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

S2= 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

S3 = 38 41 16 76 d9 93 60 f2 72 c2 ab 9a 75 6 57 a0

91 f7 b5 c9 a2 8c d2 90 f6 7 a7 27 8e b2 49 de

43 5c d7 c7 3e f5 8f 67 1f 18 6e af 2f e2 85 d

53 f0 9c 65 ea a3 ae 9e ec 80 2d 6b a8 2b 36 a6

c5 86 4d 33 fd 66 58 96 3a 9 95 10 78 d8 42 cc

ef 26 e5 61 1a 3f 3b 82 b6 db d4 98 e8 8b 2 eb

a 2c 1d b0 6f 8d 88 e 19 87 4e b a9 c 79 11

7f 22 e7 59 e1 da 3d c8 12 4 74 54 30 7e b4 28

55 68 50 be d0 c4 31 cb 2a ad f ca 70 ff 32 69

8 62 0 24 d1 fb ba ed 45 81 73 6d 84 9f ee 4a

c3 2e c1 1 e6 25 48 99 b9 b3 7b f9 ce bf df 71

29 cd 6c 13 64 9b 63 9d c0 4b b7 a5 89 5f b1 17

f4 bc d3 46 cf 37 5e 47 94 fa fc 5b 97 fe 5a ac

3c 4c 3 35 f3 23 b8 5d 6a 92 d5 21 44 51 c6 7d

39 83 dc aa 7c 77 56 5 1b a4 15 34 1e 1c f8 52

20 14 e9 bd dd e4 a1 e0 8a f1 d6 7a bb e3 40 4f

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |
| 16 |  |
| 20 | 估计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 |
| S2 | 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 | 1 0 2 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 | 1 1 1 1  2 2 2 2  3 3 3 3  4 4 4 4 | 1 4 141 1  4 141 1 1  141 1 1 4  1 1 4 141 | 10 | 75 |
| S1 | 2 0 1 3 | 0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0 | 1 1 140 141  1 140 141 1  140 141 1 1  141 1 1 140 | 10 | 25 |
| S1 | 2 0 1 3 | 3 3 3 3  3 3 3 3  3 3 3 3  3 3 3 3 | 1 1 140 141  1 140 141 1  140 141 1 1  141 1 1 140 | 10 | 25 |
| S1 | 2 0 1 3 | 0 1 2 3  3 1 0 2  1 0 3 2  1 2 0 3 | 1 1 140 141  1 140 141 1  140 141 1 1  141 1 1 140 | 10 | 50 |
| S1 | 2 0 1 3 | 7 2 5 1  4 0 1 7  6 4 2 5  3 6 3 3 | 1 1 140 141  1 140 141 1  140 141 1 1  141 1 1 140 | 10 | 55 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |