symmetry

Article

An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping

Amjad Hussain Zahid * and Muhammad Junaid Arshad

Department of Computer Science, University of Engineering and Technology, Lahore 54000, Pakistan; junaidarshad@uet.edu.pk
* Correspondence: amjad.zahid@umt.edu.pk; Tel.: +92-300-428-4001

Received: 8 February 2019; Accepted: 22 March 2019; Published: 25 March 2019

Abstract: In this paper, we propose to present a novel technique for designing cryptographically strong substitution-boxes using cubic polynomial mapping. The proposed cubic polynomial mapping is proficient to map the input sequence to a strong 8×8 S-box meeting the requirements of a bijective function. The use of cubic polynomial maintains the simplicity of S-box construction method and found consistent when compared with other existing S-box techniques used to construct S-boxes. An example proposed S-box is obtained which is analytically evaluated using standard performance criteria including nonlinearity, bijection, bit independence, strict avalanche effect, linear approximation probability, and differential uniformity. The performance results are equated with some recently scrutinized S-boxes to ascertain its cryptographic forte. The critical analyses endorse that the proposed S-box construction technique is considerably innovative and effective to generate cryptographic strong substitution-boxes.

Keywords: substitution box; cubic polynomial mapping; block ciphers; security

1. Introduction

Recent technological innovations and their fruitful usage in real life have resulted in an immense growth in the volume of data being communicated. The sensitive nature of data demands for techniques to be developed and measures to protect from misuse. Before transmission, a user's data must be transformed in such a form that is meaningless to an attacker. Symmetric block ciphers are among the most widely used techniques to fulfill this purpose due to the easy implementation and being the providers of much needed cryptographic strength [1,2]. One popular type of block cipher uses substitution and permutation operations. This type of block cipher transforms an input block of data (plaintext) into a meaningless output block (ciphertext) by using a symmetric key and different number of rounds. Generally, each round performs substitution and permutation processes on the input block of data. A substitution process replaces an input block with another output block using substitution box (S-box) [3]. Advanced Encryption Standard (AES), as an example, is most commonly used symmetric block cipher.

An S-box is a decisive component of recent block ciphers and generates a scrambled ciphertext from the given plaintext. An S-box, being the only nonlinear constituent of modern block ciphers, offers a complex relationship between the plaintext and the ciphertext. This relation is called confusion [4]. Whatever security a block cipher provides is reliant on the confusion in the ciphertext created by an S-box. As a result, many researchers are designing novel S-boxes and evaluating the strength of their respective S-boxes against some typical benchmarks such as bijective-ness, strict avalanche criterion (SAC), nonlinearity, bit independence criterion (BIC), linear and differential probabilities, etc. In [5–7], a number of properties have been suggested to be existent in an S-box to be able to resist various cryptanalytic attacks. An S-box possessing most of these properties provides more security.

2. Related Work

In literature, a number of techniques and tools are adopted for synthesis of cryptographically potent Substitution-boxes. L. R. Dragomir et al. [8] projected a technique to build repositories of vigorous and resistant S-boxes which can assist while customizing the block cryptosystems. An S-box having high nonlinearity provides more resistance against linear cryptanalysis [9]. AES employs highly nonlinear S-box in its various rounds for the encryption and decryption processes. Authors in [10–13] proposed different enrichments to the security presented by AES by optimizing the AES S-box in different aspects. A block cipher having a static S-box employs the unchanged S-box in each round. A static S-box allows the invaders to inspect S-box features, discover its flaws, and eventually get a chance of cryptanalysis of the muddled ciphertext produced by the block cipher [5,14,15]. Due to the limitations of static S-boxes, a large number of researchers have explored the ideas for S-box design such as randomness, dynamicity, and key-dependency. Mostly, a key-dependent and dynamic S-box improves the strength of the respective block cipher. For instance, Marcin Niemiec et al. [16] and K. Kazlauskas et al. [17] used key-dependent S-boxes and proposed methods to produce enormous quantity of strong S-Boxes. Authors [18–21] proposed key-dependent dynamic S-boxes and analyses show that proposed S-boxes are cryptographically very strong. C. Easttom [22] indicated various inefficiencies like added processing time, etc. and present in key-dependent S-boxes. Authors [23] proposed enhancements in AES by introducing key-dependent S-box.

The avalanche effect is one of the many needed landscapes of today's block ciphers [24]. This feature of block ciphers necessitates that single bit modification in the plaintext or key should create significant variations in the resulting ciphertext. Small value of avalanche effect indicates a weaker block cipher, and hence the ciphertext produced by such cipher may be a victim of a cryptanalytic effort. Various simple methods proposed in [25] can be used efficiently to calculate SAC and investigate a given S-Box for completeness and cryptographic strength. Authors [24,26] analyzed AES and other S-boxes, evaluated their avalanche effect, and concluded that AES S-boxes have the maximum avalanche effect. Dynamic S-boxes proposed by [27,28] demonstrate respectable avalanche effect as compared to the standard AES S-boxes. Further analysis of the proposed and AES S-boxes reveals that AES and new ciphers are independent of each other and AES has more efficiency.

Chaos is a prevalent spectacle with features of sensitivity, randomness, spread spectrum, periodicity, etc. These chaos topographies make chaotic systems as a choice for the development of modern ciphers and many researchers have used chaos in the design of S-boxes. Authors [29–39] suggested S-boxes based on chaotic map and analyzed these along with the other existing S-box design methods. Analyses disclosed that the proposed S-boxes are strong against different attacks and hence suggest their usage in modern block ciphers. Advanced form of chaos called hyperchaotic is solider than the chaos against cryptanalysis efforts due to its dynamic complexities. Using its strength, authors [40–43] designed a number of S-boxes based on hyperchaotic concepts while each S-box is very effective bearing the features like SAC, BIC, etc. [44] is another recently designed S-box using chaos and line equilibrium suitable for medical devices, etc.

Many other researchers have designed S-Boxes using several techniques and concepts like graph isomorphism [45], coset diagrams [46], linear fractional transformation [47–50], etc. Ciphers based on S-box are highly dependent on the security features of the used S-box. A tool is needed to critically analyze an S-box and check its security against some standard criteria. The authors of [51] have developed a program to evaluate the cryptographic performance of any S-box.

In this paper, an efficient technique to construct S-boxes has been suggested. The proposed technique is a pioneering one and diverse from the methods offered in the literature as we have recommended a cubic polynomial mapping and explored it for the design of robust S-Boxes. After the construction of an S-Box, its recital analysis has been carried out to evaluate its cryptographic strength. A comparison with other lately designed S-Boxes inspires about its strength. The analytical results stimulate the usage of the proposed S-Box in modern block ciphers.

The organization of the rest of the paper is as follows. Section 2 offers the design of the proposed S-Box. Performance analysis of the proposed S-Box against cryptographic landscapes is conferred in Section 3 and a comparison is made with some recently designed S-boxes. Section 4 completes the research paper with conclusions.

3. Proposed Substitution-Box Design

Most of the symmetric block ciphers use one or more S-boxes for substitution purpose to bring in the sufficient confusion. An S-box provides the confusion facility between the plaintext and the ciphertext through a nonlinear mapping. The researchers have comprehensively explored such nonlinear mappings to construct S-boxes having different cryptographic strength. However, the process of S-Box construction using these techniques is very complex and inefficient.

