# 胡泓震的活跃S盒结果

S0:  
  
70 2c b3 c0 e4 57 ea ae 23 6b 45 a5 ed 4f 1d 92  
86 af 7c 1f 3e dc 5e b a6 39 d5 5d d9 5a 51 6c  
8b 9a fb b0 74 2b f0 84 df cb 34 76 6d a9 d1 4  
14 3a de 11 32 9c 53 f2 fe cf c3 7a 24 e8 60 69  
aa a0 a1 62 54 1e e0 64 10 0 a3 75 8a e6 9 dd  
87 83 cd 90 73 f6 9d bf 52 d8 c8 c6 81 6f 13 63  
e9 a7 9f bc 29 f9 2f b4 78 6 e7 71 d4 ab 88 8d  
72 b9 f8 ac 36 2a 3c f1 40 d3 bb 43 15 ad 77 80  
82 ec 27 e5 85 35 c 41 ef 93 19 21 e 4e 65 bd  
b8 8f eb ce 30 5f c5 1a e1 ca 47 3d 1 d6 56 4d  
d 66 cc 2d 12 20 b1 99 4c c2 7e 5 b7 31 17 d7  
58 61 1b 1c f 16 18 22 44 b2 b5 91 8 a8 fc 50  
d0 7d 89 97 5b 95 ff d2 c4 48 f7 db 3 da 3f 94  
5c 2 4a 33 67 f3 7f e2 9b 26 37 3b 96 4b be 2e  
79 8c 6e 8e f5 b6 fd 59 98 6a 46 ba 25 42 a2 fa  
7 55 ee a 49 68 38 a4 28 7b c9 c1 e3 f4 c7 9e

S1:  
  
70 2c b3 c0 e4 57 ea ae 23 6b 45 a5 ed 4f 1d 92  
86 af 7c 1f 3e dc 5e b a6 39 d5 5d d9 5a 51 6c  
8b 9a fb b0 74 2b f0 84 df cb 34 76 6d a9 d1 4  
14 3a de 11 32 9c 53 f2 fe cf c3 7a 24 e8 60 69  
aa a0 a1 62 54 1e e0 64 10 0 a3 75 8a e6 9 dd  
87 83 cd 90 73 f6 9d bf 52 d8 c8 c6 81 6f 13 63  
e9 a7 9f bc 29 f9 2f b4 78 6 e7 71 d4 ab 88 8d  
72 b9 f8 ac 36 2a 3c f1 40 d3 bb 43 15 ad 77 80  
82 ec 27 e5 85 35 c 41 ef 93 19 21 e 4e 65 bd  
b8 8f eb ce 30 5f c5 1a e1 ca 47 3d 1 d6 56 4d  
d 66 cc 2d 12 20 b1 99 4c c2 7e 5 b7 31 17 d7  
58 61 1b 1c f 16 18 22 44 b2 b5 91 8 a8 fc 50  
d0 7d 89 97 5b 95 ff d2 c4 48 f7 db 3 da 3f 94  
5c 2 4a 33 67 f3 7f e2 9b 26 37 3b 96 4b be 2e  
79 8c 6e 8e f5 b6 fd 59 98 6a 46 ba 25 42 a2 fa  
7 55 ee a 49 68 38 a4 28 7b c9 c1 e3 f4 c7 9e

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 选用的S盒 | 列位移参数 | Lane位移参数 | Mds | r | 活跃S盒个数（合格线：171） |
| S1 | (2, 0, 1, 3) | 0 5 6 7 6 2 0 0 1 7 4 6 4 3 3 2 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 4 | 25 |
| 10 | 85 |
| 13 | 111 |
| 14 | 120 |
| 15 | 133 |
| 20 | 171 |
| S1 | (2, 0, 1, 3) | 1 1 1 1 2 2 2 2 3 3 3 3 4 4 4 4 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| S1 | (2, 0, 1, 3) | 5 1 3 5 7 3 7 0 2 4 4 2 4 5 1 1 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| S1 | (2, 0, 1, 3) | 1 2 1 6 2 1 4 0 6 0 6 1 5 5 3 4 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| S1 | (2, 0, 1, 3) | 0 2 3 7 4 0 5 6 5 5 2 3 3 7 1 2 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| S1 | (2, 0, 1, 3) | 7 6 3 2 3 1 6 7 2 0 1 5 1 2 4 3 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| S1 | (2, 0, 1, 3) | 5 7 5 5 7 6 7 1 3 4 6 6 6 5 0 7 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| S1 | (2, 0, 1, 3) | 3 4 2 6 0 3 1 0 6 2 5 7 1 6 7 1 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| S1 | (2, 0, 1, 3) | 4 5 6 7 1 6 4 6 7 3 7 1 5 0 5 4 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| S1 | (2, 0, 1, 3) | 5 5 7 1 4 7 0 6 1 0 6 0 2 3 4 3 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| S1 | (2, 0, 1, 3) | 2 2 3 6 1 1 0 7 7 6 2 4 5 7 6 2 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| 15 | 128 |
| 16 | 140 |
| S1 | (2, 0, 1, 3) | 1 0 2 0 7 2 3 2 6 1 1 7 3 5 0 3 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| S1 | (2, 0, 1, 3) | 2 7 2 3 0 4 3 6 4 3 1 4 1 1 5 0 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| 15 | 128 |
| 16 | 140 |
| 1 | 1 |
| 2 | 5 |
| 3 | 9 |
| 4 | 25 |
| 5 | 41 |
| 6 | 50 |
| 7 | 57 |
| 8 | 65 |
| 9 | 69 |
| 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 17 | 146 |
| 18 | 155 |
| 19 | 163 |
| S1 | (2, 0, 1, 3) | 0 1 0 2 6 6 5 3 1 4 6 5 4 7 1 7 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| 12 | 90 |
| 13 | 97 |
| 14 | 105 |
| 15 | 112 |
| 16 | 120 |
| S1 | (2, 0, 1, 3) | 1 7 1 6 7 3 6 2 2 6 2 3 4 0 7 5 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| 12 | 90 |
| 13 | 97 |
| 14 | 105 |
| 15 | 112 |
| 16 | 120 |
| S1 | (2, 0, 1, 3) | 0 4 1 5 4 3 2 6 5 2 6 4 7 0 0 0 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| 15 | 128 |
| S1 | (2, 0, 1, 3) | 5 1 1 6 1 0 4 3 0 5 6 1 3 6 2 4 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| 12 | 90 |
| 13 | 97 |
| 14 | 105 |
| 15 | 112 |
| S1 | (2, 0, 1, 3) | 7 5 7 6 2 0 3 7 1 2 4 2 5 7 6 0 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 75 |
| 11 | 82 |
| 12 | 90 |
| 13 | 97 |
| 14 | 105 |
| 15 | 112 |
| S1 | (2, 0, 1, 3) | 5 3 5 1 3 7 0 3 0 6 3 4 4 1 7 5 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| 15 | 128 |
| S1 | (2, 0, 1, 3) | 6 3 2 4 0 2 1 0 3 0 3 7 7 7 7 1 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| 15 | 128 |
| S1 | (2, 0, 1, 3) | 7 7 1 0 0 4 7 7 3 2 6 4 5 3 3 6 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| S1 | (2, 0, 1, 3) | 2 3 4 1 0 2 3 4 5 4 2 6 1 7 0 2 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| S1 | (2, 0, 1, 3) | 4 3 2 0 0 7 6 5 6 5 0 6 1 0 7 4 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| S1 | (2, 0, 1, 3) | 7 6 4 0 2 3 7 1 4 5 0 7 6 1 6 4 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| S1 | (2, 0, 1, 3) | 6 4 5 6 5 0 0 5 0 3 7 4 2 6 4 0 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| S1 | (2, 0, 1, 3) | 3 5 6 6 2 3 4 1 1 1 0 0 7 4 7 2 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| S1 | (2, 0, 1, 3) | 1 6 5 1 5 5 1 6 2 7 2 0 7 2 7 4 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |
| S1 | (2, 0, 1, 3) | 4 4 2 7 5 3 1 6 3 2 6 1 0 6 7 3 | 1 1 140 141 1 140 141 1 140 141 1 1 141 1 1 140 | 10 | 85 |
| 11 | 93 |
| 12 | 105 |
| 13 | 111 |
| 14 | 120 |