WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Innovative Construction of Substitution-Boxes Using Permutations Over Hecke Group

Zill e Huma Idrees [a]***, Nasir Siddiqui*** [b]

[a] *Department of Basic Sciences, University of Engineering and Technology Taxila, Pakistan*

[b] *Department of Basic Sciences, University of Engineering and Technology Taxila, Pakistan*

DOI: 10.55248/gengpi.4.623.45989

A B S T R A C T

One fundamental non-linear element of a block cipher is the substitution box (S-box). In the face of differential and linear threats, S-Box maintains data security. In this paper, we proposed a new technique for the construction of S-boxes using permutations of S_{16} over the Hecke Group $H(\lambda_6)$. Various standard tests are utilized to evaluate the strength of proposed S-boxes, for instance, Non-Linearity (NL), Differential Probability (DP), Strict Avalanche Criteria (SAC), Bit Independence Criteria (BIC), and Linear Probability (LP). Then we used our resultant S-boxes for image encryption.

Keywords: Projective Line, Hecke Group, Symmetric Group, S- Box, Image Encryption.

1. INTRODUCTION

In the current era of rapidly advancing technology, the secure and dependable transfer of information to end users has become an essential requirement. Cryptography is a crucial tool in ensuring data security by providing secure encryption and decryption through various algorithms [1]. These cryptographic methods protect against malicious attacks by using mathematical structures and non-linear characteristics. Block ciphers are a regularly employed technique in cryptography. Two of the most extensively used block ciphers are Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [2]. The key length of DES is only 56 bits, which is comparatively short by modern standards and renders it susceptible to brute-force attacks. Whereas, AES uses a variable key length of 128, 192 or 256 bits, making it more secure. The S-box in AES is a critical component that provides confusion in plaintext by applying non-linear substitutions to each byte of the input [3]. The strength of the S-box is a crucial factor in determining the overall security of the block cipher. Numerous approaches have been suggested to enhance the quality of the S-box, such as using genetic algorithms, neural networks, and mathematical constructions based on finite fields [4]. Overall, AES is considered to be a highly secure block cipher that provides strong encryption and is widely used in various applications, including communication systems, financial transactions, and data storage [5]. There are several techniques available for analyzing the statistical and algebraic properties of S-boxes. These methods include the linear approximation probability (LAP) method, bit independence criterion (BIC), majority logic criterion (MLC), strict avalanche criterion (SAC), non-linearity method, and differential approximation probability (DP) method [6,7]. In this paper, we establish a new technique to construct substitution boxes by the action of Hecke group $H(\lambda_6)$ on a projective line over a finite field F_{257}. Then we apply different permutations of S_{16} on the S-box obtained by the action of the Hecke Group.

In Section II, we will present the basis of our method. In Section III, We will outline the process used to build our substitute boxes. In Section IV, we will check the different analyses to assess the power of our S-boxes with the existing boxes. In Section V, we will examine its application in image encryption. Section VI is the conclusion.

2. PRELIMINARIES

This unit covers the fundamental principles of the Projective line over a finite field, Hecke group and symmetric group utilized for the construction of our S-boxes.

2.1 Projective Line Over Finite Field

For a finite field F_q with q number of elements, the projective line over a finite field $PL(F_q) = F_q \cup \{\infty\}$ has $q+1$ elements. Where ∞ is treated as an element as well as infinity [8]. The point at infinity represents the direction of lines parallel to the x-axis, rather than being a typical point. The projective line over a finite field $PL(F_q)$ exhibits a wide range of interesting characteristics in algebraic geometry, number theory, and coding theory. It can be used, for instance, to build elliptic curves over finite fields, which have significant uses in cryptography [9].

2.2 Hecke Group

Hecke group was introduced by Erich Hecke in *1936*. Hecke group $H(\lambda_6)$ is generated by two linear fractional transformations $x(z) = -1/z$and $y(z) = -1/z + \lambda$. Here, if $\lambda = \lambda_q = 2\cos(\pi/q)$ for an integer$q \geq 3$, the $H(\lambda_q)$ is a discrete group. For q=3, Hecke Group $H(\lambda_3)$ acts as a modular group $PSL(2,\mathbb{Z}) =< x, y: x^2 = y^3 = 1 >$. The Hecke Group $H(\lambda_q)$ is the free product of two cyclic groups of order 2 and q [10]. Its finite presentation is $< x, y: x^2 = y^q = 1 >$. For q=6, we have

$$H(\lambda_6) =< x, y: x^2 = y^6 = 1 > \tag{1}$$

with the generators $x(z) = -1/3z$ and $y(z) = -1/3(z+1)$. The action of Hecke groups especially on discrete data has a great impact on various branches of mathematics [11].

2.3 Symmetric Group

The collection of all permutations of bijective functions define on a set X={1,2,3,...n} is denoted by S_n then S_n forms a group under the binary operation of composition of mapping and this group is called a Symmetric group having order n! [12], Due to its wide applications and properties, it is an important subject of study in many fields.

3. METHOD OF PROPOSED S-BOXES

Step 1

For the construction of Substitution boxes, we consider the action of Hecke Group $H(\lambda_6)$ on a projective line over a finite field $PL(F_q) = F_q\{\infty\}$. Where q is a prime or power of a prime. For an instant, consider the action of $H(\lambda_6)$on $PL(F_{17}) = F_{17}\cup\{\infty\} = \{1,2,3,\ldots\ldots,16,\infty\}$. With this action, we get total of 17! number of permutations. From which two permutations are

$$\bar{u} = (0\ \ \infty)(1\ \ 11)(2\ \ 14)(3\ \ 15)(4\ \ 7)(5\ \ 9)(6\ \ 16)(8\ \ 12)(10\ \ 13)$$

$$\bar{v} = (0\ \ 11\ \ 8\ \ 5\ \ 16\ \ \infty)\ (1\ \ 14\ \ 3\ \ 7\ \ 12\ \ 10)\ (2\ \ 15\ \ 6\ \ 4\ \ 9\ \ 13)$$

Now for 16×16 matrix , consider the action of $H(\lambda_6)$ on $PL(F_{257}) = F_{257}\cup\{\infty\} = \{1,2,3,\ldots\ldots,256,\infty\}$. The resultant permutations are

$\bar{x}$ *= (0 ∞)(1 171)(2 214)(3 57)(4 107)(5 137)(6 157)(7 208)(8 182)(9 19)(10 197)(11 109)(12 207)(13 112)(14 104)(15 217)(16 91)(17 131)(18 138)(20 227)(21 155) (22 183)(23 108)(24 232)(25 233)(26 56)(27 92)(28 52) (29 192)(30 237)(31 105)(32 174)(33 122)(34 194)(35 93)(36 69)(37 213)(38 133)(39 123)(40 242)(41 117) (42 206)(43 255)(44 220)(45 158)(46 54)(47 113)(48 116)(49 250)(50 245)(51 215)(53 139)(55 176)(58 96) (59 151)(60 247)(61 66)(62 181)(63 223)(64 87)(65 228) (67 179)(68 97)(70 175)(71 111)(72 163)(73 115)(74 235)(75 249)(76 195)(77 89)(78 190)(79 90)(80 121)(81 202)(82 187)(83 225)(84 103)(85 129)(86 256)(88 110) (94 185)(95 156)(98 125)(99 212)(100 251)(101 162)(102 236)(106 198)(114 130)(118 204)(119 239)(120 252)(124 219)(126 240)(127 143)(128 172)(132 159)(134 218)(135 224)(136 177)(140 216)(141 209)(142 184)(144 210)(145 244)(146 186)(147 169)(148 246)(149 234)(150 253)(152 226)(153 243)(154 173)(160 189)(161 199)(164 222)(165 230)(166 241)(167 178)(168 180)(170 193)(188 221)(191 196)(200 254)(201 231)(203 211)(205 229)(238 248)*

$\bar{y}$*= (0 171 128 85 256 ∞)(1 214 51 28 192 170)(2 57 96 68 36 213)(3 107 23 232 25 56)(4 137 18 9 197 106)(5 157 45 54 176 136)(6 208 141 184 94 156)(7 182 22 108 11 207) (8 19 227 65 61 181)(10 109 88 77 190 196)(12 112 47 116 41 206)(13 104 31 174 70 111)(14 217 134 224 83 103)(15 91 27 52 139 216)(16 131 159 189 78 90)(17 138 53 46 113 130)(20 155 95 58 151 226)(21 183 142 127 172 154)(24 233 149 253 200 231)(26 92 35 69 175 55)(29 237 248 75 195 191)(30 105 198 161 101 236)(32 122 39 242 153 173) (33 194 76 89 79 121)(34 93 185 146 169 193)(37 133 218 124 98 212)(38 123 219 44 158 132)(40 117 204 229 165 241)(42 255 86 64 228 205)(43 220 188 160 199 254)(48 250 100 162 72 115)(49 245 148 234 74 249)(50 215 140 209 144 244)(59 247 238 119 252 150)(60 66 179 168 147 246)(62 223 135 177 167 180)(63 87 110 71 163 222)(67 97 125 240 166 178)(73 235 102 84 129 114)(80 202 211 99 251 120)(81 187 221 164 230 201)(82 225 152 243 145 186)(118 239 126 143 210 203)*