We present a very simple and efficient nonlinear mapping to construct strong S-boxes. We call this nonlinear mapping as Cubic Polynomial Mapping (CPM). The proposed cubic polynomial mapping is a function having the following general form:

$$\mathrm{C(t)} = \left[\mathrm{A} * \mathrm{t}^3 + \mathrm{B}\right] (\mathrm{mod}(2^{\mathrm{n}} + 1)) \quad \mathrm{t} \in \mathrm{N}. \tag{1}$$

where, N = {0, 1, ... , 2^n −1}, mod operation gives the remainder, and both A and B $\in$ N – {0} to construct an S-box of size n $\times$ n. A cubic polynomial mapping demonstrates a nonlinear behavior and is an inspiration for byte substitution. To ornate the erection of the proposed S-Box by Equation (1), let us have an explicit type of cubic polynomial function as specified in Equation (2). For n = 8, we have N = {0, 1, ... , 2^n −1} = {0, 1, ... , 2^8 −1} = {0, 1, ... , 255}. One can choose any values for A and B (A, B $\in$ N – {0}) to be used in Equation (1). For the sake of an example here, we have chosen A = 69, and B = 100. CPM function C(t) specified in Equation (2) spawns values N – {31} when t $\in$ N – {135}. When t = 135, C(t) calculates to 256 $\notin$ N. To preserve the function C(t) as bijective one, we explicitly describe the value of C(t) for t=135 as habituated in Equation (2). A CPM function C: N $\to$ N to generate 8 $\times$ 8 S-box is given as:

$$\mathrm{C(t)} = \left\{ \begin{array}{cc} \left[69 * \mathrm{t}^3 + 100\right] (\mathrm{mod}\ 257) & \mathrm{t} \in \mathrm{N} - \{135\} \\ 31 & \mathrm{t} = 135 \end{array} \right\}. \tag{2}$$

This particular cubic polynomial of Equation (2) produces values of our proposed 8 $\times$ 8 S-box which are arranged in 16 $\times$ 16 matrix as presented in Table 1.

Table 1. Proposed S-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

4. Performance Results

In this section, we investigate our novel technique and proposed S-box given in Table 1 for broadly established standard S-box performance benchmarks to measure its cryptographic strength.

4.1. Bijectiveness

For two sets X and Y, a function f: X $\rightarrow$ Y is bijective if and only if it is one-to-one and onto simultaneously. One-to-one mapping requires that each element of set X is matching with just one element of set Y. Onto mapping requires that each element of set Y has distinct pre-image in set X. CPM function C: N $\rightarrow$ N is bijective as it produces distinct output values for distinct input values having image(C) = N and pre-image(C) = N, where N = {0, 1, . . . , 254, 255}.

4.2. Strict Avalanche Criterion (SAC)

The SAC criterion [52,53] is an imperative feature for any cryptographic S-box which states that if a single bit is changed in the input, this change should modify half of the output bits. An S-box having a value of SAC closer to 0.5 has decent uncertainty. Dependency matrix providing the SAC values of proposed S-box is given in Table 2. It is evident from Table 2 that the average SAC value of the S-Box is equal to 0.5. This SAC value is an indication that the proposed S-box gratifies SAC property in a respectable manner.

Table 2. Dependency matrix for strict avalanche criterion (SAC) values.

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

4.3. Nonlinearity

If an S-box is designed in such a way that it has linear mapping between the plaintext and the ciphertext, it becomes easy to launch a linear cryptanalysis attack on the ciphertext to get the original plaintext. To resist this attack, an S-box must be designed with high nonlinear mapping between its input and output. Equation (3) is used to calculate the nonlinearity of an n-bit Boolean function b(k) as:

$$\mathrm{NL}(b) = \frac{1}{2}\left[2^n - \left(\max_{h\in\{0,1\}^n} |\mathrm{WS}_b(h)|\right)\right], \tag{3}$$

where, $\mathrm{WS}_b(h)$ = Walsh spectrum of function b, and it is calculated as:

$$\mathrm{WS}_b(h) = \sum_{k\in\{0,1\}^n} (-1)^{b(k)\oplus k.h},$$

where, $h \in \{0, 1\}^n$ and k.h denotes the dot product of k and h, calculated as:

$$k.h = (k_1 \oplus h_1) + \ldots + (k_n \oplus h_n)$$

The nonlinearity values of our S-box are 106, 104, 106, 108, 108, 106, 108, and 108 with minimum of 104, maximum of 108, and average of 106.8. The nonlinearities of all eight constituent Boolean functions are also provided in Table 3.

