

## Research Article

# A Novel Construction of Substitution Box Involving Coset Diagram and a Bijective Map

Abdul Razaq,<sup>1</sup> Awais Yousaf,<sup>2</sup> Umer Shuaib,<sup>3</sup> Nasir Siddiqui,<sup>4</sup>  
Atta Ullah,<sup>5</sup> and Adil Waheed<sup>6</sup>

<sup>1</sup>Department of Mathematics, University of Education Lahore, Jauharabad Campus, Jauharabad, Pakistan

<sup>2</sup>Department of Mathematics, The Islamia University of Bahawalpur, Bahawalpur, Pakistan

<sup>3</sup>Department of Mathematics, Government College University Faisalabad, Faisalabad, Pakistan

<sup>4</sup>Department of Basic Sciences, University of Engineering and Technology, Taxila, Punjab, Pakistan

<sup>5</sup>Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan

<sup>6</sup>Department of Information Technology, University of Education Lahore, Jauharabad Campus, Jauharabad, Pakistan

Correspondence should be addressed to Abdul Razaq; [makenqau@gmail.com](mailto:makenqau@gmail.com)

Received 15 August 2017; Accepted 10 October 2017; Published 20 November 2017

Academic Editor: Zheng Yan

Copyright © 2017 Abdul Razaq et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The substitution box is a basic tool to convert the plaintext into an enciphered format. In this paper, we use coset diagram for the action of  $PSL(2, \mathbb{Z})$  on projective line over the finite field  $GF(2^9)$  to construct proposed S-box. The vertices of the cost diagram are elements of  $GF(2^9)$  which can be represented by powers of  $\alpha$ , where  $\alpha$  is the root of irreducible polynomial  $p(x) = x^9 + x^4 + 1$  over  $\mathbb{Z}_2$ . Let  $GF^*(2^9)$  denote the elements of  $GF(2^9)$  which are of the form of even powers of  $\alpha$ . In the first step, we construct a  $16 \times 16$  matrix with the elements of  $GF^*(2^9)$  in a specific order, determined by the coset diagram. Next, we consider  $h : GF^*(2^9) \rightarrow GF(2^8)$  defined by  $h(\alpha^{2n}) = \omega^n$  to destroy the structure of  $GF(2^8)$ . In the last step, we apply a bijective map  $g$  on each element of the matrix to evolve proposed S-box. The ability of the proposed S-box is examined by different available algebraic and statistical analyses. The results are then compared with the familiar S-boxes. We get encouraging statistics of the proposed box after comparison.

## 1. Introduction

In secure communication, the role of the nonlinear component for block ciphers (substitution box) is of significant importance. The concept of substitution box was given by Shannon in 1949 [1]. In order to create confusion during the process of enciphering the digital data, substitution box plays a central role [2]. If the S-box is not good, it means one has to compromise on the quality of encryption. The strength of the S-box affirms the capability of block ciphers. Several attempts have been made to increase the quality of the S-box. In order to assess the properties of well-known S-boxes, the cryptographers have drawn attention to the literature. Different techniques have been developed to inspect the statistical and algebraic structure of S-boxes. These analyses include linear approximation probability (LP) method, bit independence criterion (BIC), majority logic

criterion (MLC), strict avalanche criterion (SAC), nonlinearity method, and differential approximation probability (DP) method.

In this paper, we establish a novel technique to construct substitution boxes by coset diagrams and bijective maps.

## 2. Coset Diagrams for Modular Group

The modular group, denoted by  $PSL(2, \mathbb{Z})$ , has a finite presentation  $\langle x, y : x^2 = y^3 = 1 \rangle$ , where  $x$  and  $y$  are linear fractional transformations which map  $s$  to  $-1/s$  and  $s-1/s$ , respectively. Coset diagrams ([3–7]) are the graphical representation of the action of  $PSL(2, \mathbb{Z})$  on  $GF(p^n) \cup \{\infty\}$ , where  $p$  is a prime. Since the order of  $y$  is three, its three cycles are represented by triangles. The vertices of the triangles, which are elements of  $GF(p^n) \cup \{\infty\}$ , are permuted anticlockwise by  $y$ . Any two of vertices of the triangles are joined by an edge which

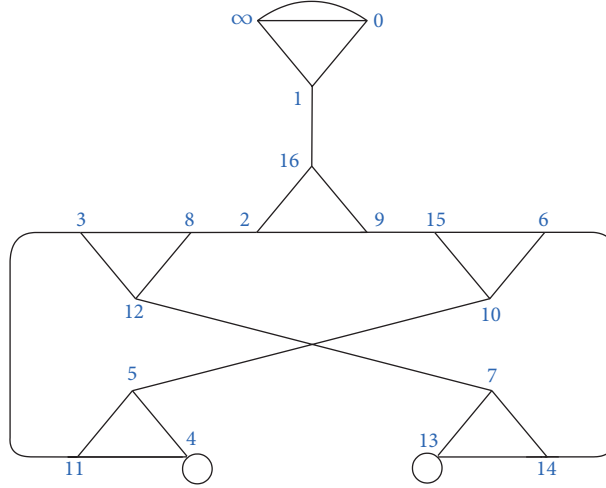


FIGURE 1: The coset diagram for the action of modular group on  $GF(17) \cup \{\infty\}$ .

represents  $x$ . The heavy dots are used to denote fixed points of  $x$  and  $y$ , if they exist.

Consider the action of modular group on  $GF(17) \cup \{\infty\}$  (Figure 1). The permutation representations of  $x$  and  $y$  can be calculated by  $x : s \rightarrow -1/s$  and  $y : s \rightarrow s - 1/s$ .

$$\begin{aligned} x : (0 \ \infty)(1 \ 16)(2 \ 8)(3 \ 11)(4)(5 \ 10)(6 \ 14)(7 \ 12)(9 \ 15)(13) \\ y : (0 \ \infty \ 1)(3 \ 12 \ 8)(2 \ 9 \ 16)(15 \ 10 \ 6)(11 \ 4 \ 5)(13 \ 14 \ 7). \end{aligned} \quad (1)$$

The action of  $PSL(2, \mathbb{Z})$  is not possible on  $GF(p^n)$ , because image of 0 under  $x$  does not belong to  $GF(p^n)$ . Therefore, we choose  $GF(p^n) \cup \{\infty\}$  for the action of  $PSL(2, \mathbb{Z})$  instead of  $GF(p^n)$ .

### 3. Coset Diagram Used in the Construction of Proposed Substitution Box

Consider a primitive irreducible polynomial  $p(x) = x^9 + x^4 + 1$  over  $\mathbb{Z}_2$ ; then  $GF(2^9) = \mathbb{Z}_2[x]/\langle x^9 + x^4 + 1 \rangle$ . The element of

$GF(2^9)$  (see Table 1) can be represented by some power of  $\alpha$ , where  $\alpha$  is the root of  $p(x)$ . Consider the action of  $PSL(2, \mathbb{Z})$  on  $GF(2^9) \cup \{\infty\}$ . Then the permutation representations of  $x$  and  $y$  can be calculated by  $(s)x = -1/s$  and  $(s)y = (s - 1)/s$ , respectively. So

$$\begin{aligned} x : (\alpha^1 \ \alpha^{510})(\alpha^{129} \ \alpha^{382})(\alpha^{381} \ \alpha^{130})(\alpha^2 \ \alpha^{509})(\alpha^{258} \ \alpha^{253})(\alpha^{251} \ \alpha^{260})(\alpha^3 \ \alpha^{508}) \\ (\alpha^{417} \ \alpha^{94})(\alpha^{91} \ \alpha^{420})(\alpha^2 \ \alpha^{509})(\alpha^{258} \ \alpha^{253})(\alpha^{251} \ \alpha^{260})(\alpha^4 \ \alpha^{507})(\alpha^5 \ \alpha^{506}) \\ (\alpha^{502} \ \alpha^9)(\alpha^6 \ \alpha^{505})(\alpha^{323} \ \alpha^{188})(\alpha^{182} \ \alpha^{329})(\alpha^7 \ \alpha^{504})(\alpha^{60} \ \alpha^{451})(\alpha^{444} \ \alpha^{67}) \\ (\alpha^8 \ \alpha^{503})(\alpha^{10} \ \alpha^{501})(\alpha^{493} \ \alpha^{18})(\alpha^{11} \ \alpha^{500})(\alpha^{459} \ \alpha^{52})(\alpha^{41} \ \alpha^{470})(\alpha^{12} \ \alpha^{499}) \\ (\alpha^{135} \ \alpha^{376})(\alpha^{364} \ \alpha^{147})(\alpha^{13} \ \alpha^{498})(\alpha^{125} \ \alpha^{386})(\alpha^{373} \ \alpha^{138})(\alpha^{14} \ \alpha^{497})(\alpha^{120} \ \alpha^{391}) \\ (\alpha^{377} \ \alpha^{134})(\alpha^{15} \ \alpha^{496})(\alpha^{111} \ \alpha^{400})(\alpha^{385} \ \alpha^{126})(\alpha^{16} \ \alpha^{495})(\alpha^{20} \ \alpha^{491})(\alpha^{475} \ \alpha^{36}) \end{aligned}$$

TABLE 1: Representation of the elements of  $GF(2^9)$ .

Binary values	$GF(2^9)$	Binary values	$GF(2^9)$	Binary values	$GF(2^9)$	Binary values	$GF(2^9)$
00000000	0	00000001	1	00000010	$\alpha^1$	00000100	$\alpha^2$
00001000	$\alpha^3$	00001000	$\alpha^4$	00010000	$\alpha^5$	00100000	$\alpha^6$
01000000	$\alpha^7$	10000000	$\alpha^8$	00001001	$\alpha^9$	00010010	$\alpha^{10}$
001000100	$\alpha^{11}$	010001000	$\alpha^{12}$	100010000	$\alpha^{13}$	000110001	$\alpha^{14}$
001100010	$\alpha^{15}$	011000100	$\alpha^{16}$	110001000	$\alpha^{17}$	100000001	$\alpha^{18}$
000010011	$\alpha^{19}$	000100110	$\alpha^{20}$	001001100	$\alpha^{21}$	010011000	$\alpha^{22}$
100110000	$\alpha^{23}$	001110001	$\alpha^{24}$	011100010	$\alpha^{25}$	111000100	$\alpha^{26}$
110011001	$\alpha^{27}$	100100011	$\alpha^{28}$	001010111	$\alpha^{29}$	010101110	$\alpha^{30}$
101011100	$\alpha^{31}$	010101001	$\alpha^{32}$	101010010	$\alpha^{33}$	010110101	$\alpha^{34}$
101101010	$\alpha^{35}$	011000101	$\alpha^{36}$	110001010	$\alpha^{37}$	100000101	$\alpha^{38}$
000011011	$\alpha^{39}$	000110110	$\alpha^{40}$	001101100	$\alpha^{41}$	011011000	$\alpha^{42}$
110110000	$\alpha^{43}$	101110001	$\alpha^{44}$	011110011	$\alpha^{45}$	111100110	$\alpha^{46}$
111011101	$\alpha^{47}$	110101011	$\alpha^{48}$	101000111	$\alpha^{49}$	010011111	$\alpha^{50}$
100111110	$\alpha^{51}$	001101101	$\alpha^{52}$	011011010	$\alpha^{53}$	110110100	$\alpha^{54}$
101111001	$\alpha^{55}$	011100011	$\alpha^{56}$	111000110	$\alpha^{57}$	110011101	$\alpha^{58}$
100101011	$\alpha^{59}$	001000111	$\alpha^{60}$	010001110	$\alpha^{61}$	100011100	$\alpha^{62}$
000101001	$\alpha^{63}$	001010010	$\alpha^{64}$	010100100	$\alpha^{65}$	101001000	$\alpha^{66}$
010000001	$\alpha^{67}$	100000010	$\alpha^{68}$	000010101	$\alpha^{69}$	000101010	$\alpha^{70}$
<b>001010100</b>	$\alpha^{71}$	010101000	$\alpha^{72}$	101010000	$\alpha^{73}$	010110001	$\alpha^{74}$
<b>101100010</b>	$\alpha^{75}$	011010101	$\alpha^{76}$	110101010	$\alpha^{77}$	101000101	$\alpha^{78}$
010011011	$\alpha^{79}$	100110110	$\alpha^{80}$	001111101	$\alpha^{81}$	011111010	$\alpha^{82}$
111110100	$\alpha^{83}$	111110001	$\alpha^{84}$	111100011	$\alpha^{85}$	111010111	$\alpha^{86}$
110111111	$\alpha^{87}$	101101111	$\alpha^{88}$	011001111	$\alpha^{89}$	110011110	$\alpha^{90}$
100101101	$\alpha^{91}$	001001011	$\alpha^{92}$	010010110	$\alpha^{93}$	100101100	$\alpha^{94}$
001001001	$\alpha^{95}$	010010010	$\alpha^{96}$	100100100	$\alpha^{97}$	001011001	$\alpha^{98}$
010110010	$\alpha^{99}$	101100100	$\alpha^{100}$	011011001	$\alpha^{101}$	110110010	$\alpha^{102}$
101110101	$\alpha^{103}$	011111011	$\alpha^{104}$	111110110	$\alpha^{105}$	111111101	$\alpha^{106}$
111101011	$\alpha^{107}$	111000111	$\alpha^{108}$	110011111	$\alpha^{109}$	100101111	$\alpha^{110}$
001001111	$\alpha^{111}$	010011110	$\alpha^{112}$	100111100	$\alpha^{113}$	001101001	$\alpha^{114}$
011010010	$\alpha^{115}$	110100100	$\alpha^{116}$	101011001	$\alpha^{117}$	010100011	$\alpha^{118}$
101000110	$\alpha^{119}$	010011101	$\alpha^{120}$	100111010	$\alpha^{121}$	001100101	$\alpha^{122}$
011001010	$\alpha^{123}$	110010100	$\alpha^{124}$	100111001	$\alpha^{125}$	001100011	$\alpha^{126}$
011000110	$\alpha^{127}$	110001100	$\alpha^{128}$	100001001	$\alpha^{129}$	000000011	$\alpha^{130}$
000000110	$\alpha^{131}$	000001100	$\alpha^{132}$	000011000	$\alpha^{133}$	000110000	$\alpha^{134}$
001100000	$\alpha^{135}$	011000000	$\alpha^{136}$	110000000	$\alpha^{137}$	100010001	$\alpha^{138}$
000110011	$\alpha^{139}$	001100110	$\alpha^{140}$	011001100	$\alpha^{141}$	110011000	$\alpha^{142}$
100100001	$\alpha^{143}$	001010011	$\alpha^{144}$	010100110	$\alpha^{145}$	101001100	$\alpha^{146}$
010001001	$\alpha^{147}$	100010010	$\alpha^{148}$	000110101	$\alpha^{149}$	001101010	$\alpha^{150}$
011010100	$\alpha^{151}$	110101000	$\alpha^{152}$	101000001	$\alpha^{153}$	010010011	$\alpha^{154}$
100100110	$\alpha^{155}$	001011101	$\alpha^{156}$	010111010	$\alpha^{157}$	101110100	$\alpha^{158}$
011111001	$\alpha^{159}$	111110010	$\alpha^{160}$	111110101	$\alpha^{161}$	111111011	$\alpha^{162}$
111100111	$\alpha^{163}$	111011111	$\alpha^{164}$	110101111	$\alpha^{165}$	101001111	$\alpha^{166}$
010001111	$\alpha^{167}$	100011110	$\alpha^{168}$	000101101	$\alpha^{169}$	001011101	$\alpha^{170}$
010110100	$\alpha^{171}$	101101000	$\alpha^{172}$	011000001	$\alpha^{173}$	110000010	$\alpha^{174}$
100010101	$\alpha^{175}$	000111011	$\alpha^{176}$	001110110	$\alpha^{177}$	011101100	$\alpha^{178}$
111011000	$\alpha^{179}$	110100001	$\alpha^{180}$	101010011	$\alpha^{181}$	010110111	$\alpha^{182}$
101101110	$\alpha^{183}$	011001101	$\alpha^{184}$	110011010	$\alpha^{185}$	100100101	$\alpha^{186}$
001011011	$\alpha^{187}$	010110110	$\alpha^{188}$	101101100	$\alpha^{189}$	011001001	$\alpha^{190}$
110010010	$\alpha^{191}$	100110101	$\alpha^{192}$	001111011	$\alpha^{193}$	011110110	$\alpha^{194}$
111101100	$\alpha^{195}$	111001001	$\alpha^{196}$	110000011	$\alpha^{197}$	100010111	$\alpha^{198}$
000111111	$\alpha^{199}$	001111110	$\alpha^{200}$	011111100	$\alpha^{201}$	111111000	$\alpha^{202}$
111100001	$\alpha^{203}$	111010011	$\alpha^{204}$	110110111	$\alpha^{205}$	101111111	$\alpha^{206}$

TABLE I: Continued.

Binary values	$GF(2^9)$	Binary values	$GF(2^9)$	Binary values	$GF(2^9)$	Binary values	$GF(2^9)$
01110111	$\alpha^{207}$	11101110	$\alpha^{208}$	11010101	$\alpha^{209}$	10100101	$\alpha^{210}$
01000011	$\alpha^{211}$	10000110	$\alpha^{212}$	00000101	$\alpha^{213}$	000011010	$\alpha^{214}$
000110100	$\alpha^{215}$	001101000	$\alpha^{216}$	011010000	$\alpha^{217}$	110100000	$\alpha^{218}$
101010001	$\alpha^{219}$	010110011	$\alpha^{220}$	101100110	$\alpha^{221}$	011011101	$\alpha^{222}$
110111010	$\alpha^{223}$	101100101	$\alpha^{224}$	011011011	$\alpha^{225}$	110110110	$\alpha^{226}$
101111101	$\alpha^{227}$	011101011	$\alpha^{228}$	111010110	$\alpha^{229}$	110111101	$\alpha^{230}$
101101011	$\alpha^{231}$	011000111	$\alpha^{232}$	110001110	$\alpha^{233}$	100001101	$\alpha^{234}$
000001011	$\alpha^{235}$	000010110	$\alpha^{236}$	000101100	$\alpha^{237}$	001011000	$\alpha^{238}$
010110000	$\alpha^{239}$	101100000	$\alpha^{240}$	011010001	$\alpha^{241}$	110100010	$\alpha^{242}$
101010101	$\alpha^{243}$	010111011	$\alpha^{244}$	101110110	$\alpha^{245}$	011111101	$\alpha^{246}$
111111010	$\alpha^{247}$	111100101	$\alpha^{248}$	111011011	$\alpha^{249}$	110100111	$\alpha^{250}$
101011111	$\alpha^{251}$	010101111	$\alpha^{252}$	101011110	$\alpha^{253}$	010101101	$\alpha^{254}$
101011010	$\alpha^{255}$	010100101	$\alpha^{256}$	101001010	$\alpha^{257}$	010000101	$\alpha^{258}$
100001010	$\alpha^{259}$	000000101	$\alpha^{260}$	000001010	$\alpha^{261}$	000010100	$\alpha^{262}$
000101000	$\alpha^{263}$	001010000	$\alpha^{264}$	010100000	$\alpha^{265}$	101000000	$\alpha^{266}$
010010001	$\alpha^{267}$	100100010	$\alpha^{268}$	001010101	$\alpha^{269}$	010101010	$\alpha^{270}$
101010100	$\alpha^{271}$	010111001	$\alpha^{272}$	101110010	$\alpha^{273}$	011110101	$\alpha^{274}$
111101010	$\alpha^{275}$	111000101	$\alpha^{276}$	110011011	$\alpha^{277}$	100100111	$\alpha^{278}$
001011111	$\alpha^{279}$	010111110	$\alpha^{280}$	101111100	$\alpha^{281}$	011101001	$\alpha^{282}$
111010010	$\alpha^{283}$	110110101	$\alpha^{284}$	101111011	$\alpha^{285}$	011100111	$\alpha^{286}$
111001110	$\alpha^{287}$	110001101	$\alpha^{288}$	100001011	$\alpha^{289}$	000000111	$\alpha^{290}$
000001110	$\alpha^{291}$	000011100	$\alpha^{292}$	000111000	$\alpha^{293}$	001110000	$\alpha^{294}$
011100000	$\alpha^{295}$	111000000	$\alpha^{296}$	110010001	$\alpha^{297}$	100110011	$\alpha^{298}$
001101111	$\alpha^{299}$	011101110	$\alpha^{300}$	111011100	$\alpha^{301}$	110101001	$\alpha^{302}$
101000011	$\alpha^{303}$	010010111	$\alpha^{304}$	100101110	$\alpha^{305}$	001001101	$\alpha^{306}$
010011010	$\alpha^{307}$	100110100	$\alpha^{308}$	001111001	$\alpha^{309}$	011110010	$\alpha^{310}$
111100100	$\alpha^{311}$	111011001	$\alpha^{312}$	110100011	$\alpha^{313}$	101010111	$\alpha^{314}$
010111111	$\alpha^{315}$	101111110	$\alpha^{316}$	011101101	$\alpha^{317}$	111011010	$\alpha^{318}$
110100101	$\alpha^{319}$	101011011	$\alpha^{320}$	010100111	$\alpha^{321}$	101001110	$\alpha^{322}$
010001101	$\alpha^{323}$	100011010	$\alpha^{324}$	000100101	$\alpha^{325}$	001001010	$\alpha^{326}$
010010100	$\alpha^{327}$	100101000	$\alpha^{328}$	001000001	$\alpha^{329}$	010000010	$\alpha^{330}$
100000100	$\alpha^{331}$	000011001	$\alpha^{332}$	000110010	$\alpha^{333}$	001100100	$\alpha^{334}$
011001000	$\alpha^{335}$	110010000	$\alpha^{336}$	100110001	$\alpha^{337}$	001110011	$\alpha^{338}$
011100110	$\alpha^{339}$	111001100	$\alpha^{340}$	110001001	$\alpha^{341}$	100000011	$\alpha^{342}$
000010111	$\alpha^{343}$	000101110	$\alpha^{344}$	001011100	$\alpha^{345}$	010111000	$\alpha^{346}$
101110000	$\alpha^{347}$	011110001	$\alpha^{348}$	111100010	$\alpha^{349}$	111010101	$\alpha^{350}$
110111011	$\alpha^{351}$	101100111	$\alpha^{352}$	011011111	$\alpha^{353}$	110111110	$\alpha^{354}$
101101101	$\alpha^{355}$	011001011	$\alpha^{356}$	110010110	$\alpha^{357}$	100111101	$\alpha^{358}$
001101011	$\alpha^{359}$	011010110	$\alpha^{360}$	110101100	$\alpha^{361}$	101001001	$\alpha^{362}$
010000011	$\alpha^{363}$	100000110	$\alpha^{364}$	000011101	$\alpha^{365}$	000111010	$\alpha^{366}$
001110100	$\alpha^{367}$	011101000	$\alpha^{368}$	111010000	$\alpha^{369}$	110110001	$\alpha^{370}$
<b>101110011</b>	$\alpha^{371}$	011101111	$\alpha^{372}$	111101110	$\alpha^{373}$	111001101	$\alpha^{374}$
<b>110001011</b>	$\alpha^{375}$	100000111	$\alpha^{376}$	000011111	$\alpha^{377}$	000111110	$\alpha^{378}$
001111100	$\alpha^{379}$	011111000	$\alpha^{380}$	111110000	$\alpha^{381}$	111110001	$\alpha^{382}$
111110011	$\alpha^{383}$	111110111	$\alpha^{384}$	111111111	$\alpha^{385}$	111101111	$\alpha^{386}$
111001111	$\alpha^{387}$	110001111	$\alpha^{388}$	100001111	$\alpha^{389}$	000001111	$\alpha^{390}$
000011110	$\alpha^{391}$	000111100	$\alpha^{392}$	001111000	$\alpha^{393}$	011110000	$\alpha^{394}$
111100000	$\alpha^{395}$	111010001	$\alpha^{396}$	110110011	$\alpha^{397}$	101110111	$\alpha^{398}$
011111111	$\alpha^{399}$	111111110	$\alpha^{400}$	111101101	$\alpha^{401}$	111001011	$\alpha^{402}$
110000111	$\alpha^{403}$	100011111	$\alpha^{404}$	000101111	$\alpha^{405}$	001011110	$\alpha^{406}$
010111100	$\alpha^{407}$	101111000	$\alpha^{408}$	011100001	$\alpha^{409}$	111000010	$\alpha^{410}$
110010101	$\alpha^{411}$	100111011	$\alpha^{412}$	001100111	$\alpha^{413}$	011001110	$\alpha^{414}$

TABLE I: Continued.

Binary values	$GF(2^9)$	Binary values	$GF(2^9)$	Binary values	$GF(2^9)$	Binary values	$GF(2^9)$
110011100	$\alpha^{415}$	100101001	$\alpha^{416}$	001000011	$\alpha^{417}$	010000110	$\alpha^{418}$
100001100	$\alpha^{419}$	000001001	$\alpha^{420}$	000010010	$\alpha^{421}$	000100100	$\alpha^{422}$
001001000	$\alpha^{423}$	010010000	$\alpha^{424}$	100100000	$\alpha^{425}$	001010001	$\alpha^{426}$
010100010	$\alpha^{427}$	101000100	$\alpha^{428}$	010011001	$\alpha^{429}$	100110010	$\alpha^{430}$
001110101	$\alpha^{431}$	011101010	$\alpha^{432}$	111010100	$\alpha^{433}$	110111001	$\alpha^{434}$
101100011	$\alpha^{435}$	011010111	$\alpha^{436}$	110101110	$\alpha^{437}$	101001101	$\alpha^{438}$
010001011	$\alpha^{439}$	100010110	$\alpha^{440}$	000111101	$\alpha^{441}$	001111010	$\alpha^{442}$
011110100	$\alpha^{443}$	111101000	$\alpha^{444}$	111000001	$\alpha^{445}$	110010011	$\alpha^{446}$
100110111	$\alpha^{447}$	001111111	$\alpha^{448}$	011111110	$\alpha^{449}$	111111100	$\alpha^{450}$
111101001	$\alpha^{451}$	111000011	$\alpha^{452}$	110010111	$\alpha^{453}$	100111111	$\alpha^{454}$
001101111	$\alpha^{455}$	011011110	$\alpha^{456}$	110111100	$\alpha^{457}$	101101001	$\alpha^{458}$
011000011	$\alpha^{459}$	110000110	$\alpha^{460}$	100011101	$\alpha^{461}$	000101011	$\alpha^{462}$
001010110	$\alpha^{463}$	010101100	$\alpha^{464}$	101011000	$\alpha^{465}$	010100001	$\alpha^{466}$
101000010	$\alpha^{467}$	010010101	$\alpha^{468}$	100101010	$\alpha^{469}$	001000010	$\alpha^{470}$
010001010	$\alpha^{471}$	100010100	$\alpha^{472}$	000111001	$\alpha^{473}$	001110010	$\alpha^{474}$
011100100	$\alpha^{475}$	111001000	$\alpha^{476}$	110000001	$\alpha^{477}$	100010011	$\alpha^{478}$
000110111	$\alpha^{479}$	001101110	$\alpha^{480}$	011011100	$\alpha^{481}$	110111000	$\alpha^{482}$
101100001	$\alpha^{483}$	011010011	$\alpha^{484}$	110100110	$\alpha^{485}$	101011101	$\alpha^{486}$
010101011	$\alpha^{487}$	101010110	$\alpha^{488}$	010111101	$\alpha^{489}$	101111010	$\alpha^{490}$
011100101	$\alpha^{491}$	111001010	$\alpha^{492}$	110000101	$\alpha^{493}$	100011011	$\alpha^{494}$
000100111	$\alpha^{495}$	001001110	$\alpha^{496}$	010011100	$\alpha^{497}$	100111000	$\alpha^{498}$
001100001	$\alpha^{499}$	011000010	$\alpha^{500}$	110000100	$\alpha^{501}$	100011001	$\alpha^{502}$
000100011	$\alpha^{503}$	001000110	$\alpha^{504}$	010001100	$\alpha^{505}$	100011000	$\alpha^{506}$
000100001	$\alpha^{507}$	001000010	$\alpha^{508}$	010000100	$\alpha^{509}$	100001000	$\alpha^{510}$

$$\begin{aligned}
& (\alpha^{17} \alpha^{494})(\alpha^{324} \alpha^{187})(\alpha^{170} \alpha^{341})(\alpha^{19} \alpha^{492})(\alpha^{402} \alpha^{109})(\alpha^{90} \alpha^{421})(\alpha^{21} \alpha^{490}) \\
& (\alpha^{285} \alpha^{226})(\alpha^{306} \alpha^{205})(\alpha^{22} \alpha^{489})(\alpha^{407} \alpha^{104})(\alpha^{82} \alpha^{429})(\alpha^{23} \alpha^{488})(\alpha^{314} \alpha^{197}) \\
& (\alpha^{174} \alpha^{337})(\alpha^{24} \alpha^{487})(\alpha^{270} \alpha^{241})(\alpha^{217} \alpha^{294})(\alpha^{25} \alpha^{486})(\alpha^{31} \alpha^{480})(\alpha^{455} \alpha^{56}) \\
& (\alpha^{26} \alpha^{485})(\alpha^{250} \alpha^{261})(\alpha^{235} \alpha^{276})(\alpha^{27} \alpha^{484})(\alpha^{115} \alpha^{396})(\alpha^{369} \alpha^{142})(\alpha^{455} \alpha^{56}) \\
& (\alpha^{28} \alpha^{483})(\alpha^{240} \alpha^{271})(\alpha^{243} \alpha^{268})(\alpha^{29} \alpha^{482})(\alpha^{434} \alpha^{77})(\alpha^{48} \alpha^{463})(\alpha^{30} \alpha^{481}) \\
& (\alpha^{222} \alpha^{289})(\alpha^{259} \alpha^{252})(\alpha^{32} \alpha^{479})(\alpha^{40} \alpha^{471})(\alpha^{439} \alpha^{72})(\alpha^{33} \alpha^{478})(\alpha^{148} \alpha^{363}) \\
& (\alpha^{330} \alpha^{181})(\alpha^{34} \alpha^{477})(\alpha^{137} \alpha^{374})(\alpha^{340} \alpha^{171})(\alpha^{35} \alpha^{476})(\alpha^{196} \alpha^{315})(\alpha^{280} \alpha^{231}) \\
& (\alpha^{37} \alpha^{474})(\alpha^{338} \alpha^{173})(\alpha^{136} \alpha^{375})(\alpha^{38} \alpha^{473})(\alpha^{293} \alpha^{218})(\alpha^{180} \alpha^{331})(\alpha^{39} \alpha^{472}) \\
& (\alpha^{175} \alpha^{336})(\alpha^{297} \alpha^{214})(\alpha^{42} \alpha^{469})(\alpha^{59} \alpha^{452})(\alpha^{410} \alpha^{101})(\alpha^{43} \alpha^{468})(\alpha^{327} \alpha^{184}) \\
& (\alpha^{141} \alpha^{370})(\alpha^{44} \alpha^{467})(\alpha^{303} \alpha^{208})(\alpha^{164} \alpha^{347})(\alpha^{45} \alpha^{466})(\alpha^{265} \alpha^{246})(\alpha^{201} \alpha^{310}) \\
& (\alpha^{46} \alpha^{465})(\alpha^{117} \alpha^{394})(\alpha^{348} \alpha^{163})(\alpha^{47} \alpha^{464})(\alpha^{254} \alpha^{257})(\alpha^{210} \alpha^{301})(\alpha^{49} \alpha^{462}) \\
& (\alpha^{70} \alpha^{441})(\alpha^{392} \alpha^{119})(\alpha^{50} \alpha^{461})(\alpha^{62} \alpha^{449})(\alpha^{51} \alpha^{460})(\alpha^{403} \alpha^{108})(\alpha^{57} \alpha^{454}) \\
& (\alpha^{53} \alpha^{458})(\alpha^{172} \alpha^{339})(\alpha^{286} \alpha^{225})(\alpha^{54} \alpha^{457})(\alpha^{230} \alpha^{281})(\alpha^{227} \alpha^{284})(\alpha^{55} \alpha^{456}) \\
& (\alpha^{353} \alpha^{158})(\alpha^{103} \alpha^{408})(\alpha^{58} \alpha^{453})(\alpha^{357} \alpha^{154})(\alpha^{96} \alpha^{415})(\alpha^{61} \alpha^{450})(\alpha^{106} \alpha^{405})
\end{aligned}$$

