JACOB S. SANTOS **12/02/24**

BSCOE 4-1 **Dr. Ariel Sison**

Sha-3

Input Message: [83, 109, 97, 114, 116, 87, 97, 116, 99, 104]

Padded Message:
536D617274576174636806000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000
0000000080

Absorbing Block 1:

State BEFORE absorbing block:

0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000

State AFTER absorbing block:

7461577472616D53 0000000000066863 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 8000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000

Round 0:

State BEFORE round transformations:

7461577472616D53 0000000000066863 0000000000000000 0000000000000000
0000000000000000

0000000000000000 0000000000000000 0000000000000000 8000000000000000
0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000
0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000
0000000000000000

0000000000000000 0000000000000000 0000000000000000 0000000000000000
0000000000000000

Computing C[x] (Column parity):

C[0] = state[0][0] XOR state[0][1] XOR state[0][2] XOR state[0][3] XOR state[0][4] =
7461577472616D53

C[1] = state[1][0] XOR state[1][1] XOR state[1][2] XOR state[1][3] XOR state[1][4] =
0000000000066863

C[2] = state[2][0] XOR state[2][1] XOR state[2][2] XOR state[2][3] XOR state[2][4] =
0000000000000000

C[3] = state[3][0] XOR state[3][1] XOR state[3][2] XOR state[3][3] XOR state[3][4] =
8000000000000000

C[4] = state[4][0] XOR state[4][1] XOR state[4][2] XOR state[4][3] XOR state[4][4] =
0000000000000000

Computing D[x]:

D[0] = C[4] XOR ROTL(C[1], 1) = 0000000000000000 XOR 00000000000CD0C6 =
00000000000CD0C6

D[1] = C[0] XOR ROTL(C[2], 1) = 7461577472616D53 XOR 0000000000000000 =
7461577472616D53

D[2] = C[1] XOR ROTL(C[3], 1) = 0000000000066863 XOR 0000000000000001 =
0000000000066862

D[3] = C[2] XOR ROTL(C[4], 1) = 0000000000000000 XOR 0000000000000000 =
0000000000000000

D[4] = C[3] XOR ROTL(C[0], 1) = 8000000000000000 XOR E8C2AEE8E4C2DAA6 =
68C2AEE8E4C2DAA6

Updating State with θ (Theta) transformation:

state[0][0] XOR = D[0]: 7461577472616D53 -> 74615774726DBD95

state[0][1] XOR = D[0]: 0000000000000000 -> 00000000000CD0C6

state[0][2] XOR = D[0]: 0000000000000000 -> 00000000000CD0C6

state[0][3] XOR = D[0]: 0000000000000000 -> 00000000000CD0C6

state[0][4] XOR = D[0]: 0000000000000000 -> 00000000000CD0C6

state[1][0] XOR = D[1]: 0000000000066863 -> 7461577472670530

state[1][1] XOR = D[1]: 0000000000000000 -> 7461577472616D53

state[1][2] XOR = D[1]: 0000000000000000 -> 7461577472616D53

state[1][3] XOR = D[1]: 0000000000000000 -> 7461577472616D53

state[1][4] XOR = D[1]: 0000000000000000 -> 7461577472616D53

state[2][0] XOR = D[2]: 0000000000000000 -> 0000000000066862

state[2][1] XOR = D[2]: 0000000000000000 -> 0000000000066862

state[2][2] XOR = D[2]: 0000000000000000 -> 0000000000066862

state[2][3] XOR = D[2]: 0000000000000000 -> 0000000000066862

state[2][4] XOR = D[2]: 0000000000000000 -> 0000000000066862

state[3][0] XOR = D[3]: 0000000000000000 -> 0000000000000000

state[3][1] XOR = D[3]: 8000000000000000 -> 8000000000000000

state[3][2] XOR = D[3]: 0000000000000000 -> 0000000000000000

state[3][3] XOR = D[3]: 0000000000000000 -> 0000000000000000

state[3][4] XOR = D[3]: 0000000000000000 -> 0000000000000000

state[4][0] XOR = D[4]: 0000000000000000 -> 68C2AEE8E4C2DAA6

state[4][1] XOR = D[4]: 0000000000000000 -> 68C2AEE8E4C2DAA6

state[4][2] XOR = D[4]: 0000000000000000 -> 68C2AEE8E4C2DAA6

state[4][3] XOR = D[4]: 0000000000000000 -> 68C2AEE8E4C2DAA6

state[4][4] XOR = D[4]: 0000000000000000 -> 68C2AEE8E4C2DAA6

State AFTER θ (Theta):

74615774726DBD95 7461577472670530 0000000000066862 0000000000000000
68C2AEE8E4C2DAA6

00000000000CD0C6 7461577472616D53 0000000000066862 8000000000000000
68C2AEE8E4C2DAA6

00000000000CD0C6 7461577472616D53 0000000000066862 0000000000000000
68C2AEE8E4C2DAA6

00000000000CD0C6 7461577472616D53 0000000000066862 0000000000000000
68C2AEE8E4C2DAA6

00000000000CD0C6 7461577472616D53 0000000000066862 0000000000000000
68C2AEE8E4C2DAA6

ρ (Rho) Transformation

Each lane is rotated by a specific offset based on its (x, y) position:

Lane (0, 0): Original = 74615774726DBD95, Offset = 0, Rotated =
74615774726DBD95

Lane (0, 1): Original = 00000000000CD0C6, Offset = 36, Rotated =
00CD0C6000000000

Lane (0, 2): Original = 00000000000CD0C6, Offset = 3, Rotated =
0000000000668630

Lane (0, 3): Original = 00000000000CD0C6, Offset = 41, Rotated =
19A18C0000000000

Lane (0, 4): Original = 00000000000CD0C6, Offset = 18, Rotated =
0000003343180000

Lane (1, 0): Original = 7461577472670530, Offset = 1, Rotated =
E8C2AEE8E4CE0A60

Lane (1, 1): Original = 7461577472616D53, Offset = 44, Rotated =
16D5374615774726

Lane (1, 2): Original = 7461577472616D53, Offset = 10, Rotated =
855DD1C985B54DD1

Lane (1, 3): Original = 7461577472616D53, Offset = 45, Rotated =
2DAA6E8C2AEE8E4C

Lane (1, 4): Original = 7461577472616D53, Offset = 2, Rotated =
D1855DD1C985B54D

Lane (2, 0): Original = 0000000000066862, Offset = 62, Rotated = 8000000000019A18

Lane (2, 1): Original = 0000000000066862, Offset = 6, Rotated = 00000000019A1880

Lane (2, 2): Original = 0000000000066862, Offset = 43, Rotated = 3343100000000000

Lane (2, 3): Original = 0000000000066862, Offset = 15, Rotated = 0000000334310000

Lane (2, 4): Original = 0000000000066862, Offset = 61, Rotated = 400000000000CD0C

Lane (3, 0): Original = 0000000000000000, Offset = 28, Rotated = 0000000000000000

Lane (3, 1): Original = 8000000000000000, Offset = 55, Rotated = 0040000000000000

Lane (3, 2): Original = 0000000000000000, Offset = 25, Rotated = 0000000000000000

Lane (3, 3): Original = 0000000000000000, Offset = 21, Rotated = 0000000000000000

Lane (3, 4): Original = 0000000000000000, Offset = 56, Rotated = 0000000000000000

Lane (4, 0): Original = 68C2AEE8E4C2DAA6, Offset = 27, Rotated = 472616D533461577

Lane (4, 1): Original = 68C2AEE8E4C2DAA6, Offset = 20, Rotated = EE8E4C2DAA668C2A

Lane (4, 2): Original = 68C2AEE8E4C2DAA6, Offset = 39, Rotated = 616D533461577472

Lane (4, 3): Original = 68C2AEE8E4C2DAA6, Offset = 8, Rotated = C2AEE8E4C2DAA668

Lane (4, 4): Original = 68C2AEE8E4C2DAA6, Offset = 14, Rotated = ABBA3930B6A99A30

State AFTER ρ (Rho):

74615774726DBD95 E8C2AEE8E4CE0A60 8000000000019A18 0000000000000000 472616D533461577

00CD0C6000000000 16D5374615774726 00000000019A1880 0040000000000000 EE8E4C2DAA668C2A

0000000000668630 855DD1C985B54DD1 3343100000000000 0000000000000000 616D533461577472

19A18C0000000000 2DAA6E8C2AEE8E4C 0000000334310000 0000000000000000 C2AEE8E4C2DAA668

0000003343180000 D1855DD1C985B54D 400000000000CD0C 0000000000000000 ABBA3930B6A99A30

Applying π (Pi) transformation:

Moving lane (0, 0) -> (0, 0)

Moving lane (0, 1) -> (1, 3)

Moving lane (0, 2) -> (2, 1)

Moving lane (0, 3) -> (3, 4)

Moving lane (0, 4) -> (4, 2)

Moving lane (1, 0) -> (0, 2)

Moving lane (1, 1) -> (1, 0)

Moving lane (1, 2) -> (2, 3)

Moving lane (1, 3) -> (3, 1)

Moving lane (1, 4) -> (4, 4)

Moving lane (2, 0) -> (0, 4)

Moving lane (2, 1) -> (1, 2)

Moving lane (2, 2) -> (2, 0)

Moving lane (2, 3) -> (3, 3)

Moving lane (2, 4) -> (4, 1)

Moving lane (3, 0) -> (0, 1)

Moving lane (3, 1) -> (1, 4)

Moving lane (3, 2) -> (2, 2)

Moving lane (3, 3) -> (3, 0)

Moving lane (3, 4) -> (4, 3)

Moving lane (4, 0) -> (0, 3)

Moving lane (4, 1) -> (1, 1)

Moving lane (4, 2) -> (2, 4)

Moving lane (4, 3) -> (3, 2)

Moving lane (4, 4) -> (4, 0)

State AFTER π (Pi):

74615774726DBD95 16D5374615774726 3343100000000000 0000000000000000 ABBA3930B6A99A30

0000000000000000 EE8E4C2DAA668C2A 0000000000668630 2DAA6E8C2AEE8E4C 400000000000CD0C

E8C2AEE8E4CE0A60 00000000019A1880 0000000000000000 C2AEE8E4C2DAA668 0000003343180000

472616D533461577 00CD0C6000000000 855DD1C985B54DD1 0000000334310000 0000000000000000

8000000000019A18 0040000000000000 616D533461577472 19A18C0000000000 D1855DD1C985B54D

Applying χ (Chi) transformation:

Lane (0, 0): 74615774726DBD95 -> 55635774726DBD95

Lane (0, 1): 0000000000000000 -> 0000000000000210

Lane (0, 2): E8C2AEE8E4CE0A60 -> E8C2AEE8E4CE0A60

Lane (0, 3): 472616D533461577 -> C236C75CB6F358A6

Lane (0, 4): 8000000000019A18 -> E12D53346156EE6A

Lane (1, 0): 16D5374615774726 -> 16D5374615774726

Lane (1, 1): EE8E4C2DAA668C2A -> C32422A180EE8466

Lane (1, 2): 00000000019A1880 -> C2AEE8E4C340BEE8

Lane (1, 3): 00CD0C6000000000 -> 00CD0C6230000000

Lane (1, 4): 0040000000000000 -> 18C08C0000000000

Lane (2, 0): 3343100000000000 -> 98F92930B6A99A30

Lane (2, 1): 0000000000668630 -> 400000000066C730

Lane (2, 2): 0000000000000000 -> 0000001301000000

Lane (2, 3): 855DD1C985B54DD1 -> 855DD1C985B54DD1

Lane (2, 4): 616D533461577472 -> A16902E5A8D2C13F

Lane (3, 0): 0000000000000000 -> 5441464440442585

Lane (3, 1): 2DAA6E8C2AEE8E4C -> 2DAA6E8C2AEE8E4C

Lane (3, 2): C2AEE8E4C2DAA668 -> 2A6C462C661CAC08

Lane (3, 3): 0000000334310000 -> 472616D607771577

Lane (3, 4): 19A18C0000000000 -> 19A18C0000000A10

Lane (4, 0): ABBA3930B6A99A30 -> A92E1932B3BBD812

Lane (4, 1): 400000000000CD0C -> AE8E4C2DAA664126

Lane (4, 2): 0000003343180000 -> 0000003342081080

Lane (4, 3): 0000000000000000 -> 00C9082000000000

Lane (4, 4): D1855DD1C985B54D -> D1C55DD1C985B54D

State AFTER χ (Chi):

55635774726DBD95 16D5374615774726 98F92930B6A99A30 5441464440442585 A92E1932B3BBD812

0000000000000210 C32422A180EE8466 400000000066C730 2DAA6E8C2AEE8E4C AE8E4C2DAA664126

E8C2AEE8E4CE0A60 C2AEE8E4C340BEE8 0000001301000000 2A6C462C661CAC08 0000003342081080

C236C75CB6F358A6 00CD0C6230000000 855DD1C985B54DD1 472616D607771577 00C9082000000000

E12D53346156EE6A 18C08C0000000000 A16902E5A8D2C13F 19A18C0000000A10 D1C55DD1C985B54D

Applying ι (Iota) transformation:

Lane (0, 0): 55635774726DBD95 -> 55635774726DBD94 (XOR with RC[0] = 0000000000000001)

State AFTER ι (Iota):

55635774726DBD94 16D5374615774726 98F92930B6A99A30 5441464440442585 A92E1932B3BBD812

0000000000000210 C32422A180EE8466 400000000066C730 2DAA6E8C2AEE8E4C AE8E4C2DAA664126

E8C2AEE8E4CE0A60 C2AEE8E4C340BEE8 0000001301000000 2A6C462C661CAC08 0000003342081080

C236C75CB6F358A6 00CD0C6230000000 855DD1C985B54DD1 472616D607771577 00C9082000000000

E12D53346156EE6A 18C08C0000000000 A16902E5A8D2C13F 19A18C0000000A10 D1C55DD1C985B54D

State AFTER Round 0:

55635774726DBD94 16D5374615774726 98F92930B6A99A30 5441464440442585 A92E1932B3BBD812

0000000000000210 C32422A180EE8466 400000000066C730 2DAA6E8C2AEE8E4C AE8E4C2DAA664126

E8C2AEE8E4CE0A60 C2AEE8E4C340BEE8 0000001301000000 2A6C462C661CAC08 0000003342081080

C236C75CB6F358A6 00CD0C6230000000 855DD1C985B54DD1 472616D607771577 00C9082000000000

E12D53346156EE6A 18C08C0000000000 A16902E5A8D2C13F 19A18C0000000A10 D1C55DD1C985B54D

Round 1:

State BEFORE round transformations:

55635774726DBD94 16D5374615774726 98F92930B6A99A30 5441464440442585 A92E1932B3BBD812

0000000000000210 C32422A180EE8466 400000000066C730 2DAA6E8C2AEE8E4C AE8E4C2DAA664126

E8C2AEE8E4CE0A60 C2AEE8E4C340BEE8 0000001301000000 2A6C462C661CAC08 0000003342081080

C236C75CB6F358A6 00CD0C6230000000 855DD1C985B54DD1 472616D607771577 00C9082000000000

E12D53346156EE6A 18C08C0000000000 A16902E5A8D2C13F 19A18C0000000A10 D1C55DD1C985B54D

Computing C[x] (Column parity):

C[0] = state[0][0] XOR state[0][1] XOR state[0][2] XOR state[0][3] XOR state[0][4] = 9EBA6DF441060328

C[1] = state[1][0] XOR state[1][1] XOR state[1][2] XOR state[1][3] XOR state[1][4] = 0F527D6166D97DA8

C[2] = state[2][0] XOR state[2][1] XOR state[2][2] XOR state[2][3] XOR state[2][4] = FCCDFA0F9AA8D1EE