The combination of functions x(z) and y(z) produces a total of 258 elements, including ∞ and 256. However, for the 16×16 matrix, we exclude ∞ and 256 since they are only necessary for the action of $H(\lambda_6)$. So we can make 257! S-boxes. Our proposed S-box is presented in Table 1 and has an acceptable non-linearity of 103.75

Table 1 -S-box proposed by Hecke Group.

128	**154**	**32**	**70**	**55**	**136**	**167**	**67**	**168**	**62**	**8**	**22**	**142**	**94**	**146**	**82**
221	160	78	196	29	170	34	76	191	10	106	161	254	231	81	211
118	229	42	12	7	141	144	203	99	37	2	51	140	15	134	124
44	188	164	63	135	83	152	20	65	205	165	201	24	25	149	74
102	30	248	119	126	166	40	153	145	50	148	60	238	75	49	100
120	150	200	43	86	0	171	214	57	107	137	157	208	182	19	197
109	207	112	104	217	91	131	138	9	227	155	183	108	232	233	56

92	52	192	237	105	174	122	194	93	69	213	133	123	242	117	206
255	220	158	54	113	116	250	245	215	28	139	46	176	26	3	96
151	247	66	181	223	87	228	61	179	97	36	175	111	163	115	235
249	195	89	190	90	121	202	187	225	103	129	64	110	77	79	16
27	35	185	156	58	68	125	1	212	251	162	236	84	14	31	198
4	23	11	88	71	13	47	130	73	48	41	204	239	252	80	33
39	219	98	240	143	172	85	114	17	159	38	218	224	177	5	18
53	216	209	184	127	210	244	186	169	246	234	253	59	226	243	173
21	95	6	45	132	189	199	101	72	222	230	241	178	180	147	193

Step 2

Symmetric group S_{16} has 16! permutations. We improved the uncertainty of our S-box by applying different permutations along the rows. For instance, we apply a permutation

$$a = (1\ 7\ 2\ 9\ 16\ 15\ 10\ 14\ 13\ 5\ 6\ 11\ 12\ 3\ 8\ 4) \tag{2}$$

on the S-box obtained from the Hecke group. By this method, we obtain an S-box given in Table 2. Similarly, we apply a permutation

$$b = (1\ 4\ 13\ 9\ 7\ 14\ 2)(3\ 8\ 5)(10\ 6\ 11\ 15\ 12\ 16) \tag{3}$$

on the 16×16 matrix proposed by the Hecke group to obtain another S-box given in Table 3.

Table 2 -Proposed S-box after applying permutation 'a'

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

Table 3 - Proposed S-box after applying permutation 'b'

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

4. Security Analysis and Comparisons

To evaluate the cryptographic strength of our proposed S-box, we subject it to various tests such as linear approximation probability (LP), differential approximation probability (DP), non-linearity, bit independence criterion (BIC), and strict avalanche criterion. These tests are conducted to assess the effectiveness of the substitution box [13,14]. Furthermore, we also compare our S-box with several standard S-boxes.

4.1. Non-linearity

The degree of non-linearity in a function is a measure of its resistance against linear attacks, indicating how much it deviates from the set of all affine functions. Mathematically, the non-linearity of an n-variable Boolean function can be expressed through its relationship with the Walsh-Hadamard transform [15].

$$N(f) = 2^{n-1} - 2^{\frac{n}{2}-1} \quad (4)$$

Our proposed S-box exhibits an average non-linearity of 105, with a minimum value of 102 and a maximum value of 108.

Table 4 – Comparison of Non-linearity

S boxes	Max	Min	Avg
Proposed S box	108	102	105
AES	112	112	112
Xyi	106	104	105
Gray	112	112	112
Skipjack	108	104	105.75
APA	112	112	112
Prime	104	94	99.5

4.2. Strict Avalanche Criteria

Strict Avalanche Criteria (SAC) was first introduced by Tavares and Webster which take the differences between the input and output bits into account [16]. A cryptosystem satisfies the SAC condition only when altering one input bit causes the output bits for half of the system to change.

$$\frac{1}{2}\sum_{i=1}^{n} |f(x) \oplus f(x \oplus e_i) = 2^{n-1} \quad (5)$$

A comparison of SAC is performed among various S-boxes, and the results are displayed in Table 5.