$$\begin{aligned}
& (\alpha^{344} \alpha^{167})(\alpha^{63} \alpha^{448})(\alpha^{200} \alpha^{311})(\alpha^{248} \alpha^{263})(\alpha^{64} \alpha^{447})(\alpha^{80} \alpha^{431})(\alpha^{367} \alpha^{144}) \\
& (\alpha^{65} \alpha^{446})(\alpha^{191} \alpha^{320})(\alpha^{255} \alpha^{256})(\alpha^{66} \alpha^{445})(\alpha^{296} \alpha^{215})(\alpha^{149} \alpha^{362})(\alpha^{68} \alpha^{443}) \\
& (\alpha^{274} \alpha^{237})(\alpha^{169} \alpha^{342})(\alpha^{69} \alpha^{442})(\alpha^{249} \alpha^{262})(\alpha^{71} \alpha^{440})(\alpha^{198} \alpha^{313})(\alpha^{242} \alpha^{269}) \\
& (\alpha^{73} \alpha^{438})(\alpha^{146} \alpha^{365})(\alpha^{292} \alpha^{219})(\alpha^{74} \alpha^{437})(\alpha^{165} \alpha^{346})(\alpha^{272} \alpha^{239})(\alpha^{75} \alpha^{436}) \\
& (\alpha^{360} \alpha^{151})(\alpha^{146} \alpha^{365})(\alpha^{76} \alpha^{435})(\alpha^{78} \alpha^{433})(\alpha^{350} \alpha^{161})(\alpha^{83} \alpha^{428})(\alpha^{79} \alpha^{432}) \\
& (\alpha^{228} \alpha^{283})(\alpha^{204} \alpha^{307})(\alpha^{81} \alpha^{430})(\alpha^{298} \alpha^{213})(\alpha^{132} \alpha^{379})(\alpha^{84} \alpha^{427})(\alpha^{118} \alpha^{393}) \\
& (\alpha^{309} \alpha^{202})(\alpha^{85} \alpha^{426})(\alpha^{264} \alpha^{247})(\alpha^{162} \alpha^{349})(\alpha^{86} \alpha^{425})(\alpha^{143} \alpha^{368})(\alpha^{282} \alpha^{229}) \\
& (\alpha^{87} \alpha^{424})(\alpha^{267} \alpha^{244})(\alpha^{157} \alpha^{354})(\alpha^{88} \alpha^{423})(\alpha^{95} \alpha^{416})(\alpha^{328} \alpha^{183})(\alpha^{89} \alpha^{422}) \\
& (\alpha^{325} \alpha^{186})(\alpha^{97} \alpha^{414})(\alpha^{92} \alpha^{419})(\alpha^{234} \alpha^{277})(\alpha^{185} \alpha^{326})(\alpha^{93} \alpha^{418})(\alpha^{211} \alpha^{300}) \\
& (\alpha^{207} \alpha^{304})(\alpha^{98} \alpha^{413})(\alpha^{140} \alpha^{371})(\alpha^{273} \alpha^{238})(\alpha^{99} \alpha^{412})(\alpha^{121} \alpha^{390})(\alpha^{291} \alpha^{220}) \\
& (\alpha^{100} \alpha^{411})(\alpha^{124} \alpha^{387})(\alpha^{287} \alpha^{224})(\alpha^{102} \alpha^{409})(\alpha^{295} \alpha^{216})(\alpha^{114} \alpha^{397})(\alpha^{105} \alpha^{406}) \\
& (\alpha^{279} \alpha^{232})(\alpha^{127} \alpha^{384})(\alpha^{107} \alpha^{404})(\alpha^{168} \alpha^{343})(\alpha^{236} \alpha^{275})(\alpha^{110} \alpha^{401})(\alpha^{195} \alpha^{316}) \\
& (\alpha^{206} \alpha^{305})(\alpha^{113} \alpha^{398})(\alpha^{245} \alpha^{266})(\alpha^{153} \alpha^{358})(\alpha^{116} \alpha^{395})(\alpha^{203} \alpha^{308})(\alpha^{192} \alpha^{319}) \\
& (\alpha^{122} \alpha^{389})(\alpha^{212} \alpha^{299})(\alpha^{177} \alpha^{334})(\alpha^{123} \alpha^{388})(\alpha^{233} \alpha^{278})(\alpha^{155} \alpha^{356})(\alpha^{128} \alpha^{383}) \\
& (\alpha^{179} \alpha^{332})(\alpha^{139} \alpha^{372})(\alpha^{194} \alpha^{317})(\alpha^{145} \alpha^{366})(\alpha^{176} \alpha^{335})(\alpha^{190} \alpha^{321})(\alpha^{150} \alpha^{361}) \\
& c(\alpha^{209} \alpha^{302})(\alpha^{152} \alpha^{359})(\alpha^{156} \alpha^{355})(\alpha^{189} \alpha^{322})(\alpha^{166} \alpha^{345})(0 \infty)(1)
\end{aligned}$$

$$\begin{aligned}
y : & (\alpha^1 \alpha^{129} \alpha^{381})(\alpha^{510} \alpha^{130} \alpha^{382})(\alpha^2 \alpha^{258} \alpha^{251})(\alpha^{509} \alpha^{260} \alpha^{253})(\alpha^3 \alpha^{417} \alpha^{91})(\alpha^{508} \alpha^{420} \alpha^{94}) \\
& (\alpha^4 \alpha^5 \alpha^{502})(\alpha^{507} \alpha^9 \alpha^{506})(\alpha^6 \alpha^{323} \alpha^{182})(\alpha^{505} \alpha^{329} \alpha^{188})(\alpha^7 \alpha^{60} \alpha^{444})(\alpha^{504} \alpha^{67} \alpha^{451}) \\
& (\alpha^8 \alpha^{10} \alpha^{493})(\alpha^{503} \alpha^{18} \alpha^{501})(\alpha^{11} \alpha^{459} \alpha^{41})(\alpha^{500} \alpha^{470} \alpha^{52})(\alpha^{12} \alpha^{135} \alpha^{364})(\alpha^{499} \alpha^{147} \alpha^{376}) \\
& (\alpha^{13} \alpha^{125} \alpha^{373})(\alpha^{498} \alpha^{138} \alpha^{386})(\alpha^{14} \alpha^{120} \alpha^{377})(\alpha^{497} \alpha^{134} \alpha^{391})(\alpha^{15} \alpha^{111} \alpha^{385})(\alpha^{496} \alpha^{126} \alpha^{400}) \\
& (\alpha^{16} \alpha^{20} \alpha^{475})(\alpha^{495} \alpha^{36} \alpha^{491})(\alpha^{17} \alpha^{324} \alpha^{170})(\alpha^{494} \alpha^{341} \alpha^{187})(\alpha^{19} \alpha^{402} \alpha^{90})(\alpha^{492} \alpha^{421} \alpha^{109}) \\
& (\alpha^{21} \alpha^{285} \alpha^{205})(\alpha^{490} \alpha^{306} \alpha^{226})(\alpha^{22} \alpha^{407} \alpha^{82})(\alpha^{489} \alpha^{429} \alpha^{104})(\alpha^{23} \alpha^{314} \alpha^{174})(\alpha^{488} \alpha^{337} \alpha^{197}) \\
& (\alpha^{24} \alpha^{270} \alpha^{217})(\alpha^{487} \alpha^{294} \alpha^{241})(\alpha^{25} \alpha^{31} \alpha^{455})(\alpha^{486} \alpha^{56} \alpha^{480})(\alpha^{26} \alpha^{250} \alpha^{235})(\alpha^{485} \alpha^{276} \alpha^{261}) \\
& (\alpha^{27} \alpha^{115} \alpha^{369})(\alpha^{484} \alpha^{142} \alpha^{396})(\alpha^{28} \alpha^{240} \alpha^{243})(\alpha^{483} \alpha^{268} \alpha^{271})(\alpha^{29} \alpha^{434} \alpha^{48})(\alpha^{482} \alpha^{463} \alpha^{77}) \\
& (\alpha^{30} \alpha^{222} \alpha^{259})(\alpha^{481} \alpha^{252} \alpha^{289})(\alpha^{32} \alpha^{40} \alpha^{439})(\alpha^{479} \alpha^{72} \alpha^{471})(\alpha^{33} \alpha^{148} \alpha^{330})(\alpha^{478} \alpha^{181} \alpha^{363}) \\
& (\alpha^{34} \alpha^{137} \alpha^{340})(\alpha^{477} \alpha^{171} \alpha^{374})(\alpha^{35} \alpha^{196} \alpha^{280})(\alpha^{476} \alpha^{231} \alpha^{315})(\alpha^{37} \alpha^{338} \alpha^{136})(\alpha^{474} \alpha^{375} \alpha^{173}) \\
& (\alpha^{38} \alpha^{293} \alpha^{180})(\alpha^{473} \alpha^{331} \alpha^{218})(\alpha^{39} \alpha^{175} \alpha^{297})(\alpha^{472} \alpha^{214} \alpha^{336})(\alpha^{42} \alpha^{59} \alpha^{410})(\alpha^{469} \alpha^{101} \alpha^{452}) \\
& (\alpha^{43} \alpha^{327} \alpha^{141})(\alpha^{468} \alpha^{370} \alpha^{184})(\alpha^{44} \alpha^{303} \alpha^{164})(\alpha^{467} \alpha^{347} \alpha^{208})(\alpha^{45} \alpha^{265} \alpha^{201})(\alpha^{466} \alpha^{310} \alpha^{246}) \\
& (\alpha^{46} \alpha^{117} \alpha^{348})(\alpha^{465} \alpha^{163} \alpha^{394})(\alpha^{47} \alpha^{254} \alpha^{210})(\alpha^{464} \alpha^{301} \alpha^{257})(\alpha^{49} \alpha^{70} \alpha^{392})(\alpha^{462} \alpha^{119} \alpha^{441}) \\
& (\alpha^{50} \alpha^{62} \alpha^{399})(\alpha^{461} \alpha^{112} \alpha^{449})(\alpha^{51} \alpha^{403} \alpha^{57})(\alpha^{460} \alpha^{454} \alpha^{108})(\alpha^{53} \alpha^{172} \alpha^{286})(\alpha^{458} \alpha^{225} \alpha^{339})
\end{aligned}$$

$$\begin{aligned}
& (\alpha^{54} \alpha^{230} \alpha^{227}) (\alpha^{457} \alpha^{284} \alpha^{281}) (\alpha^{55} \alpha^{353} \alpha^{103}) (\alpha^{456} \alpha^{408} \alpha^{158}) (\alpha^{58} \alpha^{357} \alpha^{96}) (\alpha^{453} \alpha^{415} \alpha^{154}) \\
& (\alpha^{61} \alpha^{106} \alpha^{344}) (\alpha^{450} \alpha^{167} \alpha^{405}) (\alpha^{63} \alpha^{200} \alpha^{248}) (\alpha^{448} \alpha^{263} \alpha^{311}) (\alpha^{64} \alpha^{80} \alpha^{367}) (\alpha^{447} \alpha^{144} \alpha^{431}) \\
& (\alpha^{65} \alpha^{191} \alpha^{255}) (\alpha^{446} \alpha^{256} \alpha^{320}) (\alpha^{66} \alpha^{296} \alpha^{149}) (\alpha^{445} \alpha^{362} \alpha^{215}) (\alpha^{68} \alpha^{274} \alpha^{169}) (\alpha^{443} \alpha^{342} \alpha^{237}) \\
& (\alpha^{69} \alpha^{193} \alpha^{249}) (\alpha^{442} \alpha^{262} \alpha^{318}) (\alpha^{71} \alpha^{198} \alpha^{242}) (\alpha^{440} \alpha^{269} \alpha^{313}) (\alpha^{73} \alpha^{146} \alpha^{292}) (\alpha^{438} \alpha^{219} \alpha^{365}) \\
& (\alpha^{74} \alpha^{165} \alpha^{272}) (\alpha^{437} \alpha^{239} \alpha^{346}) (\alpha^{75} \alpha^{360} \alpha^{76}) (\alpha^{436} \alpha^{435} \alpha^{151}) (\alpha^{78} \alpha^{350} \alpha^{83}) (\alpha^{433} \alpha^{428} \alpha^{161}) \\
& (\alpha^{79} \alpha^{228} \alpha^{204}) (\alpha^{432} \alpha^{307} \alpha^{283}) (\alpha^{81} \alpha^{298} \alpha^{132}) (\alpha^{430} \alpha^{379} \alpha^{213}) (\alpha^{84} \alpha^{118} \alpha^{309}) (\alpha^{427} \alpha^{202} \alpha^{393}) \\
& (\alpha^{85} \alpha^{264} \alpha^{162}) (\alpha^{426} \alpha^{349} \alpha^{247}) (\alpha^{86} \alpha^{143} \alpha^{282}) (\alpha^{425} \alpha^{229} \alpha^{368}) (\alpha^{87} \alpha^{267} \alpha^{157}) (\alpha^{424} \alpha^{354} \alpha^{244}) \\
& (\alpha^{88} \alpha^{95} \alpha^{328}) (\alpha^{423} \alpha^{183} \alpha^{416}) (\alpha^{89} \alpha^{325} \alpha^{97}) (\alpha^{422} \alpha^{414} \alpha^{186}) (\alpha^{92} \alpha^{234} \alpha^{185}) (\alpha^{419} \alpha^{326} \alpha^{277}) \\
& (\alpha^{93} \alpha^{211} \alpha^{207}) (\alpha^{418} \alpha^{304} \alpha^{300}) (\alpha^{98} \alpha^{140} \alpha^{273}) (\alpha^{413} \alpha^{238} \alpha^{371}) (\alpha^{99} \alpha^{121} \alpha^{291}) (\alpha^{412} \alpha^{220} \alpha^{390}) \\
& (\alpha^{100} \alpha^{124} \alpha^{287}) (\alpha^{411} \alpha^{224} \alpha^{387}) (\alpha^{102} \alpha^{295} \alpha^{114}) (\alpha^{409} \alpha^{397} \alpha^{216}) (\alpha^{105} \alpha^{279} \alpha^{127}) (\alpha^{406} \alpha^{384} \alpha^{232}) \\
& (\alpha^{107} \alpha^{168} \alpha^{236}) (\alpha^{404} \alpha^{275} \alpha^{343}) (\alpha^{110} \alpha^{195} \alpha^{206}) (\alpha^{401} \alpha^{305} \alpha^{316}) (\alpha^{113} \alpha^{245} \alpha^{153}) (\alpha^{398} \alpha^{358} \alpha^{266}) \\
& (\alpha^{116} \alpha^{203} \alpha^{192}) (\alpha^{395} \alpha^{319} \alpha^{308}) (\alpha^{122} \alpha^{212} \alpha^{177}) (\alpha^{389} \alpha^{334} \alpha^{299}) (\alpha^{123} \alpha^{233} \alpha^{155}) (\alpha^{388} \alpha^{356} \alpha^{278}) \\
& (\alpha^{128} \alpha^{160} \alpha^{223}) (\alpha^{383} \alpha^{288} \alpha^{351}) (\alpha^{131} \alpha^{159} \alpha^{221}) (\alpha^{380} \alpha^{290} \alpha^{352}) (\alpha^{133} \alpha^{199} \alpha^{179}) (\alpha^{378} \alpha^{332} \alpha^{312}) \\
& c (\alpha^{139} \alpha^{194} \alpha^{178}) (\alpha^{372} \alpha^{333} \alpha^{317}) (\alpha^{145} \alpha^{176} \alpha^{190}) (\alpha^{366} \alpha^{321} \alpha^{335}) (\alpha^{150} \alpha^{209} \alpha^{152}) (\alpha^{361} \alpha^{359} \alpha^{302}) \\
& (\alpha^{156} \alpha^{189} \alpha^{166}) (\alpha^{355} \alpha^{345} \alpha^{322}) (\infty \ 1 \ 0)
\end{aligned}$$

(2)

The coset diagram for this action has 86 orbits (fragments). It has one copy of  $\lambda$  (Figure 2) and 85 copies of  $\gamma_j$  (Figure 3). First, we find the orbit of coset diagram which contains  $\alpha^1$  (Figure 4).

In each  $\gamma_j$ , one can see that  $xyxy^{-1}x \in PSL(2, \mathbb{Z})$  is a path from the vertex  $\alpha^k$  to the vertex  $\alpha^l$ , such that, during this journey, one has to pass each vertex of  $\gamma_j$ .

#### 4. Algebraic Structure of Proposed Substitution Box

In the literature, algebraic techniques are being applied on Galois fields. In this novel technique, the initial sequence of Galois field is destroyed with the help of vertices of the coset diagram.

Let  $GF^*(2^9)$  denote the elements of  $GF(2^9)$  which are of the form of even powers of  $\alpha$ .

Our first aim is to write the vertices of coset diagram in a  $16 \times 16$  matrix. For this, we choose only those vertices which belong to  $GF^*(2^9)$ .

*Step 1.* Our coset diagram has 86 orbits; we construct a  $16 \times 16$  matrix having entries from  $GF^*(2^9)$  in the following way.

First, we find the orbit of coset diagram which contains  $\alpha^1$ . Let us denote this orbit by  $\gamma_1$  and apply  $xyxy^{-1}x$  on  $\alpha^1$ , so that we reach  $\alpha^{382}$ . During this journey, we pass through  $\alpha^{510}$ ,  $\alpha^{130}$ ,  $\alpha^{381}$ , and  $\alpha^{129}$  and at the end reach  $\alpha^{382}$ . Write  $\alpha^{510}$ ,  $\alpha^{130}$ , and  $\alpha^{382}$  as first three elements of the first row of  $16 \times 16$  matrix.

After writing 3 vertices of any  $\gamma_k \in \{\gamma_j : j = 1, 2, 3, \dots, 85\}$ , in order to select the next copy from  $\gamma_j$ , we find a vertex  $v = \alpha^{i_1+1}$ , where  $\alpha^{i_1}$ ,  $\alpha^{i_2}$ ,  $\alpha^{i_3}$ ,  $\alpha^{i_4}$ ,  $\alpha^{i_5}$ , and  $\alpha^{i_6}$  are the vertices of  $\gamma_k$ , such that  $i_1 < i_j$ , where  $j = 2, 3, 4, 5, 6$ . If  $\alpha^{i_1+1}$  is already exhausted in previously chosen copies of  $\gamma_j$ , then we move to the copy of  $\gamma_j$  containing  $v = \alpha^{i_1+2}$  and so on. Apply  $xyxy^{-1}x$  on  $v$  so that we pass through each vertex. Note that, in each  $\gamma_j$ , only three vertices belong to  $GF^*(2^9)$  out of 6. Write these 3 vertices in  $16 \times 16$  matrix in order. The process continues until all the 510 vertices of  $\gamma_j$  are exhausted. Next, pick 0 from  $\lambda$  and write it as last element of the last row.

*Step 2.* Consider  $h : GF^*(2^9) \rightarrow GF(2^8)$  defined by  $f(\alpha^{2^n}) = \bar{\omega}^n$ ; the elements of  $F_{2^8}$  can be represented by powers of  $\omega$  (see Table 3), where  $\omega$  is the root of irreducible polynomial  $p(x) = x^8 + x^4 + x^3 + x^2 + 1$  over  $\mathbb{Z}_2$ . In this step, we apply  $h$  on each element of the matrix evolved in the first step. In this

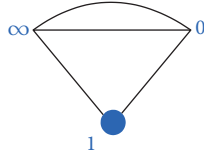


FIGURE 2: The orbit  $\lambda$  of the coset diagram for the action of modular group on  $GF(2^9) \cup \{\infty\}$ .

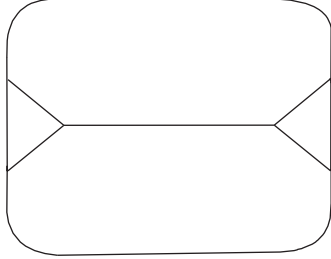


FIGURE 3: The orbit  $\gamma_j$  of the coset diagram for the action of modular group on  $GF(2^9) \cup \{\infty\}$ .

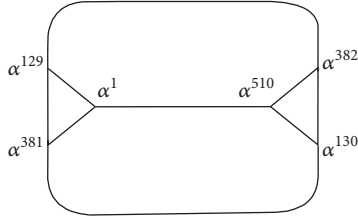


FIGURE 4: The copy of  $\gamma_j$  having the vertex  $\alpha^1$ .

way, we obtain a  $16 \times 16$  matrix having entries from  $GF(2^8)$ . Next, we convert each entry of the matrix into binary form and ultimately into decimal form (Table 4).

Before going to Step 3, let us define a map  $g$  in the following way.

Let  $f$  be the linear fractional transformation, obtained by the action of  $PGL(2, (F(2^8))$  on  $GF(2^8)$ ; that is,  $f : PGL(2, GF(2^8) \times GF(2^8)) \rightarrow GF(2^8)$ .

Clearly  $f$  is of the form  $az + b/cz + d$ , where  $a, b, c, d \in GF(2^8)$ , and is a mapping from  $GF(2^8) \rightarrow GF(2^8)$ . But, usually  $f$  is not a bijective map.

- (i) Let there be  $n$  elements of  $GF(2^8)$  missing in the range of  $f$ .
- (ii) Let  $s_1, s_2, s_3, \dots, s_k \in GF(2^8)$  be repeated in the range of  $f$ .
- (iii) Let  $t_1, t_2, t_3, \dots, t_k$  be the smallest elements in  $GF(2^8)$  whose images are  $s_1, s_2, s_3, \dots, s_k$ , respectively.

Suppose that  $A = \{a_1, a_2, \dots, a_n : a_i < a_{i+1}\}$  is the set of all those elements, except  $t_1, t_2, t_3, \dots, t_k$ , whose images are  $s_1, s_2, s_3, \dots, s_k$ , and  $B = \{b_1, b_2, \dots, b_n : b_i > b_{i+1}\}$  is the set of missing elements in the range of  $f$ . Then

$$g(z) = \begin{cases} f(z) & \text{if } z \in GF(2^8) - A \\ b_i & \text{if } z = a_i. \end{cases} \quad (3)$$

In this paper, we have taken  $f(z) = 214z + 93/124z + 123$ .

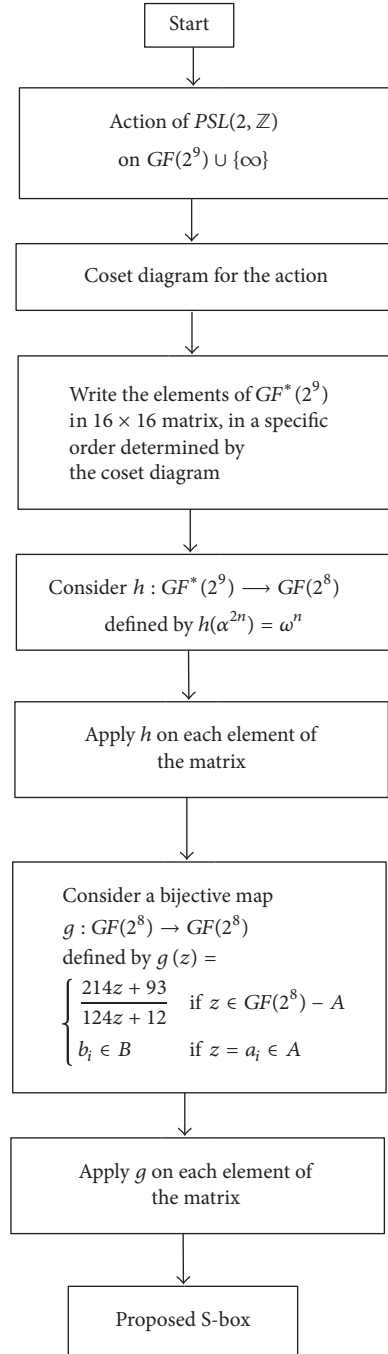


FIGURE 5: Flowchart for the construction of the proposed S-box.