C[3] = state[3][0] XOR state[3][1] XOR state[3][2] XOR state[3][3] XOR state[3][4] = 0D00F4320BC118A6

C[4] = state[4][0] XOR state[4][1] XOR state[4][2] XOR state[4][3] XOR state[4][4] = D6AC00DD92503CF9

Computing D[x]:

D[0] = C[4] XOR ROTL(C[1], 1) = D6AC00DD92503CF9 XOR 1EA4FAC2CDB2FB50 = C808FA1F5FE2C7A9

D[1] = C[0] XOR ROTL(C[2], 1) = 9EBA6DF441060328 XOR F99BF41F3551A3DD = 672199EB7457A0F5

D[2] = C[1] XOR ROTL(C[3], 1) = 0F527D6166D97DA8 XOR 1A01E8641782314C = 15539505715B4CE4

D[3] = C[2] XOR ROTL(C[4], 1) = FCCDFA0F9AA8D1EE XOR AD5801BB24A079F3 = 5195FBB4BE08A81D

D[4] = C[3] XOR ROTL(C[0], 1) = 0D00F4320BC118A6 XOR 3D74DBE8820C0651 = 30742FDA89CD1EF7

Updating State with θ (Theta) transformation:

state[0][0] XOR = D[0]: 55635774726DBD94 -> 9D6BAD6B2D8F7A3D

state[0][1] XOR = D[0]: 0000000000000210 -> C808FA1F5FE2C5B9

state[0][2] XOR = D[0]: E8C2AEE8E4CE0A60 -> 20CA54F7BB2CCDC9

state[0][3] XOR = D[0]: C236C75CB6F358A6 -> 0A3E3D43E9119F0F

state[0][4] XOR = D[0]: E12D53346156EE6A -> 2925A92B3EB429C3

state[1][0] XOR = D[1]: 16D5374615774726 -> 71F4AEAD6120E7D3

state[1][1] XOR = D[1]: C32422A180EE8466 -> A405BB4AF4B92493

state[1][2] XOR = D[1]: C2AEE8E4C340BEE8 -> A58F710FB7171E1D

state[1][3] XOR = D[1]: 00CD0C6230000000 -> 67EC95894457A0F5

state[1][4] XOR = D[1]: 18C08C0000000000 -> 7FE115EB7457A0F5

state[2][0] XOR = D[2]: 98F92930B6A99A30 -> 8DAABC35C7F2D6D4

state[2][1] XOR = D[2]: 400000000066C730 -> 55539505713D8BD4

state[2][2] XOR = D[2]: 0000001301000000 -> 15539516705B4CE4

state[2][3] XOR = D[2]: 855DD1C985B54DD1 -> 900E44CCF4EE0135

state[2][4] XOR = D[2]: A16902E5A8D2C13F -> B43A97E0D9898DDB

state[3][0] XOR = D[3]: 5441464440442585 -> 05D4BDF0FE4C8D98

state[3][1] XOR = D[3]: 2DAA6E8C2AEE8E4C -> 7C3F953894E62651

state[3][2] XOR = D[3]: 2A6C462C661CAC08 -> 7BF9BD98D8140415

state[3][3] XOR = D[3]: 472616D607771577 -> 16B3ED62B97FBD6A

state[3][4] XOR = D[3]: 19A18C0000000A10 -> 483477B4BE08A20D

state[4][0] XOR = D[4]: A92E1932B3BBD812 -> 995A36E83A76C6E5

state[4][1] XOR = D[4]: AE8E4C2DAA664126 -> 9EFA63F723AB5FD1

state[4][2] XOR = D[4]: 0000003342081080 -> 30742FE9CBC50E77

state[4][3] XOR = D[4]: 00C9082000000000 -> 30BD27FA89CD1EF7

state[4][4] XOR = D[4]: D1C55DD1C985B54D -> E1B1720B4048ABBA

State AFTER θ (Theta):

9D6BAD6B2D8F7A3D 71F4AEAD6120E7D3 8DAABC35C7F2D6D4
05D4BDF0FE4C8D98 995A36E83A76C6E5

C808FA1F5FE2C5B9 A405BB4AF4B92493 55539505713D8BD4
7C3F953894E62651 9EFA63F723AB5FD1

20CA54F7BB2CCDC9 A58F710FB7171E1D 15539516705B4CE4
7BF9BD98D8140415 30742FE9CBC50E77

0A3E3D43E9119F0F 67EC95894457A0F5 900E44CCF4EE0135
16B3ED62B97FBD6A 30BD27FA89CD1EF7

2925A92B3EB429C3 7FE115EB7457A0F5 B43A97E0D9898DDB
483477B4BE08A20D E1B1720B4048ABBA

ρ (Rho) Transformation

Each lane is rotated by a specific offset based on its (x, y) position:

Lane (0, 0): Original = 9D6BAD6B2D8F7A3D, Offset = 0, Rotated =
9D6BAD6B2D8F7A3D

Lane (0, 1): Original = C808FA1F5FE2C5B9, Offset = 36, Rotated =
FE2C5B9C808FA1F5

Lane (0, 2): Original = 20CA54F7BB2CCDC9, Offset = 3, Rotated =
0652A7BDD9666E49

Lane (0, 3): Original = 0A3E3D43E9119F0F, Offset = 41, Rotated =
233E1E147C7A87D2