Table 3. Nonlinearities of constituent Boolean functions of proposed S-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 a comparison of proposed S-box and other recent S-boxes with respect to nonlinearity metric. It can be seen that proposed S-box has the right competence to insipid the linearity and thus the linear cryptanalysis is an uphill task for the attacker.

Table 4. Different S-boxes and the respective nonlinearity values.

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

4.4. Bit Independence Criterion (BIC)

According to this criterion [52,53], the inversion of an input bit p modifies output bits q and r without any dependence on each other. An S-box that makes the output bits independent of each other strengthens the security. If an S-box fulfills BIC property, all the constituent Boolean functions of that S-Box own high nonlinearity and also meet SAC very well. Tables 5 and 6 exhibit the nonlinearity and SAC values for constituent Boolean functions of the proposed S-Box.

Table 5. Bit independence criterion (BIC) results for nonlinearity.

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	-

It is evident from Tables 5 and 6 that average nonlinearity and SAC values for BIC are 103.9 and 0.5, respectively. According to [53], if an S-box exhibit nonlinearity and SAC, it fulfills BIC. The obtained scores of 103.9 and 0.5 for proposed S-box clearly indicate an extremely weak linear association among the output bits and thus fully validate BIC of our S-box.

4.5. Linear Probability

The cryptologist of modern block ciphers tries to create ample confusion and diffusion of bits to secure the data against cryptanalytic efforts. Strong S-boxes help in achieving these requirements through nonlinear mapping between input and output. An S-box having low linear probability (LP) indicates higher nonlinear mapping and provides resistance against the linear cryptanalysis. Mathematically, Equation (4) is used to calculate the linear probability of an S-box:

$$LP = \max_{\alpha_z,\beta_z \neq 0} \left| \frac{\#\{z \in N | z \cdot \alpha_z = S(z) \cdot \beta_z\}}{2^n} - \frac{1}{2} \right|. \tag{4}$$

where, α_z and β_z are the corresponding input and output masks and N = {0,1, . . . , 255}. Maximum value of LP of our S-box is only 0.140, and thus provides good resistance against linear cryptanalysis.

4.6. Differential Probability

Differential cryptanalysis is considered as a useful tool to grasp the original plaintext. During this effort, variances in the plaintext and the ciphertext are found. The coupling of these variances assists the attackers to attain some part of the key. A low value of differential probability helps in resisting this attack. Differential probability (DP) is calculated as:

$$DP = \max_{\Delta z \neq 0,\, \Delta y} \left[\frac{\#\{z \in N | S(z) \oplus S(z \oplus \Delta z) = \Delta y\}}{2^n} \right]. \tag{5}$$

where, Δz and Δy are corresponding input and output differentials. An S-box with smaller differentials is sturdier to deter differential cryptanalysis. Table 7 shows that the proposed S-box has value of differential probability as 0.054. This small value indicates that the proposed S-Box provides respectable resistance to differential cryptanalytic efforts.

Table 7. Performance comparison of different 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

4.7. Performance Comparison

Using cryptographic features, a performance comparison of proposed S-box and other S-boxes is given in Table 7. Our verdicts are given below:

- Our S-box has average value of nonlinearity greater than the other S-boxes in Table 7. As a result, proposed S-box provides good resistance against linear cryptanalysis.
- Table 7 validates that SAC value (0.507) of proposed S-box is very near to ideal value of SAC (0.5). We can say that our S-box is gratifying SAC in a respectable manner.
- It can be observed from Tables 5–7 that the BIC value of the proposed S-box is quite good ensuing gratification of the BIC test.
- Differential probability value of proposed S-box is just 0.054. This small value of DP reveals the cryptographic strength of our S-box.
- Proposed S-Box has LP value equal to 0.140. This small value guarantees that our S-box has the potential to confront the linear cryptanalysis.

