r individually. An ideal S-box ensures that the output bits are independent of each other, thereby strengthening security [22]. If an S-box achieves Balancedness in the number of Input Coincidences (BIC) assets, it enhances security further. Tables 5 and 6 display the Nonlinearity (NL) and Strict Avalanche Criterion (SAC) standards for the fundamental Boolean functions of the proposed Substitution.

Table 5

BIC results for NL.

Boolean Function	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
b_1	-	104	106	106	104	104	102	102
b_2	104	-	104	102	108	104	104	100
b_3	106	104	-	104	102	104	108	106
b_4	106	102	104	-	106	106	100	102
b_5	104	108	102	106	-	108	106	100
b_6	104	104	104	106	108	-	98	106
b_7	102	104	108	100	106	98	-	104
b_8	102	100	106	102	100	106	104	-

Table 6

BIC results for SAC.

Boolean Function	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
b_1	-	0.502	0.510	0.506	0.500	0.504	0.484	0.477
b_2	0.502	-	0.512	0.479	0.510	0.488	0.512	0.518
b_3	0.510	0.512	-	0.479	0.520	0.492	0.461	0.500
b_4	0.506	0.479	0.479	-	0.504	0.518	0.520	0.467
b_5	0.500	0.510	0.520	0.504	-	0.521	0.498	0.510
b_6	0.504	0.488	0.492	0.518	0.521	-	0.488	0.512
b_7	0.484	0.512	0.461	0.520	0.498	0.488	-	0.504
b_8	0.477	0.518	0.500	0.467	0.510	0.512	0.504	-

E. Linear Probability

The cryptologist of recent block ciphers tries to make sufficient misunderstanding then dissemination of bits to safe the information alongside cryptanalytic determinations. Solid S-boxes assistance in attaining these necessities over NL mapping between input and output. An S-box consuming little LP specifies advanced NL planning and delivers opposition alongside the direct cryptanalysis [23].

F. *Differential Probability*

Difference cryptanalysis is careful such by way of a valuable implement to grip the unique plaintext. Throughout this work, alterations in the plaintext and the cipher text are initiate. The connection of these modifications supports the defenders to reach certain portion of the key. A little significance of DP assistances in attacking this occurrence [24]. DP is planned as

Table 7

Act comparison of changed S-boxes.

S-box Method	Nonlinearity Min.	Max.	Average	SAC	BIC-NL	LP	DP
[17]	98	108	102.5	0.492	103.3	0.141	0.062
[28]	96	110	104.3	0.497	103.4	0.133	0.047
[30]	102	108	105.3	0.491	103.6	0.133	0.039
[38]	102	108	105.3	0.496	103.8	0.156	0.039
[43]	102	108	104.5	0.498	104.6	0.125	0.047
[44]	104	110	106	0.520	104.2	0.132	0.039
[48]	98	108	104	0.505	103.4	0.133	0.250
[54]	98	108	104	0.507	102.9	0.086	0.047
[55]	102	106	104	0.498	102.9	0.148	0.039
[56]	102	108	105.3	0.502	103.7	0.125	0.047
[57]	100	110	105.5	0.499	106	0.133	0.125
[58]	104	106	105.3	0.504	104.6	0.133	0.039
[59]	100	108	105.7	0.498	104.3	0.109	0.047
[60]	100	108	104.8	0.501	105.1	0.125	0.125
[61]	94	104	99.5	0.516	101.7	0.132	0.281
[62]	96	108	103.5	0.494	103.6	0.152	0.039
[63]	100	106	103.3	0.505	103.7	0.133	0.039
[64]	84	106	100	0.481	101.9	0.180	0.063
[65]	100	108	104.5	0.498	103.6	0.141	0.047
Proposed	104	108	106.8	0.507	103.9	0.140	0.054

Where, ΔZ and ΔY are consistent contribution then yield differences. An S-box with smaller differences is stronger towards discourage differential cryptanalysis. Table7 shows that the planned S-box has significance of difference probability as 0.054. This slight value specifies that the planned S-Box delivers good opposition to difference cryptanalytic exertions.

G. Performance Comparison

By cryptographic structures, a presentation difference of planned Substitution box and other S-boxes is assumed, our results are given below: Our S-box has normal significance of NL larger than the additional S-boxes in Table. For example, a outcome, planned S-box delivers virtuous scuffle against linear cryptanalysis. Authorizes the PURSE value (0.507) of planned S-box is actual close to perfect significance of SAC (0.5). We can say that our S-box is satisfying SAC now a reputable method [25].

Conclusions

In this study, we introduce a novel approach to designing inexpensive S-Boxes by utilizing a new nonlinear mapping technique, specifically a cubic polynomial mapping. We propose this method to enhance the security of cryptographic algorithms while keeping costs low. The effectiveness of our proposed S-Box is evaluated through comprehensive cryptanalysis, comparing it with established standards in the field. Our analysis demonstrates that our S-Box performs competitively with existing ones, meeting key criteria such as BIC, nonlinearity, and SAC. We believe that our approach holds promise for future block ciphers, offering potential improvements in security and efficiency. It is worth noting that our method represents a pioneering exploration of cubic polynomial mapping for S-Box design, indicating a new direction in cryptographic research. We anticipate that this innovative technique will lead to the development of even stronger S-Boxes, contributing to secure data transmission in real-world applications.

References

[1] A. Ab. M. Ragab, A. Madani, A. M. Wahdan, and G. M. I. Selim, "Design, analysis, and implementation of a new lightweight block cipher for protecting IoT smart devices," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 5, pp. 6077–6094, May 2023, doi: 10.1007/s12652-020-02782-6.

[2] S. Arshad, "Construction of confusion component based on the isogeny of elliptic curves," *Multimed. Tools Appl.*, vol. 83, no. 16, pp. 47735–47749, Oct. 2023, doi: 10.1007/s11042-023-17399-y.

[3] H. Kimura, K. Emura, T. Isobe, R. Ito, K. Ogawa, and T. Ohigashi, "A Deeper Look into Deep Learning-based Output Prediction Attacks Using Weak SPN Block Ciphers," *J. Inf. Process.*, vol. 31, pp. 550–561, 2023.

[4] F. Sun and Z. Lv, "A secure image encryption based on spatial surface chaotic system and AES algorithm," *Multimed. Tools Appl.*, vol. 81, no. 3, pp. 3959–3979, Jan. 2022, doi: 10.1007/s11042-021-11690-6.

[5] J. N. Mamvong, G. L. Goteng, B. Zhou, and Y. Gao, "Efficient security algorithm for power-constrained IoT devices," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5498–5509, 2020.

[6] S. Taware, R. R. Chakravarthi, C. A. Palagan, K. Chandrasekaran, and N. Vadivelan, "RETRACTED ARTICLE: Preserving mobile commerce IoT data using light weight SIMON block cipher cryptographic paradigm," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 6, pp. 6081–6089, Jun. 2021, doi: 10.1007/s12652-020-02173-x.

[7] P. A. Eliasi, S. Mella, L. Weissbart, L. Batina, and S. Picek, "Xoodyak Under SCA Siege," in *2024 27th International Symposium on Design & Diagnostics of Electronic Circuits & Systems (DDECS)*, IEEE, 2024, pp. 61–66. Available: https://ieeexplore.ieee.org/abstract/document/10508930/

[8] A. T. Momani, "Cryptography Approaches in Wireless Sensor Networks a Survey Study," Master's Thesis, Texas A&M University-Kingsville, 2023. Available: https://search.proquest.com/openview/f4bb57a13e247e73240d188eefa1793d/1?pq-origsite=gscholar&cbl=18750&diss=y

[9] P. Gao, Y. Zhang, F. Song, T. Chen, and F.-X. Standaert, "Compositional Verification of Efficient Masking Countermeasures against Side-Channel Attacks," *Proc. ACM Program. Lang.*, vol. 7, no. OOPSLA2, pp. 1817–1847, Oct. 2023, doi: 10.1145/3622862.

[10] R. S. Ali *et al.*, "Enhancement of the cast block algorithm based on novel S-box for image encryption," *Sensors*, vol. 22, no. 21, p. 8527, 2022.

[11] A. Razaq, A. Ullah, H. Alolaiyan, and A. Yousaf, "A Novel Group Theoretic and Graphical Approach for Designing Cryptographically Strong Nonlinear Components of Block Ciphers," *Wirel. Pers. Commun.*, vol. 116, no. 4, pp. 3165–3190, Feb. 2021, doi: 10.1007/s11277-020-07841-x.

[12] S. Eddahmani and S. Mesnager, "A Suitable Proposal of S-Boxes (Inverse-Like) for the AES, Their Analysis and Performances," in *Security and Privacy*, vol. 1497, P. Stănică, S. Mesnager, and S. K. Debnath, Eds., in Communications in Computer and Information Science, vol. 1497. , Cham: Springer International Publishing, 2021, pp. 49–63. doi: 10.1007/978-3-030-90553-8_4.

[13] O. Kuznetsov, N. Poluyanenko, E. Frontoni, and S. Kandiy, "Enhancing Smart Communication Security: A Novel Cost Function for Efficient S-Box Generation in Symmetric Key Cryptography," *Cryptography*, vol. 8, no. 2, p. 17, 2024.

[14] P.-P. Duong *et al.*, "Construction of Robust Lightweight S-Boxes Using Enhanced Logistic and Enhanced Sine Maps," *IEEE Access*, 2024. Available: https://ieeexplore.ieee.org/abstract/document/10518043/

[15] R. S. Jenny, R. Sudhakar, and M. Karthikpriya, "Design of compact s box for resource constrained applications," in *Journal of Physics: Conference Series*, IOP Publishing, 2021, p. 012059. Available: https://iopscience.iop.org/article/10.1088/1742-6596/1767/1/012059/meta

[16] M. Ahmad and E. Al-Solami, "Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme," *Entropy*, vol. 22, no. 7, p. 717, 2020.

[17] T. Shah, D. A. Khan, and A. Ali, "Design of nonlinear component of block cipher using quaternion integers," *Multimed. Tools Appl.*,

vol. 83, no. 9, pp. 25657–25674, Aug. 2023, doi: 10.1007/s11042-023-16518-z.

[18] M. Rana, Q. Mamun, and R. Islam, "An S-box Design Using Irreducible Polynomial with Affine Transformation for Lightweight Cipher," in *Quality, Reliability, Security and Robustness in Heterogeneous Systems*, vol. 402, X. Yuan, W. Bao, X. Yi, and N. H. Tran, Eds., in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 402. , Cham: Springer International Publishing, 2021, pp. 214–227. doi: 10.1007/978-3-030-91424-0_13.

[19] F. Tita, A. Setiawan, and B. Susanto, "construction of substitution box (s-box) based on irreducible polynomials on gf (2^ 8)," *barekeng j. Ilmu Mat. Dan Terap.*, vol. 18, no. 1, pp. 0517–0528, 2024.

[20] Y. Aydın and F. Özkaynak, "Automated Chaos-Driven S-Box Generation and Analysis Tool for Enhanced Cryptographic Resilience," *IEEE Access*, 2023. Available: https://ieeexplore.ieee.org/abstract/document/10371318/

[21] F. Dridi, S. El Assad, W. El Hadj Youssef, M. Machhout, and R. Lozi, "Design, implementation, and analysis of a block cipher based on a secure chaotic generator," *Appl. Sci.*, vol. 12, no. 19, p. 9952, 2022.

[22] A. Hadj Brahim, A. Ali Pacha, and N. Hadj Said, "An image encryption scheme based on a modified AES algorithm by using a variable S-box," *J. Opt.*, vol. 53, no. 2, pp. 1170–1185, Apr. 2024, doi: 10.1007/s12596-023-01232-8.

[23] M. Zhao, Z. Yuan, L. Li, and X.-B. Chen, "A novel efficient S-box design algorithm based on a new chaotic map and permutation," *Multimed. Tools Appl.*, Jan. 2024, doi: 10.1007/s11042-023-17720-9.

[24] S. Marochok and P. Zajac, "Algorithm for generating s-boxes with prescribed differential properties," *Algorithms*, vol. 16, no. 3, p. 157, 2023.

[25] A. Singh, A. Prasad, and Y. Talwar, "Compact and Secure S-Box Implementations of AES—A Review," in *Smart Systems and IoT: Innovations in Computing*, vol. 141, A. K. Somani, R. S. Shekhawat, A. Mundra, S. Srivastava, and V. K. Verma, Eds., in Smart

Innovation, Systems and Technologies, vol. 141. , Singapore: Springer Singapore, 2020, pp. 857–871. doi: 10.1007/978-981-13-8406-6_80.