Lane (0, 4): Original = 2925A92B3EB429C3, Offset = 18, Rotated =
A4ACFAD0A70CA496

Lane (1, 0): Original = 71F4AEAD6120E7D3, Offset = 1, Rotated =
E3E95D5AC241CFA6

Lane (1, 1): Original = A405BB4AF4B92493, Offset = 44, Rotated =
92493A405BB4AF4B

Lane (1, 2): Original = A58F710FB7171E1D, Offset = 10, Rotated =
3DC43EDC5C787696

Lane (1, 3): Original = 67EC95894457A0F5, Offset = 45, Rotated =
F41EACFD92B1288A

Lane (1, 4): Original = 7FE115EB7457A0F5, Offset = 2, Rotated =
FF8457ADD15E83D5

Lane (2, 0): Original = 8DAABC35C7F2D6D4, Offset = 62, Rotated = 236AAF0D71FCB5B5

Lane (2, 1): Original = 55539505713D8BD4, Offset = 6, Rotated = 54E5415C4F62F515

Lane (2, 2): Original = 15539516705B4CE4, Offset = 43, Rotated = DA6720AA9CA8B382

Lane (2, 3): Original = 900E44CCF4EE0135, Offset = 15, Rotated = 22667A77009AC807

Lane (2, 4): Original = B43A97E0D9898DDB, Offset = 61, Rotated = 768752FC1B3131BB

Lane (3, 0): Original = 05D4BDF0FE4C8D98, Offset = 28, Rotated = 0FE4C8D9805D4BDF

Lane (3, 1): Original = 7C3F953894E62651, Offset = 55, Rotated = 28BE1FCA9C4A7313

Lane (3, 2): Original = 7BF9BD98D8140415, Offset = 25, Rotated = 31B028082AF7F37B

Lane (3, 3): Original = 16B3ED62B97FBD6A, Offset = 21, Rotated = AC572FF7AD42D67D

Lane (3, 4): Original = 483477B4BE08A20D, Offset = 56, Rotated = 0D483477B4BE08A2

Lane (4, 0): Original = 995A36E83A76C6E5, Offset = 27, Rotated = 41D3B6372CCAD1B7

Lane (4, 1): Original = 9EFA63F723AB5FD1, Offset = 20, Rotated = 3F723AB5FD19EFA6

Lane (4, 2): Original = 30742FE9CBC50E77, Offset = 39, Rotated = E2873B983A17F4E5

Lane (4, 3): Original = 30BD27FA89CD1EF7, Offset = 8, Rotated = BD27FA89CD1EF730

Lane (4, 4): Original = E1B1720B4048ABBA, Offset = 14, Rotated = 5C82D0122AEEB86C

State AFTER ρ (Rho):

9D6BAD6B2D8F7A3D E3E95D5AC241CFA6 236AAF0D71FCB5B5
0FE4C8D9805D4BDF 41D3B6372CCAD1B7

FE2C5B9C808FA1F5 92493A405BB4AF4B 54E5415C4F62F515
28BE1FCA9C4A7313 3F723AB5FD19EFA6

0652A7BDD9666E49 3DC43EDC5C787696 DA6720AA9CA8B382
31B028082AF7F37B E2873B983A17F4E5

233E1E147C7A87D2 F41EACFD92B1288A 22667A77009AC807
AC572FF7AD42D67D BD27FA89CD1EF730

A4ACFAD0A70CA496 FF8457ADD15E83D5 768752FC1B3131BB
0D483477B4BE08A2 5C82D0122AEEB86C

Applying π (Pi) transformation:

Moving lane (0, 0) -> (0, 0)

Moving lane (0, 1) -> (1, 3)

Moving lane (0, 2) -> (2, 1)

Moving lane (0, 3) -> (3, 4)

Moving lane (0, 4) -> (4, 2)

Moving lane (1, 0) -> (0, 2)

Moving lane (1, 1) -> (1, 0)

Moving lane (1, 2) -> (2, 3)

Moving lane (1, 3) -> (3, 1)

Moving lane (1, 4) -> (4, 4)

Moving lane (2, 0) -> (0, 4)

Moving lane (2, 1) -> (1, 2)

Moving lane (2, 2) -> (2, 0)

Moving lane (2, 3) -> (3, 3)

Moving lane (2, 4) -> (4, 1)

Moving lane (3, 0) -> (0, 1)

Moving lane (3, 1) -> (1, 4)

Moving lane (3, 2) -> (2, 2)

Moving lane (3, 3) -> (3, 0)

Moving lane (3, 4) -> (4, 3)

Moving lane (4, 0) -> (0, 3)

Moving lane (4, 1) -> (1, 1)

Moving lane (4, 2) -> (2, 4)

Moving lane (4, 3) -> (3, 2)

Moving lane (4, 4) -> (4, 0)

State AFTER π (Pi):

9D6BAD6B2D8F7A3D 92493A405BB4AF4B DA6720AA9CA8B382
AC572FF7AD42D67D 5C82D0122AEEB86C

0FE4C8D9805D4BDF 3F723AB5FD19EFA6 0652A7BDD9666E49
F41EACFD92B1288A 768752FC1B3131BB

E3E95D5AC241CFA6 54E5415C4F62F515 31B028082AF7F37B
BD27FA89CD1EF730 A4ACFAD0A70CA496

41D3B6372CCAD1B7 FE2C5B9C808FA1F5 3DC43EDC5C787696
22667A77009AC807 0D483477B4BE08A2

236AAF0D71FCB5B5 28BE1FCA9C4A7313 E2873B983A17F4E5
233E1E147C7A87D2 FF8457ADD15E83D5

Applying χ (Chi) transformation:

Lane (0, 0): 9D6BAD6B2D8F7A3D -> D54DADC1A9876ABD

Lane (0, 1): 0FE4C8D9805D4BDF -> 0FE44DD1803B4B96

Lane (0, 2): E3E95D5AC241CFA6 -> C2F9755AE2D4CDCC

Lane (0, 3): 41D3B6372CCAD1B7 -> 4013927770BA87B5

Lane (0, 4): 236AAF0D71FCB5B5 -> E16B8F1D53E93151

Lane (1, 0): 92493A405BB4AF4B -> B65935157AF6EB36

Lane (1, 1): 3F723AB5FD19EFA6 -> CF7E32F5FF88EF24

Lane (1, 2): 54E5415C4F62F515 -> D8E293DD8A6AF115

Lane (1, 3): FE2C5B9C808FA1F5 -> FC0E1BBF800D29F4

Lane (1, 4): 28BE1FCA9C4A7313 -> 29861BCED8227001

Lane (2, 0): DA6720AA9CA8B382 -> 8AE7F0AA9E049B82

Lane (2, 1): 0652A7BDD9666E49 -> 04D3F5BDD0667F78

Lane (2, 2): 31B028082AF7F37B -> 3138285808F7F3FD

Lane (2, 3): 3DC43EDC5C787696 -> 30CC3ADCE85C7636

Lane (2, 4): E2873B983A17F4E5 -> 3E077A31BB13F4E0

Lane (3, 0): AC572FF7AD42D67D -> 2D3E029EA843946C

Lane (3, 1): F41EACFD92B1288A -> FD7E24FC12FD62CE

Lane (3, 2): BD27FA89CD1EF730 -> FE66FF838D5FBC10

Lane (3, 3): 22667A77009AC807 -> 62F5F87708DA1912

Lane (3, 4): 233E1E147C7A87D2 -> 2354B6145CDAB3F2

Lane (4, 0): 5C82D0122AEEB86C -> 5E82C21278DE3D2E

Lane (4, 1): 768752FC1B3131BB -> 469560D86631959B

Lane (4, 2): A4ACFAD0A70CA496 -> B0A8FAD4AA2E9487

Lane (4, 3): 0D483477B4BE08A2 -> B3647DFF34BB28E2

Lane (4, 4): FF8457ADD15E83D5 -> F710476F5D5CC1D7

State AFTER χ (Chi):

D54DADC1A9876ABD B65935157AF6EB36 8AE7F0AA9E049B82
2D3E029EA843946C 5E82C21278DE3D2E

0FE44DD1803B4B96 CF7E32F5FF88EF24 04D3F5BDD0667F78
FD7E24FC12FD62CE 469560D86631959B

C2F9755AE2D4CDCC D8E293DD8A6AF115 3138285808F7F3FD
FE66FF838D5FBC10 B0A8FAD4AA2E9487

4013927770BA87B5 FC0E1BBF800D29F4 30CC3ADCE85C7636
62F5F87708DA1912 B3647DFF34BB28E2

E16B8F1D53E93151 29861BCED8227001 3E077A31BB13F4E0
2354B6145CDAB3F2 F710476F5D5CC1D7

Applying ι (Iota) transformation:

Lane (0, 0): D54DADC1A9876ABD -> D54DADC1A987EA3F (XOR with RC[1] = 0000000000008082)

State AFTER ι (Iota):

D54DADC1A987EA3F B65935157AF6EB36 8AE7F0AA9E049B82 2D3E029EA843946C 5E82C21278DE3D2E

0FE44DD1803B4B96 CF7E32F5FF88EF24 04D3F5BDD0667F78 FD7E24FC12FD62CE 469560D86631959B

C2F9755AE2D4CDCC D8E293DD8A6AF115 3138285808F7F3FD FE66FF838D5FBC10 B0A8FAD4AA2E9487

4013927770BA87B5 FC0E1BBF800D29F4 30CC3ADCE85C7636 62F5F87708DA1912 B3647DFF34BB28E2

E16B8F1D53E93151 29861BCED8227001 3E077A31BB13F4E0 2354B6145CDAB3F2 F710476F5D5CC1D7

State AFTER Round 1:

D54DADC1A987EA3F B65935157AF6EB36 8AE7F0AA9E049B82 2D3E029EA843946C 5E82C21278DE3D2E

0FE44DD1803B4B96 CF7E32F5FF88EF24 04D3F5BDD0667F78 FD7E24FC12FD62CE 469560D86631959B

C2F9755AE2D4CDCC D8E293DD8A6AF115 3138285808F7F3FD FE66FF838D5FBC10 B0A8FAD4AA2E9487

4013927770BA87B5 FC0E1BBF800D29F4 30CC3ADCE85C7636 62F5F87708DA1912 B3647DFF34BB28E2

E16B8F1D53E93151 29861BCED8227001 3E077A31BB13F4E0 2354B6145CDAB3F2 F710476F5D5CC1D7

Computing C[x] (Column parity):