5. Conclusions

In this paper, using a new nonlinear mapping (cubic polynomial mapping), we have suggested an innovative and simple method to design efficient S-Boxes. Then the proposed S-Box is tested for cryptographic strength using different standard benchmarks. The analysis results are in harmony with the related S-boxes to justify our method. Recital of our S-Box sounds good when we compare it with topical S-boxes. The promising scores of BIC, nonlinearity, SAC, and other criteria of our S-Box reflect its potential candidature for future block ciphers. It is worth declaring that our proposed method is the pioneer one to explore the cubic polynomial mapping for S-Box design. One can expect the emergence of stronger S-boxes for secure transmission of data using cubic polynomial mapping in real life.

Author Contributions: All the authors collaborated in this research work in all aspects.

Funding: This research received no external funding.

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

References

1. Paar, C.; Pelzl, J.; Preneel, B. *Understanding Cryptography*, 1st ed.; Springer: Berlin, Germany, 2010.
2. Shamir, A. Stream Ciphers: Dead or Alive? In Proceedings of the 10th International Conference on Theory and Application of Cryptology and Information Security, Jeju Island, Korea, 5–9 December 2004.
3. Lambić, D.; Živković, M. Comparison of Random S-Box Generation Methods. *De L'institut Mathématique* **2013**, *93*, 109–115.
4. Lauridsen, M.M.; Rechberger, C.; Knudsen, L.R. *Design and Analysis of Symmetric Primitive*; Kgs. Lyngby, Technical University of Denmark: Kongens Lyngby, Denmark, 2016.
5. Mohamed, K.; Nazran, M.; Pauzi, M.; Hani, F.; Ali, H.M.; Ariffin, S.; Huda, N.; Zulkipli, N. Study of S-box Properties in Block Cipher. In Proceedings of the International Conference on Computer Communication and Control Technology, Langkawi Island, Kedah, Malaysia, 2–4 September 2014.
6. Manjula, G.; Mohan, H.S. Constructing Key Dependent Dynamic S-Box for AES Block Cipher System. In Proceedings of the International Conference on Applied and Theoretical Computing and Communication Technology, Bengaluru, Karnataka, India, 21–23 July 2016.
7. Radhakrishnan, S.V.; Subramanian, S. An Analytical Approach to S-box Generation. In Proceedings of the International Conference on Communication and Signal Processing, Chennai, India, 4–5 April 2012.
8. Dragomir, I.R.; Lazăr, M. Generating and Testing the Components of a Block Cipher. In Proceedings of the 18th International Conference on Electronics, Computers and Artificial Intelligence, Ploiesti, Romania, 30 June–2 July 2016.
9. Du, Z.; Xu, Q.; Zhang, J.; Li, M. Design and Analysis of Dynamic S-Box based on Feistel. In Proceedings of the International Conference on Advanced Information Technology, Electronic and Automation Control, Chongqing, China, 19–20 December 2015.
10. Juremi, J.; Mahmod, R.; Sulaiman, S. A Proposal for Improving AES S-box with Rotation and Key-Dependent. In Proceedings of the International Conference on Digital Cyber Security, Cyber Warfare and Digital Forensic, Kuala Lumpur, Malaysia, 26–28 June 2012.
11. Sahoo, O.B.; Kole, D.K.; Rahaman, H. An optimized S-box for Advanced Encryption Standard (AES) design. In Proceedings of the International Conference on Advanced Computer Communication, Chennai, India, 3–5 August 2012.
12. Wang, H.; Zheng, H.; Hu, B.; Tang, H. Improved lightweight encryption algorithm based on optimized S-box. In Proceedings of the International Conference on Computational and Information Sciences, Hubei, China, 21–23 June 2013.
13. Cui, J.; Huang, L.; Zhong, H.; Chang, C.; Yang, W. An Improved AES S-Box and its Performance Analysis. *Int. J. Innov. Comput. Inf. Control* **2011**, *7*, 2291–2302.
14. Katiyar, S.; Jeyanthi, N. Pure Dynamic S-box Construction. *Int. J. Comput.* **2016**, *1*, 42–46.
15. Alabaichi, A.; Salih, A.I. Enhance Security of Advance Encryption Standard Algorithm Based on Key-dependent S-Box. In Proceedings of the International Conference on Digital Information Processing and Communications, Sierre, Switzerland, 7–9 October 2015.
16. Niemiec, M.; Machowski, Ł. A new symmetric block cipher based on key-dependent S-boxes. In Proceedings of the International Conference on ultra-Modern Telecommunications and Control Systems, St. Petersburg, Russia, 3–5 October 2012.
17. Kazlauskas, K.; Smaliukas, R.; Vaicekauskas, G. A Novel Method to Design S-Boxes Based on Key- Dependent Permutation Schemes and its Quality Analysis. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 93–99. [CrossRef]
18. Kazlauskas, K.; Vaicekauskas, G.; Smaliukas, R. An Algorithm for Key-Dependent S-Box Generation in Block Cipher System. *Informatica* **2015**, *26*, 51–65. [CrossRef]
19. Mathura, N.; Bansodeb, R. AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection. *Procedia Comput. Sci.* **2016**, *79*, 1036–1043. [CrossRef]
20. Zobeiri, M.; Maybodi, B.M. Introducing a New Method in Cryptography by using Dynamic P-Box and S-Box based on Modular Calculation and Key Encryption. *Arpn J. Eng. Appl. Sci.* **2017**, *12*, 2946–2953.
21. Rahaman, Z.; Corraya, A.D.; Sumi, M.A.; Bahar, A.N. A Novel Structure of Advance Encryption Standard with 3-Dimensional Dynamic S-box and Key Generation Matrix. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 314–320. [CrossRef]