Table 5– Comparison of SAC

S boxes	Min	Max	Square deviation	Avg
Proposed S box	0.406	0.609	0.046	0.504
AES	0.453	0.562	0.0156	0.504
Xyi	0.406	0.609	0.022	0.502
Gray	0.437	0.562	0.015	0.499
Skipjack	0.39	0.593	0.024	0.503
APA	0.437	0.562	0.016	0.5
Prime	0.343	0.671	0.032	0.516

4.3. Linear Approximation Probability

The probability of linear approximation is utilized for evaluating the degree of imbalance in an event, and this analysis aids in determining the maximum imbalance value of the event's outcome [17]. Mathematically defined as

$$LP = max_{u_x,u_y}|\#x \in {}^{A}/_{x} \,.u_x = S(x).u_y/2^n - {}^{1}/_{2}| \quad (6)$$

The variables u_x and u_y signify the input and output differentials, respectively. A comparison of LAP is performed among various S-boxes, and the outcomes are displayed in Table 6.

Table 6– Comparison of LAP

S boxes	Max LP	Max value
Proposed S box	0.132	162
AES	0.062	144
Xyi	0.156	168
Gray	0.062	144
Skipjack	0.109	156
APA	0.062	144
Prime	0.132	162

4.4. Differential Approximation Probability

This criterion quantifies an S-box's differential homogeneity. In this method, a particular output adjustment must be made when just one input bit is altered. The inputs and outputs of the substitution box's XOR distribution are calculated [18]. Mathematically defined as

$$DP = [\#\{x \in X | S(x) \oplus S(x \oplus \nabla_x) = \nabla_y\}/2^m] \tag{7}$$

where∇_x is known as a differential input and ∇_y as differential output.

Table 7– Comparison of DP

S boxes	Proposed S box	AES	Xyi	Gray	Skipjack	APA	Prime
Max DP	0.0429	**0.015**	0.0468	0.0156	0.0468	0.015	0.281

4.5. BIT Independence Criteria

Webster and Tavares introduced a noteworthy criterion stating that two output bits must also change when one input bit in a cryptosystem is altered [19]. Consequently, it becomes challenging to manipulate the system in a manner that is independent of its individual bits.

Table 8– Comparison of BIT

S boxes	Min	Avg	Square Deviation
Proposed S box	96	103.35	2.763
AES	112	112	0
Xyi	98	103.78	2.743
Gray	112	112	0
Skipjack	102	104.14	1.767
APA	112	112	0
Prime	94	101.71	3.53

5. Image Encryption

To evaluate the S-box's statistical power for use in image encryption, we apply the majority logic criterion (MLC). Since the encryption procedure may distort the image, we conduct multiple analyses to explore its statistical properties, including entropy, correlation, energy, contrast and homogeneity [20]. We perform the encryption process on Lena's image and Capsicum's image.Fig. 1 and Fig. 2 show the encryption of the image, (a) is original image (b) encrypted image.