Step 3. In this step, the bijective map  $g$  defined by

$$g(z) = \begin{cases} \frac{214z + 93}{124z + 123} & \text{if } z \in GF(2^8) - A \\ b_i & \text{if } z = a_i \end{cases} \quad (4)$$

is applied on the matrix obtained at the end of Step 2 to evolve proposed S-box (Figure 5 and Table 5). More details of this last step are given in Table 2.



TABLE 2: Construction of S-box using linear fractional transformation.

$z$	$f(z) = \frac{214z + 93}{124z + 123}$		$g(z)$
0	$f(0) = \frac{93}{124} = \frac{01011101}{01111011} = \frac{\omega^{56}}{\omega^{172}} = \omega^{139} = 1000010 = 66$		66
1	$f(1) = \frac{51}{247} = \frac{00110011}{11110111} = \frac{\omega^{125}}{\omega^{232}} = \omega^{148} = 01010010 = 82$		82
2	$f(2) = \frac{9}{115} = \frac{00001001}{01110011} = \frac{\omega^{223}}{\omega^{159}} = \omega^{64} = 01011111 = 95$		95
	$\vdots$		
254	$f(254) = \frac{177}{131} = \frac{10110001}{10000011} = \frac{\omega^{86}}{\omega^{247}} = \omega^{94} = 01110001 = 113$		2
255	$f(255) = \frac{135}{255} = \frac{10000111}{11111111} = \frac{\omega^{13}}{\omega^{175}} = \omega^{93} = 10110110 = 182$		0

TABLE 3: Representation of the elements of  $GF(2^8)$ .

Binary values	$GF(2^8)$	Binary values	$GF(2^8)$	Binary values	$GF(2^8)$	Binary values	$GF(2^8)$
00000000	0	00000001	1	00000010	$\omega^1$	00000100	$\omega^2$
00001000	$\omega^3$	00010000	$\omega^4$	00100000	$\omega^5$	01000000	$\omega^6$
10000000	$\omega^7$	00011010	$\omega^8$	00111010	$\omega^9$	01110100	$\omega^{10}$
11101000	$\omega^{11}$	11001101	$\omega^{12}$	10000111	$\omega^{13}$	00010011	$\omega^{14}$
00100110	$\omega^{15}$	01001100	$\omega^{16}$	10011000	$\omega^{17}$	00101101	$\omega^{18}$
01011010	$\omega^{19}$	10110100	$\omega^{20}$	01110101	$\omega^{21}$	11101010	$\omega^{22}$
11001001	$\omega^{23}$	10001111	$\omega^{24}$	00000011	$\omega^{25}$	00000110	$\omega^{26}$
00001100	$\omega^{27}$	00011000	$\omega^{28}$	00110000	$\omega^{29}$	01100000	$\omega^{30}$
11000000	$\omega^{31}$	10011101	$\omega^{32}$	00100111	$\omega^{33}$	01001110	$\omega^{34}$
10011100	$\omega^{35}$	00100101	$\omega^{36}$	01001010	$\omega^{37}$	10010100	$\omega^{38}$
00110101	$\omega^{39}$	01101010	$\omega^{40}$	11010100	$\omega^{41}$	10110101	$\omega^{42}$
01110111	$\omega^{43}$	11101110	$\omega^{44}$	11000001	$\omega^{45}$	10011111	$\omega^{46}$
00100011	$\omega^{47}$	01000110	$\omega^{48}$	10001100	$\omega^{49}$	00000101	$\omega^{50}$
00001010	$\omega^{51}$	00010100	$\omega^{52}$	00101000	$\omega^{53}$	01010000	$\omega^{54}$
10100000	$\omega^{55}$	01011101	$\omega^{56}$	10111010	$\omega^{57}$	01101001	$\omega^{58}$
11010010	$\omega^{59}$	10111001	$\omega^{60}$	01101111	$\omega^{61}$	11011110	$\omega^{62}$
10100001	$\omega^{63}$	01011111	$\omega^{64}$	10111110	$\omega^{65}$	01100001	$\omega^{66}$
11000010	$\omega^{67}$	10011001	$\omega^{68}$	00101111	$\omega^{69}$	01011110	$\omega^{70}$
10111100	$\omega^{71}$	01100101	$\omega^{72}$	11001010	$\omega^{73}$	10001001	$\omega^{74}$
00001111	$\omega^{75}$	00011110	$\omega^{76}$	00111100	$\omega^{77}$	01111000	$\omega^{78}$
11110000	$\omega^{79}$	11111101	$\omega^{80}$	11100111	$\omega^{81}$	11010011	$\omega^{82}$
10111011	$\omega^{83}$	01101011	$\omega^{84}$	11010110	$\omega^{85}$	10110001	$\omega^{86}$
01111111	$\omega^{87}$	11111110	$\omega^{88}$	11100001	$\omega^{89}$	11011111	$\omega^{90}$
10100011	$\omega^{91}$	01011011	$\omega^{92}$	10110110	$\omega^{93}$	01110001	$\omega^{94}$
11100010	$\omega^{95}$	11011001	$\omega^{96}$	10101111	$\omega^{97}$	01000011	$\omega^{98}$
10000110	$\omega^{99}$	00010001	$\omega^{100}$	00100010	$\omega^{101}$	01000100	$\omega^{102}$
10001000	$\omega^{103}$	00001101	$\omega^{104}$	00011010	$\omega^{105}$	00110100	$\omega^{106}$
01101000	$\omega^{107}$	11010000	$\omega^{108}$	10111101	$\omega^{109}$	01100111	$\omega^{110}$
11001110	$\omega^{111}$	10000001	$\omega^{112}$	00011111	$\omega^{113}$	00111110	$\omega^{114}$
01111100	$\omega^{115}$	11111000	$\omega^{116}$	11101101	$\omega^{117}$	11000111	$\omega^{118}$
10010011	$\omega^{119}$	00111011	$\omega^{120}$	01110110	$\omega^{121}$	11101100	$\omega^{122}$
11000101	$\omega^{123}$	10010111	$\omega^{124}$	00110011	$\omega^{125}$	01100110	$\omega^{126}$
11001100	$\omega^{127}$	10000101	$\omega^{128}$	00010111	$\omega^{129}$	00101110	$\omega^{130}$
01011100	$\omega^{131}$	10111000	$\omega^{132}$	01101101	$\omega^{133}$	11011010	$\omega^{134}$

TABLE 3: Continued.

Binary values	$GF(2^8)$	Binary values	$GF(2^8)$	Binary values	$GF(2^8)$	Binary values	$GF(2^8)$
10101001	$\omega^{135}$	01001111	$\omega^{136}$	10011110	$\omega^{137}$	00100001	$\omega^{138}$
01000010	$\omega^{139}$	10000100	$\omega^{140}$	00010101	$\omega^{141}$	00101010	$\omega^{142}$
01010100	$\omega^{143}$	10101000	$\omega^{144}$	01001101	$\omega^{145}$	10011010	$\omega^{146}$
00101001	$\omega^{147}$	01010010	$\omega^{148}$	10100100	$\omega^{149}$	01010101	$\omega^{150}$
10101010	$\omega^{151}$	01001001	$\omega^{152}$	10010010	$\omega^{153}$	00111001	$\omega^{154}$
01110010	$\omega^{155}$	11100100	$\omega^{156}$	11010101	$\omega^{157}$	10110111	$\omega^{158}$
01110011	$\omega^{159}$	11100110	$\omega^{160}$	11010001	$\omega^{161}$	10111111	$\omega^{162}$
01100011	$\omega^{163}$	11000110	$\omega^{164}$	10010001	$\omega^{165}$	00111111	$\omega^{166}$
01111110	$\omega^{167}$	11111100	$\omega^{168}$	11100101	$\omega^{169}$	11010111	$\omega^{170}$
10110011	$\omega^{171}$	01111011	$\omega^{172}$	11110110	$\omega^{173}$	11110001	$\omega^{174}$
11111111	$\omega^{175}$	11100011	$\omega^{176}$	11011011	$\omega^{177}$	10101011	$\omega^{178}$
01001011	$\omega^{179}$	10010110	$\omega^{180}$	00110001	$\omega^{181}$	01100010	$\omega^{182}$
11000100	$\omega^{183}$	10010101	$\omega^{184}$	00110111	$\omega^{185}$	01101110	$\omega^{186}$
11011100	$\omega^{187}$	10100101	$\omega^{188}$	01010111	$\omega^{189}$	10101110	$\omega^{190}$
01000001	$\omega^{191}$	10000010	$\omega^{192}$	00011001	$\omega^{193}$	00110010	$\omega^{194}$
01100100	$\omega^{195}$	11001000	$\omega^{196}$	10001101	$\omega^{197}$	00000111	$\omega^{198}$
00001110	$\omega^{199}$	00011100	$\omega^{200}$	00111000	$\omega^{201}$	01110000	$\omega^{202}$
11100000	$\omega^{203}$	11011101	$\omega^{204}$	10100111	$\omega^{205}$	01010011	$\omega^{206}$
10100110	$\omega^{207}$	01010001	$\omega^{208}$	10100010	$\omega^{209}$	01011001	$\omega^{210}$
10110010	$\omega^{211}$	01111001	$\omega^{212}$	11110010	$\omega^{213}$	11111001	$\omega^{214}$
11101111	$\omega^{215}$	11000011	$\omega^{216}$	10011011	$\omega^{217}$	00101011	$\omega^{218}$
01010110	$\omega^{219}$	10101100	$\omega^{220}$	01000101	$\omega^{221}$	10001010	$\omega^{222}$
00001001	$\omega^{223}$	00010010	$\omega^{224}$	00100100	$\omega^{225}$	01001000	$\omega^{226}$
10010000	$\omega^{227}$	00111101	$\omega^{228}$	01111010	$\omega^{229}$	11110100	$\omega^{230}$
11110101	$\omega^{231}$	11110111	$\omega^{232}$	11110011	$\omega^{233}$	11111011	$\omega^{234}$
11101011	$\omega^{235}$	11001011	$\omega^{236}$	10001011	$\omega^{237}$	00001011	$\omega^{238}$
00010110	$\omega^{239}$	00101100	$\omega^{240}$	01011000	$\omega^{241}$	10110000	$\omega^{242}$
01111101	$\omega^{243}$	11111010	$\omega^{244}$	11101001	$\omega^{245}$	11001111	$\omega^{246}$
10000011	$\omega^{247}$	00011011	$\omega^{248}$	00110110	$\omega^{249}$	01101100	$\omega^{250}$
11011000	$\omega^{251}$	10101101	$\omega^{252}$	01000111	$\omega^{253}$	10001110	$\omega^{254}$

TABLE 4:  $16 \times 16$  matrix evolved after 2nd step.

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

TABLE 5: Proposed S-box evolved after 3rd step.

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

TABLE 6: Nonlinearity of basic functions of various substitution boxes.