C[0] = state[0][0] XOR state[0][1] XOR state[0][2] XOR state[0][3] XOR state[0][4] = B9288820E83BDA81

C[1] = state[1][0] XOR state[1][1] XOR state[1][2] XOR state[1][3] XOR state[1][4] = 744D944C573BACF2

C[2] = state[2][0] XOR state[2][1] XOR state[2][2] XOR state[2][3] XOR state[2][4] = B1C76DA215DA95D1

C[3] = state[3][0] XOR state[3][1] XOR state[3][2] XOR state[3][3] XOR state[3][4] = 6F87978263E1E052

C[4] = state[4][0] XOR state[4][1] XOR state[4][2] XOR state[4][3] XOR state[4][4] = ECCB628EDD26D507

Computing D[x]:

D[0] = C[4] XOR ROTL(C[1], 1) = ECCB628EDD26D507 XOR E89B2898AE7759E4 = 04504A1673518CE3

D[1] = C[0] XOR ROTL(C[2], 1) = B9288820E83BDA81 XOR 638EDB442BB52BA3 = DAA65364C38EF122

D[2] = C[1] XOR ROTL(C[3], 1) = 744D944C573BACF2 XOR DF0F2F04C7C3C0A4 = AB42BB4890F86C56

D[3] = C[2] XOR ROTL(C[4], 1) = B1C76DA215DA95D1 XOR D996C51DBA4DAA0F = 6851A8BFAF973FDE

D[4] = C[3] XOR ROTL(C[0], 1) = 6F87978263E1E052 XOR 72511041D077B503 = 1DD687C3B3965551

Updating State with θ (Theta) transformation:

state[0][0] XOR = D[0]: D54DADC1A987EA3F -> D11DE7D7DAD666DC

state[0][1] XOR = D[0]: 0FE44DD1803B4B96 -> 0BB407C7F36AC775

state[0][2] XOR = D[0]: C2F9755AE2D4CDCC -> C6A93F4C9185412F

state[0][3] XOR = D[0]: 4013927770BA87B5 -> 4443D86103EB0B56

state[0][4] XOR = D[0]: E16B8F1D53E93151 -> E53BC50B20B8BDB2

state[1][0] XOR = D[1]: B65935157AF6EB36 -> 6CFF6671B9781A14

state[1][1] XOR = D[1]: CF7E32F5FF88EF24 -> 15D861913C061E06

state[1][2] XOR = D[1]: D8E293DD8A6AF115 -> 0244C0B949E40037

state[1][3] XOR = D[1]: FC0E1BBF800D29F4 -> 26A848DB4383D8D6

state[1][4] XOR = D[1]: 29861BCED8227001 -> F32048AA1BAC8123

state[2][0] XOR = D[2]: 8AE7F0AA9E049B82 -> 21A54BE20EFCF7D4

state[2][1] XOR = D[2]: 04D3F5BDD0667F78 -> AF914EF5409E132E

state[2][2] XOR = D[2]: 3138285808F7F3FD -> 9A7A9310980F9FAB

state[2][3] XOR = D[2]: 30CC3ADCE85C7636 -> 9B8E819478A41A60

state[2][4] XOR = D[2]: 3E077A31BB13F4E0 -> 9545C1792BEB98B6

state[3][0] XOR = D[3]: 2D3E029EA843946C -> 456FAA2107D4ABB2

state[3][1] XOR = D[3]: FD7E24FC12FD62CE -> 952F8C43BD6A5D10

state[3][2] XOR = D[3]: FE66FF838D5FBC10 -> 9637573C22C883CE

state[3][3] XOR = D[3]: 62F5F87708DA1912 -> 0AA450C8A74D26CC

state[3][4] XOR = D[3]: 2354B6145CDAB3F2 -> 4B051EABF34D8C2C

state[4][0] XOR = D[4]: 5E82C21278DE3D2E -> 435445D1CB48687F

state[4][1] XOR = D[4]: 469560D86631959B -> 5B43E71BD5A7C0CA

state[4][2] XOR = D[4]: B0A8FAD4AA2E9487 -> AD7E7D1719B8C1D6

state[4][3] XOR = D[4]: B3647DFF34BB28E2 -> AEB2FA3C872D7DB3

state[4][4] XOR = D[4]: F710476F5D5CC1D7 -> EAC6C0ACEECA9486

State AFTER θ (Theta):

D11DE7D7DAD666DC 6CFF6671B9781A14 21A54BE20EFCF7D4
456FAA2107D4ABB2 435445D1CB48687F

0BB407C7F36AC775 15D861913C061E06 AF914EF5409E132E
952F8C43BD6A5D10 5B43E71BD5A7C0CA

C6A93F4C9185412F 0244C0B949E40037 9A7A9310980F9FAB
9637573C22C883CE AD7E7D1719B8C1D6

4443D86103EB0B56 26A848DB4383D8D6 9B8E819478A41A60
0AA450C8A74D26CC AEB2FA3C872D7DB3

E53BC50B20B8BDB2 F32048AA1BAC8123 9545C1792BEB98B6
4B051EABF34D8C2C EAC6C0ACEECA9486

ρ (Rho) Transformation

Each lane is rotated by a specific offset based on its (x, y) position:

Lane (0, 0): Original = D11DE7D7DAD666DC, Offset = 0, Rotated =
D11DE7D7DAD666DC

Lane (0, 1): Original = 0BB407C7F36AC775, Offset = 36, Rotated = 36AC7750BB407C7F