Figure 1 *(a)* *(b)*

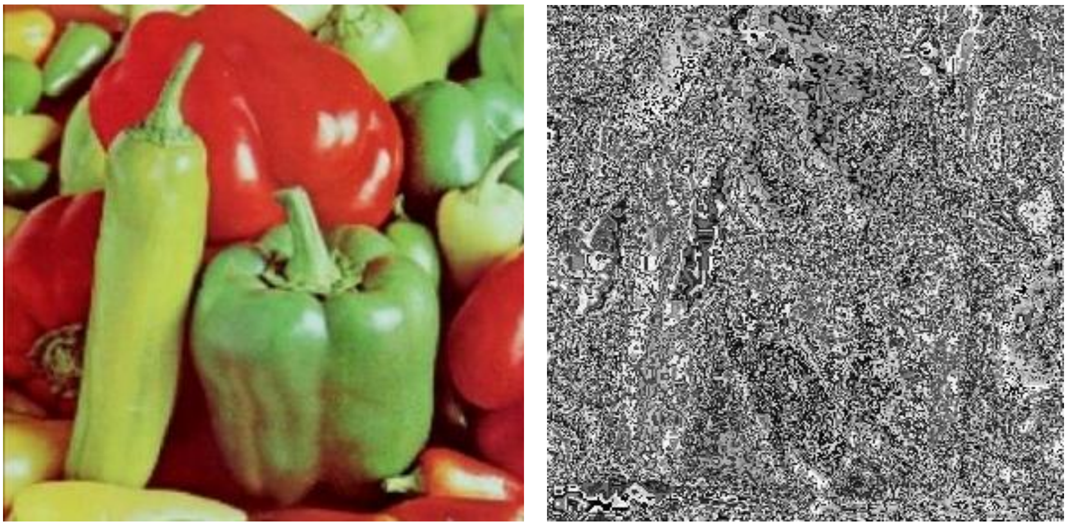

Figure 2 *(a)* *(b)*

6. Conclusions

Our research introduces a novel approach to constructing S-boxes by utilizing the action of Hecke group $H(\lambda_6)$ on the projective line $PL(F_{257})$over the finite field F_{257} To enhance the efficacy of the S-boxes, we subject them to various permutations of the Symmetric group S_{16}. Using different common tests, we have evaluated the strength of the created S-boxes and employed them for image encryption. Going forward, we aim to extend our technique to generate n x n S-boxes by utilizing different permutations of S_{16} in diverse ways.

References

[1] J. Menezes, P.C. Oorschot and S. A Vanstone. “Handbook of Applied Cryptography.” CRC, 2001.

[2] Damico, Tony M. “A Brief History of Cryptography.” Inquiries Journal. 1 Nov.2009, www.inquiriesjournal.com/articles/1698 /a- Brief -history-of- Cryptography.

[3] R. A. Mollin, “An Introduction to Cryptograph.” Chapman and Hall/ CRC, 2007.

[4] C. Paar, J. Pelzl. “Understanding Cryptography.” Springer 2009.

[5] K. Ruohonen, “Mathematical Cryptology”, Translation by J. Kangas and P. Coughlan, 2014.

[6] Y. Naseer , T. Shah , D. Shah, S. Hussain. A Novel Algorithm of Constructing Highly Nonlinear S-p-boxes. Cryptography. 2019; 3(1):6.

[7] N. Siddiqui, A. Naseer, and M. Ehatisham-ul-Haq. A Novel Scheme of Substitution-Box Design Based on Modified Pascal’s Triangle and Elliptic Curve. Wirel. Pers. Commun. 116, 4 (Feb 2021), 3015–3030.

[8] Siddiqui, Nasir et al. “A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field.” PloS one vol. 15, 11 e0241890. 12 Nov. 2020.

[9] I. Shahzad, Q. Mushtaq and A. Razaq. “Construction of New S Box using Action of Quotient of the Modular Group for Multimedia Security.” Security and Communication Network, vol.2019, 2019, pp.1-13.

[10]Q. Afza1, F. Afzal, “Golden Mean and the Action of Mobius Group M”,International Journal of Mathematics and Computational Science, Vol. 4,No. 4, pp. 124-127; ISSN: 2381-702X. 2018.

[11] Deajim, Abdulaziz. “The Hecke group H(λ4) acting on imaginary quadratic number fields.” arXiv: Group Theory (2019): n. pag

[12] A. Razaq et al., A Novel Method for Generation of Strong Substitution Boxes Based on Coset Graphs and Symmetric Groups. in IEEE Access, vol. 8, pp. 75473-75490, 2020.

[13] N. Siddiqui, U. Afsar. “A Novel Construction of S16 AES S-boxes.” International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, August 2016.

[14] Daemen, Joan and Vincent Rijmen. “The Block Cipher Rijndael.” Smart Card Research and Advanced Application Conference (1998).

[15] Nizam Chew LC, Ismail ES. S-box Construction Based on Linear Fractional Transformation and Permutation Function. Symmetry. 2020; 12(5):826.

[16] A. Altaleb, M. S. Saeed, I. Hussain, M. Aslam. ”An algorithm for the construction of substitution box for block ciphers based on projective general linear group.” AIP Advances 1 March 2017; 7 (3): 035116.

[17] N. Siddiqui, U. Afsar. “A Novel Construction of S16 AES S-boxes.” International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, August 2016.

[18] Razaq, A., Ahmad, M., Yousaf, A. et al. A Group Theoretic Construction of Large Number of AES-Like Substitution-Boxes. Wireless PersCommun 122, 2057–2080 (2022).

[19] T. Shah, I. Hussain, M. Gondal and Y. Wang. . Analyses of SKIPJACK S-box. World Applied Sciences Journal. (2011). 13. 2385-2388.

[20] B. Arshad, N. Siddiqui, Z. Hussain. ”A Novel Method for Designing Substitution Boxes Based on Mobius Group.” 15 March 2021,