S-box	$f_0$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$	$f_7$	Ave
Gray [13]	112	112	112	112	112	112	112	112	112
Gautam et al. [14]	108	106	104	98	102	102	98	74	99
Prime [15]	94	100	104	104	102	100	98	94	99.5
$S_8$ AES [16]	112	112	112	112	112	112	112	112	112
Shi et al. [17]	106	104	106	106	104	106	104	106	105
AES [2]	112	112	112	112	112	112	112	112	112
Skipjac and Kea [18]	104	108	108	108	108	104	104	106	106.75
Alkhalidi et al. [19]	108	104	106	106	102	98	104	108	104
Chen et al. [20]	100	102	103	104	106	106	106	108	104.3
Tang et al. [21]	100	103	104	104	105	105	106	109	104.5
Khan et al. [22]	102	108	106	102	106	106	106	98	104.25
Belazi et al. [23]	106	106	106	104	108	102	106	104	105.25
Proposed	108	106	108	108	108	104	106	106	106.75

## 5. Statistical Analysis and Simulation Results

In this section, we implement various security performance tests on newly created S-box to examine its special properties. The assessment of the characteristics of proposed S-box determines its application in different encryption methods and for security purposes. We use five different security performance tests, namely, linear approximation probability (LP), differential approximation probability (DP), nonlinearity, bit independence criterion (BIC), and strict avalanche criterion, to assess the cryptographic competence of substitution box. The results obtained from proposed S-box are then compared with the well-known S-boxes. The description of different types of tests implemented on these S-boxes is given below.

**5.1. Nonlinearity.** The concept of nonlinearity was first introduced by Pieprzyk and Finkelstein in 1988 [8]. It is the basic tool to measure the strength of the S-box. An S-box with bigger nonlinearity is more secure than that with lesser nonlinearity. The nonlinearity is expressed as

$$N_h = 2^{n-1} (1 - 2^{-n} \max |S_{(h)}(\alpha)|), \quad (5)$$

where  $S_{(h)}(\alpha) = \sum (-1)^{h(\beta) \oplus \beta \alpha}$  is Walsh spectrum and  $\alpha, \beta \in GF(2^n)$ .

The average value of the nonlinearity of the proposed S-box is 106.75. In Table 6, nonlinearity of the proposed S-box is compared with multiple renowned substitution boxes. One can see that the nonlinearity of the proposed S-box is better than most of the familiar S-boxes.

TABLE 7: Nonlinearity of bit independence criterion of the proposed S-box.

—	96	104	104	106	106	108	106
96	—	106	102	102	102	106	106
104	106	—	104	102	106	102	106
104	102	104	—	104	102	104	102
106	102	102	104	—	104	104	96
106	102	106	102	104	—	102	106
108	106	102	104	104	102	—	104
106	106	106	102	96	106	104	—

TABLE 8: Bit independence criterion of various substitution boxes.

S-boxes	Minimum value	Average	Square deviation
Proposed	96	103.643	2.7283
Gray [13]	112	112	0
Gautam et al. [14]	92	103	3.5225
Prime [15]	94	101.71	3.53
S <sub>8</sub> AES [16]	112	112	0
Hussain et al. [12]	98	103.78	2.743
AES [2]	112	112	0
Hussain et al. [15]	102	104.14	1.767

TABLE 9: Strict avalanche criterion of the proposed S-box.

.4375	.5000	.5000	.4844	.4844	.4844	.5312	.4375
.5000	.4375	.5000	.5625	.5000	.5469	.4688	.5000
.5312	.5469	.5156	.4687	.4531	.5312	.5156	.4375
.4844	.4375	.5469	.5312	.4688	.5781	.5781	.5000
.4688	.5156	.4531	.5625	.5781	.5469	.4844	.5156
.5000	.5156	.5312	.5000	.4688	.5156	.5488	.5000
.5156	.5313	.4844	.4687	.4531	.5000	.4688	.4531
.5312	.4844	.5625	.5469	.4844	.4531	.5625	.5000

**5.2. Bit Independence Criterion.** According to bit independence criterion [9, 10], if any input bit  $i$  is inverted, then the output bits  $j$  and  $k$  must change independently. In other words, the avalanche variables must be pairwise independent for a given set of avalanche vectors. We have tested the nonlinearity of bit independence criterion of S-box (Table 7). We also compared the minimum and average values of bit independence criterion along with square deviation of the proposed S-box with different renowned S-boxes (Table 8).

**5.3. Strict Avalanche Criterion.** Strict avalanche criterion (SAC) introduced by Tavares and Webster is founded on the ideas of the avalanche and completeness effect [9, 10]. It is a formalization of the avalanche effect. If by complementing a single input bit all the output bits are changed with a 0.5 probability, SAC is said to be satisfied. Table 9 displays the outcomes of the strict avalanche criterion.

**5.4. Linear Approximation Probability.** In linear approximation probability method, we examine the imbalance of an event [11]. The analysis is used to calculate the highest value of imbalance of the outcome of the event. The uniformity of the input bits should be similar to that of the output bits. Each  $i$ th input bit is analyzed individually and its outcomes are checked in the output bits. The masks which are applied on the parity of both input and output bits are denoted by  $\chi_x$  and  $\chi_y$ , respectively. Mathematically,

$$LP = \max_{\chi_x, \chi_y \neq 0} \left| \frac{\# \{d/d \cdot \chi_x = S(d) \cdot \chi_y\}}{2^n} - \frac{1}{2} \right|, \quad (6)$$

where  $d$  represents the collection of all possible inputs and  $2^n$  is the total number of elements. The results of this important

TABLE 10: Linear approximation probability analyses of different S-boxes.

S-boxes	AES	Gray	Skipjack	Prime	Proposed	Gautam et al. [14]	S <sub>8</sub> AES	Xyi
Max value	144	144	156	162	162	164	144	168
Max LP	0.062	0.062	0.109	0.132	0.1484	0.2109	0.062	0.156

TABLE 11: Differential probability of the proposed S-box.

.02344	.02344	.02344	.02344	.03125	.02344	.02344	.02344	.02344	.03125	.02344	.02344	.02344	.01562	.02344	.03125
.02344	.02344	.03125	.03125	.03125	.03125	.03125	.02344	.02344	.03125	.02344	.02344	.02344	.02344	.02344	.02344
.01563	.02344	.02344	.03125	.03125	.03125	.02344	.02344	.02344	.02344	.03125	.02344	.02344	.02344	.01562	.02344
.03125	.03906	.02344	.03125	.02344	.02344	.03125	.02344	.03125	.03125	.03125	.02344	.02344	.02344	.02344	.02344
.03125	.04688	.03906	.02344	.02344	.02344	.03125	.02344	.01562	.02344	.03125	.02344	.02344	.02344	.02344	.03125
.03125	.03125	.02344	.03125	.03125	.03125	.03125	.03125	.02344	.02344	.02344	.03125	.02344	.03125	.02344	.02344
.02344	.03125	.03125	.03906	.03125	.02344	.03125	.03906	.02344	.02344	.03125	.02344	.03125	.02344	.03125	.02344
.01563	.03125	.03125	.03125	.03125	.03125	.02344	.02344	.03125	.03125	.02344	.03125	.02344	.03125	.02344	.02344
.03125	.03125	.03906	.02344	.03125	.02344	.02344	.03125	.03125	.03125	.02344	.03125	.02344	.03906	.03125	.03125
.03125	.02344	.03125	.02344	.03125	.03125	.02344	.03125	.02344	.02344	.02344	.03125	.02344	.03125	.02344	.02344
.02344	.03125	.02344	.02344	.02344	.03125	.03125	.02344	.03125	.02344	.02344	.03125	.02344	.02344	.02344	.03125
.02344	.02344	.03125	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.03125	.03125	.02344	.02344	.02344	.02344
.02344	.02344	.02344	.02344	.02344	.02344	.03125	.02344	.02344	.02344	.03125	.02344	.02344	.03125	.03125	.03125
.03125	.02344	.04688	.02344	.02344	.02344	.03906	.03125	.03125	.02344	.02344	.02344	.03125	.03125	.02344	.03125
.02344	.02344	.03906	.03125	.02344	.02344	.02344	.02344	.02344	.03125	.03125	.02344	.03125	.02344	.03906	.03125
.03125	.03125	.02344	.02344	.03125	.03125	.02344	.02344	.02344	.03125	.02344	.02344	.02344	.03125	.02344	—

analysis obtained from our S-box and different established S-boxes are given in Table 10. The comparison shows that our S-box is strong enough to deal with different linear attacks.

**5.5. Differential Approximation Probability.** In this analysis, differential uniformity is determined by examining the mapping from the input bits to the output. The main focus of this test is to ensure differential uniformity; that is, the input differential must be associated with an output differential in a unique way.

It is represented by

$$D_{p^s}(\Delta\mu \longrightarrow \Delta\nu) = \frac{[\#\{\mu \in I/S(\mu) \oplus S(\mu \oplus \Delta\mu) = \Delta\nu\}]}{2^n}, \quad (7)$$

where  $\Delta\mu$  and  $\Delta\nu$  are the input and output differentials, respectively. We have applied differential approximation probability test on our S-box. The results are presented in Table 11.

## 6. Majority Logic Criterion

The majority logic criterion [12] is helpful in finding the premier candidate S-box fit for a certain kind of encryption application. In this criterion, image encryption strength of the

S-box is investigated through statistical studies. A distortion in the image is created by encryption process; therefore, it is important to study the statistical characteristics. It is achieved with the help of various analyses such as entropy, contrast, correlation, energy, and homogeneity. The proposed S-box can further be used for encryption and multimedia security. In this paper, we have used two JPEG images, Pepper and Baboon, for MLC analysis. The results of these analyses in comparison with the other well-known S-boxes are depicted in Table 12. Figure 6 shows the result of image encryption with proposed S-box. The histogram of the original image and the encrypted images of Baboon and Pepper are shown in Figure 7. These results show that our S-box fulfills all the requirements to be declared as a very suitable S-box for encryption applications. Thus, it is recommended to become a part of algorithms designed for the secure transmission of information/data.

## 7. Conclusion

In the present study, a strong S-box is created with the help of coset graph for the action of modular group and a bijective map. According to our information, this is the first use of coset graphs in the construction of S-box. The proposed S-box is highly secure and the results obtained from different analyses are nearly equal to the ideal ones. Therefore, it is very useful for secure communication.

TABLE 12: Comparison of MLC for proposed S-box over different S-boxes.