22. Easttom, C. An Examination of Inefficiencies in Key Dependent Variations of the Rijndael S-Box. In Proceedings of the Iranian Conference on Electrical Engineering, Mashhad, Iran, 8–10 May 2018.
23. Shekhar, S.; Singh, P.; Jaiswal, M. An Enhanced AES Algorithm Based on Variable S-box and 200 Bit Data Block. *Int. J. Innov. Res. Comput. Commun. Eng.* **2016**, *4*, 6470–6477.
24. Agrawal, H.; Sharma, M. Implementation and analysis of various symmetric cryptosystems. *Indian J. Sci. Technol.* **2010**, *3*, 1173–1176.
25. Mar, P.P.; Latt, K.M. New Analysis Methods on Strict Avalanche Criterion of S-Boxes. *Int. J. Math. Comput. Sci.* **2008**, *2*, 899–903.
26. Shi, H.; Deng, Y.; Guan, Y. Analysis of the Avalanche Effect of the AES S Box. In Proceedings of the International Conference on Artificial Intelligence, Management Science and Electronic Commerce, Deng Feng, China, 8–10 August 2011.
27. Nejad, F.H.; Sabah, S.; Jam, A.J. Analysis of Avalanche Effect on Advance Encryption Standard by using Dynamic S-Box Depends on Rounds Keys. In Proceedings of the International Conference on Computational Science and Technology, Sabah, Malaysia, 27–28 August 2014.
28. Mahmoud, E.M.; Hafez, A.A.; Elgarf, T.A.; Zekry, A.H. Dynamic AES-128 with Key-Dependent S-box. *Int. J. Eng. Res. Appl.* **2013**, *3*, 1662–1670.
29. Ahmad, M.; Mittal, N.; Garg, P.; Khan, M.M. Efficient Cryptographic Substitution Box Design Using Travelling Salesman Problem and Chaos. *Perspect. Sci.* **2016**, *8*, 465–468. [CrossRef]
30. Ahmad, M.; Haleem, H.; Khan, P.M. A New Chaotic Substitution Box Design for Block Ciphers. In Proceedings of the International Conference on Signal Processing and Integrated Networks, Delhi, India, 20–21 February 2014.
31. Ahmed, H.A.; Zolkipli, M.F.; Ahmad, M. A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. *Neural Comput. Appl.* **2018**. [CrossRef]
32. Ahmad, M.; Doja, M.N.; Beg, M.M.S. ABC Optimization Based Construction of Strong Substitution-Boxes. *Wirel. Pers. Commun.* **2018**, *101*, 1715–1729. [CrossRef]
33. Alzaidi, A.A.; Ahmad, M.; Doja, M.N.; Solami, E.A.; Beg, M.M.S. A New 1D Chaotic Map and beta-Hill Climbing for Generating Substitution-Boxes. *IEEE Access* **2018**, *6*, 55405–55418. [CrossRef]