S-boxes	Entropy	Contrast	Correlation	Energy	Homogeneity
Pepper image					
Plaintext	7.5909	0.2760	0.9383	0.1288	0.9024
Proposed	7.9532	8.5155	0.0079	0.0174	0.4100
AES	7.9211	7.5509	0.0554	0.0202	0.4662
Ullah et al. [24]	7.9823	8.6727	-0.0043	0.0173	0.4076
Skipjack	7.7561	7.7058	0.1205	0.0239	0.4708
Khan et al. [25]	7.9562	8.3129	0.0103	0.0180	0.4219
Belazi	7.9233	8.1423	-0.0112	0.0286	0.4648
Baboon image					
Plaintext	7.1273	0.7179	0.6782	0.1025	0.7669
Proposed	7.9551	8.5267	$4.4609e - 004$	0.0174	.4088
AES	7.2531	7.5509	0.0554	0.0202	0.4662
Prime	6.9311	7.6236	0.0855	0.0202	0.4640
Xyi	7.2531	8.3108	0.0417	0.0196	0.4533
Skipjack	7.2531	7.7058	0.1025	0.0193	0.4689
Khan et al. [25]	7.9612	8.1213	-0.0512	0.0210	0.4011
Belazi	7.9252	8.0391	0.0119 0	.02219	0.4428

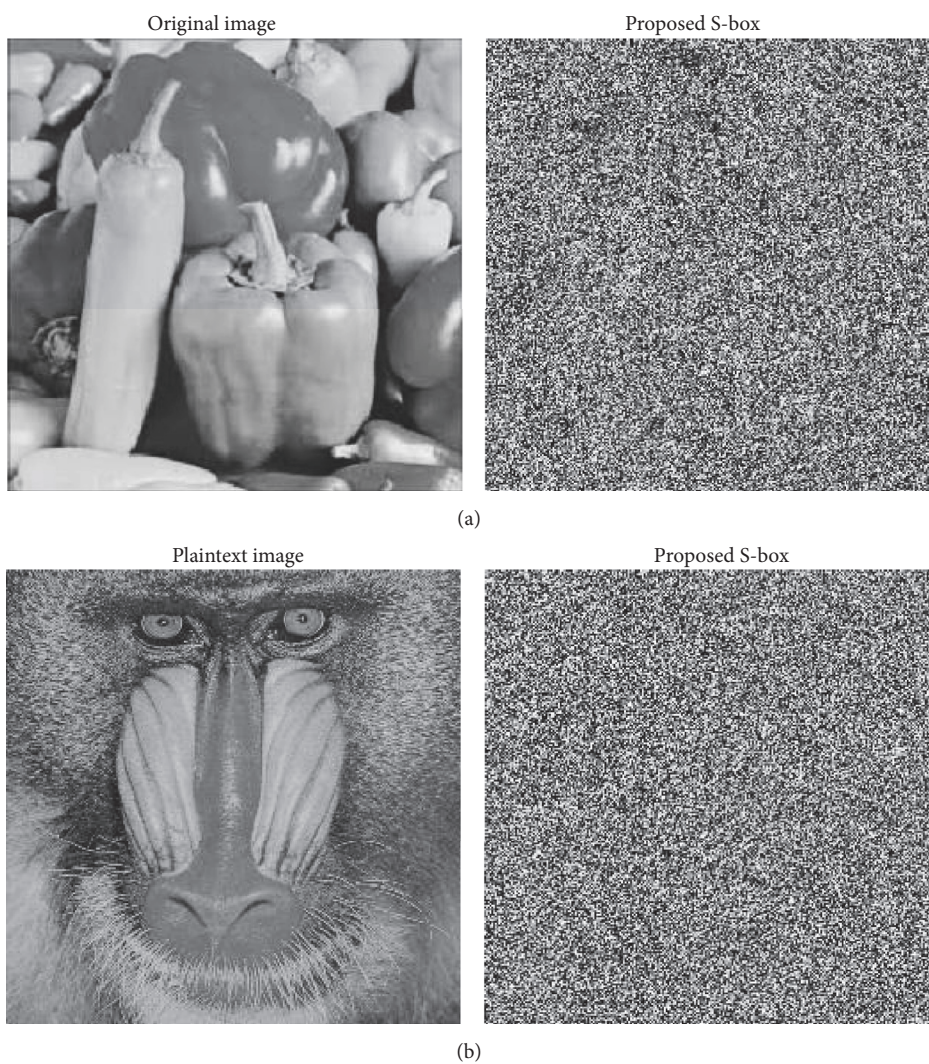


FIGURE 6: Original image and the encrypted images using two rounds of encryption: (a) Pepper and (b) Baboon.

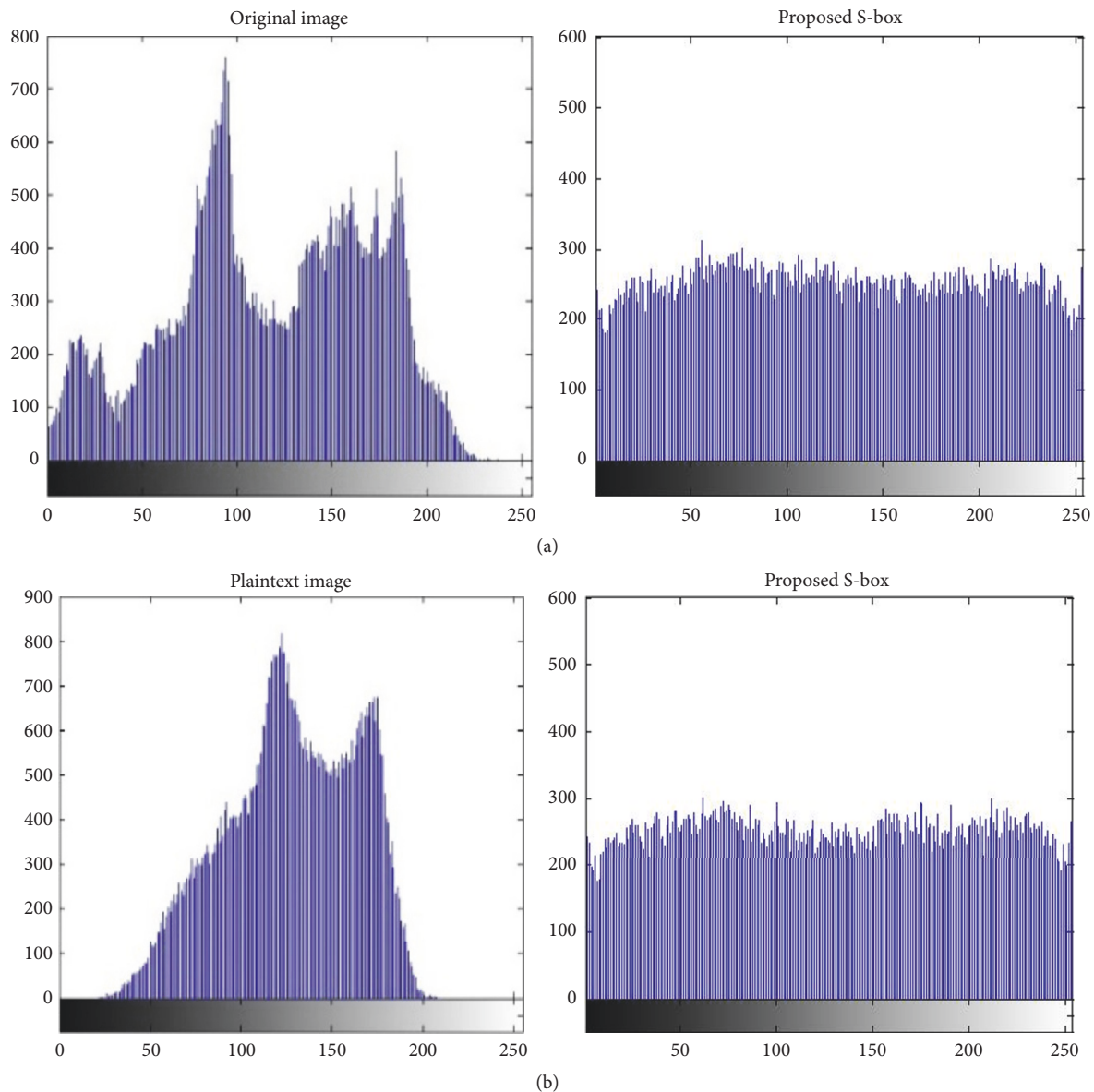


FIGURE 7: Histogram of the original image and the encrypted images: (a) Pepper and (b) Baboon.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## References

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, pp. 656–715, 1949.
- [2] J. Daemen and V. Rijmen, *The Design of Rijndael-AES: The Advanced Encryption Standard*, Springer, Berlin, Germany, 2002.
- [3] P. J. Cameron, "encyclopaedia of design theory," in *Cayley Graphs and Coset Diagrams*, pp. 1–9, 2013.
- [4] B. Everitt, "Alternating quotients of the  $(3,q,r)$  triangle groups," *Communications in Algebra*, vol. 25, no. 6, pp. 1817–1832, 1997.
- [5] R. C. Lyndon and E. Paul, *Combinatorial group theory*, vol. 89, Springer, 2015.
- [6] Q. Mushtaq and H. Servatius, "Permutation representation of the symmetry groups of regular hyperbolic tessellations," *Journal of the London Mathematical Society*, vol. 2, no. 48, pp. 77–86, 1993.
- [7] A. Torstensson, "Coset diagrams in the study of finitely presented groups with an application to quotients of the modular group," *Journal of Commutative Algebra*, vol. 2, no. 4, pp. 501–514, 2010.
- [8] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," *IEE Proceedings Part E Computers and Digital Techniques*, vol. 135, no. 6, pp. 325–335, 1988.
- [9] I. Vergili and M. D. Yücel, "Avalanche and bit independence properties for the ensembles of randomly chosen  $n \times n$  s-boxes," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 9, no. 2, pp. 137–145, 2001.

- [10] A. F. Webster and S. E. Tavares, "On the design of s-boxes, advances in cryptology," in *Proceedings of CRYPTO'85*, Springer, Berlin, Germany, 1986.
- [11] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.
- [12] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "Generalized Majority Logic Criterion to Analyze the Statistical Strength of S-Boxes," *Zeitschrift für Naturforschung A*, vol. 67, no. 5, pp. 282–288, 2012.
- [13] M. T. Tran, D. K. Bui, and A. D. Doung, "Gray S-box for advanced encryption standard," in *Proceedings of the International Conference on Computer Intel Security*, vol. 1, pp. 253–258, 2008.
- [14] A. Gautam, G. S. Gaba, R. Miglani, and R. Pasricha, "Application of Chaotic Functions for Construction of Strong Substitution Boxes," *Indian Journal of Science and Technology*, vol. 8, no. 28, pp. 1–5, 2015.
- [15] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal, and U. Y. Bhatti, "Some analysis of S-box based on residue of prime number," *Proceedings of the Pakistan Academy of Sciences*, vol. 48, no. 2, pp. 111–115, 2011.
- [16] I. Hussain, T. Shah, and H. Mahmood, "A new algorithm to construct secure keys for AES," *International Journal of Contemporary Mathematical Sciences*, vol. 5, no. 25–28, pp. 1263–1270, 2010.
- [17] X. Y. Shi, Hu. Xiao, X. C. You, and K. Y. Lam, "A method for obtaining cryptographically strong 8\*8 S-boxes," in *Proceedings of the International Conference on Advanced Information Networking and Applications*, vol. 2, pp. 14–20, 2002.
- [18] Skipjack and Kea, "Algorithm Specifications Version 2," <http://csrc.nist.gov/CryptoToolkit/>.
- [19] A. H. Alkhalidi, I. Hussain, and M. A. Gondal, "A novel design for the construction of safe S-boxes based on TDERC sequence," *Alexandria Engineering Journal*, vol. 54, pp. 65–69, 2015.
- [20] G. Chen, Y. Chen, and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps," *Chaos, Solitons & Fractals*, vol. 31, no. 3, pp. 571–579, 2007.
- [21] G. Tang, X. Liao, and Y. Chen, "A novel method for designing S-boxes based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 23, no. 2, pp. 413–419, 2005.
- [22] M. Khan, T. Shah, and M. A. Gondal, "An efficient technique for the construction of substitution box with chaotic partial differential equation," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 1795–1801, 2013.
- [23] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 337–361, 2017.
- [24] A. Ullah, S. S. Jamal, and T. Shah, "A novel construction of substitution box using a combination of chaotic maps with improved chaotic range," in *Nonlinear Dynamics*, vol. 88, pp. 2757–2769, Dynamics, 2017.
- [25] M. Khan, T. Shah, and S. I. Batool, "Construction of S-box based on chaotic Boolean functions and its application in image encryption," *Neural Computing and Applications*, vol. 27, no. 3, pp. 677–685, 2016.





**Hindawi**

Submit your manuscripts at  
<https://www.hindawi.com>