34. Alzaidi, A.A.; Ahmad, M.; Ahmed, H.S.; Solami, E.A. Sine-Cosine Optimization-Based Bijective Substitution-Boxes Construction Using Enhanced Dynamics of Chaotic Map. *Complexity* **2018**, *2018*, 9389065. [CrossRef]
35. Lai, Q.; Akgul, A.; Li, C.; Xu, G.; Çavusoglu, U. A New Chaotic System with Multiple Attractors: Dynamic Analysis, Circuit Realization and S-Box Design. *Entropy* **2018**, *20*, 12. [CrossRef]
36. Ahmad, M.; Ahmad, F.; Nasim, Z.; Bano, Z.; Zafar, S. Designing Chaos Based Strong Substitution Box. In Proceedings of the International Conference on Contemporary Computing, Noida, India, 20–22 August 2015.
37. Zahid, A.; Arshad, M.; Ahmad, M. A Novel Construction of Efficient Substitution-Boxes Using Cubic Fractional Transformation. *Entropy* **2019**, *21*, 245. [CrossRef]
38. Belazi, A.; Khan, M.; Latif, A.A.A.; Belghith, S. Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. *Nonlinear Dyn.* **2017**, *87*, 337–361. [CrossRef]
39. Lambić, D. S-box design method based on improved one dimensional discrete chaotic map. *J. Inf. Telecommun.* **2018**, *2*, 181–191. [CrossRef]
40. Peng, J.; Jin, S.; Lei, L.; Jia, R. A Novel Method for Designing Dynamical Key-Dependent S-Boxes based on Hyperchaotic System. *Int. J. Adv. Comput. Technol.* **2016**, *4*, 282–289.
41. Solami, E.A.; Ahmad, M.; Volos, C.; Doja, M.; Beg, M. A New Hyperchaotic System-Based Design for Efficient Bijective Substitution-Boxes. *Entropy* **2018**, *20*, 525. [CrossRef]
42. Ababneh, M. A new four-dimensional chaotic attractor. *Ain Shams Eng. J.* **2018**, *9*, 1849–1854. [CrossRef]
43. Liu, L.; Zhang, Y.; Wang, X. A Novel Method for Constructing the S-Box Based on Spatiotemporal Chaotic Dynamics. *Appl. Sci.* **2018**, *8*, 2650. [CrossRef]
44. Wang, X.; Akgul, A.; Cavusoglu, U.; Pham, V.; Hoang, D.V.; Nguyen, X.Q. A Chaotic System with Infinite Equilibria and Its S-Box Constructing Application. *Appl. Sci.* **2018**, *8*, 2132. [CrossRef]
45. Tran, B.N.; Nguyen, T.D.; Tran, T.D. A New S-Box Structure Based on Graph Isomorphism. In Proceedings of the International Conference on Computational Intelligence and Security, Beijing, China, 11–14 December 2009.

46. Razaq, A.; Yousaf, A.; Shuaib, U.; Siddiqui, N.; Ullah, A.; Waheed, A. A Novel Construction of Substitution Box involving Coset Diagram and a Bijective Map. *Secur. Comm. Netw.* **2017**, *2017*, 5101934. [CrossRef]
47. Farwa, S.; Shah, T.; Idrees, L. A Highly Nonlinear S-Box based on a Fractional Linear Transformation. *SpringerPlus* **2016**, *5*, 1–12. [CrossRef]
48. Hussain, I.; Shah, T.; Gondal, M.A.; Khan, M.; Khan, W.A. Construction of New S-box using a Linear Fractional Transformation. *World Appl. Sci. J.* **2011**, *14*, 1779–1785.
49. Altaleb, A.; Saeed, M.S.; Hussain, I.; Aslam, M. An Algorithm for the Construction of Substitution Box for Block Ciphers based on Projective General Linear Group. *AIP Adv.* **2017**, *7*, 035116. [CrossRef]
50. Sarfraz, M.; Hussain, I.; Ali, F. Construction of S-Box Based on Mobius Transformation and Increasing its Confusion Creating Ability through Invertible Function. *Int. J. Comput. Sci. Inf. Secur.* **2016**, *14*, 187–199.
51. Wang, Y.; Xie, Q.; Wu, Y.; Du, B. A Software for S-box Performance Analysis and Test. In Proceedings of the International Conference on Electronic Commerce and Business Intelligence, Beijing, China, 6–7 June 2009.
52. Webster, A.F.; Tavares, S.E. On the Design of S-Boxes. In Proceedings of the Conference on Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 18–22 August 1986.
53. Adams, C.; Tavares, S. The Structured Design of Cryptographically Good S-Boxes. *J. Cryptol.* **1990**, *3*, 27–31. [CrossRef]
54. Alkhaldi, A.H.; Hussain, I.; Gondal, M.A. A novel design for the construction of safe S-boxes based on TDERC sequence. *Alex. Eng. J.* **2015**, *54*, 65–69. [CrossRef]
55. Chen, G. A novel heuristic method for obtaining S-boxes. *Chaos Solitons Fractals* **2008**, *36*, 1028–1036. [CrossRef]
56. Belazi, A.; Rhouma, R.; Belghith, S. A novel approach to construct S-box based on Rossler system. In Proceedings of the International Wireless Communications and Mobile Computing Conference, Dubrovnik, Croatia, 24–28 August 2015.
57. Mahmood, S.; Farwa, S.; Rafiq, M.; Riaz, S.M.J.; Shah, T.; Jamal, S.S. To Study the Effect of the Generating Polynomial on the Quality of Nonlinear Components in Block Ciphers. *Secur. Commun. Netw.* **2018**, *2018*, 582323. [CrossRef]
58. Siddiqui, N.; Afsar, U.; Shah, T.; Qureshi, A. A Novel Construction of S16 AES S-boxes. *Int. J. Comput. Sci. Inf. Secur.* **2016**, *14*, 811–818.
59. Hussain, I.; Shah, T.; Gondal, M.A.; Wang, Y. Analyses of SKIPJACK S-Box. *World Appl. Sci. J.* **2011**, *13*, 2385–2388.
60. Hussain, I.; Shah, T.; Gondal, M.A.; Khan, W.A.; Mahmood, H. A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Comput. Appl.* **2013**, *23*, 97–104. [CrossRef]
61. Hussain, I.; Shah, T.; Gondal, M.A.; Mahmood, H. Some analysis of S-box based on residue of prime number. *Proc. Pak. Acad. Sci.* **2011**, *48*, 111–115.
62. Asim, M.; Jeoti, V. Efficient and Simple Method for Designing Chaotic S-Boxes. *ETRI J.* **2008**, *30*, 170–172. [CrossRef]
63. Özkaynak, F.; Özer, A.B. A method for designing strong S-boxes based on chaotic Lorenz system. *Phys. Lett. A* **2102**, *374*, 3733–3738. [CrossRef]
64. Khan, M.; Shah, T.; Batool, S.I. Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Comput. Appl.* **2016**, *27*, 677–685. [CrossRef]
65. Khan, M.; Shah, T. An efficient construction of substitution box with fractional chaotic system. *SIViP* **2015**, *9*, 1335–1338. [CrossRef]