Lane (0, 2): Original = C6A93F4C9185412F, Offset = 3, Rotated = 3549FA648C2A097E

Lane (0, 3): Original = 4443D86103EB0B56, Offset = 41, Rotated = D616AC8887B0C207

Lane (0, 4): Original = E53BC50B20B8BDB2, Offset = 18, Rotated = 142C82E2F6CB94EF

Lane (1, 0): Original = 6CFF6671B9781A14, Offset = 1, Rotated = D9FECCE372F03428

Lane (1, 1): Original = 15D861913C061E06, Offset = 44, Rotated = 61E0615D861913C0

Lane (1, 2): Original = 0244C0B949E40037, Offset = 10, Rotated = 1302E5279000DC09

Lane (1, 3): Original = 26A848DB4383D8D6, Offset = 45, Rotated = 7B1AC4D5091B6870

Lane (1, 4): Original = F32048AA1BAC8123, Offset = 2, Rotated = CC8122A86EB2048F

Lane (2, 0): Original = 21A54BE20EFCF7D4, Offset = 62, Rotated = 086952F883BF3DF5

Lane (2, 1): Original = AF914EF5409E132E, Offset = 6, Rotated = E453BD502784CBAB

Lane (2, 2): Original = 9A7A9310980F9FAB, Offset = 43, Rotated = 7CFD5CD3D49884C0

Lane (2, 3): Original = 9B8E819478A41A60, Offset = 15, Rotated = 40CA3C520D304DC7

Lane (2, 4): Original = 9545C1792BEB98B6, Offset = 61, Rotated = D2A8B82F257D7316

Lane (3, 0): Original = 456FAA2107D4ABB2, Offset = 28, Rotated = 107D4ABB2456FAA2

Lane (3, 1): Original = 952F8C43BD6A5D10, Offset = 55, Rotated = 884A97C621DEB52E

Lane (3, 2): Original = 9637573C22C883CE, Offset = 25, Rotated = 784591079D2C6EAE

Lane (3, 3): Original = 0AA450C8A74D26CC, Offset = 21, Rotated = 1914E9A4D981548A

Lane (3, 4): Original = 4B051EABF34D8C2C, Offset = 56, Rotated = 2C4B051EABF34D8C

Lane (4, 0): Original = 435445D1CB48687F, Offset = 27, Rotated = 8E5A4343FA1AA22E

Lane (4, 1): Original = 5B43E71BD5A7C0CA, Offset = 20, Rotated = 71BD5A7C0CA5B43E

Lane (4, 2): Original = AD7E7D1719B8C1D6, Offset = 39, Rotated = DC60EB56BF3E8B8C

Lane (4, 3): Original = AEB2FA3C872D7DB3, Offset = 8, Rotated = B2FA3C872D7DB3AE

Lane (4, 4): Original = EAC6C0ACEECA9486, Offset = 14, Rotated = B02B3BB2A521BAB1

State AFTER ρ (Rho):

D11DE7D7DAD666DC D9FECCE372F03428 086952F883BF3DF5 107D4ABB2456FAA2 8E5A4343FA1AA22E

36AC7750BB407C7F 61E0615D861913C0 E453BD502784CBAB 884A97C621DEB52E 71BD5A7C0CA5B43E

3549FA648C2A097E 1302E5279000DC09 7CFD5CD3D49884C0 784591079D2C6EAE DC60EB56BF3E8B8C

D616AC8887B0C207 7B1AC4D5091B6870 40CA3C520D304DC7 1914E9A4D981548A B2FA3C872D7DB3AE

142C82E2F6CB94EF CC8122A86EB2048F D2A8B82F257D7316 2C4B051EABF34D8C B02B3BB2A521BAB1

Applying π (Pi) transformation:

Moving lane (0, 0) -> (0, 0)

Moving lane (0, 1) -> (1, 3)

Moving lane (0, 2) -> (2, 1)

Moving lane (0, 3) -> (3, 4)

Moving lane (0, 4) -> (4, 2)

Moving lane (1, 0) -> (0, 2)

Moving lane (1, 1) -> (1, 0)

Moving lane (1, 2) -> (2, 3)

Moving lane (1, 3) -> (3, 1)

Moving lane (1, 4) -> (4, 4)

Moving lane (2, 0) -> (0, 4)

Moving lane (2, 1) -> (1, 2)

Moving lane (2, 2) -> (2, 0)

Moving lane (2, 3) -> (3, 3)

Moving lane (2, 4) -> (4, 1)

Moving lane (3, 0) -> (0, 1)

Moving lane (3, 1) -> (1, 4)

Moving lane (3, 2) -> (2, 2)

Moving lane (3, 3) -> (3, 0)

Moving lane (3, 4) -> (4, 3)

Moving lane (4, 0) -> (0, 3)

Moving lane (4, 1) -> (1, 1)

Moving lane (4, 2) -> (2, 4)

Moving lane (4, 3) -> (3, 2)

Moving lane (4, 4) -> (4, 0)

State AFTER π (Pi):

D11DE7D7DAD666DC 61E0615D861913C0 7CFD5CD3D49884C0
1914E9A4D981548A B02B3BB2A521BAB1

107D4ABB2456FAA2 71BD5A7C0CA5B43E 3549FA648C2A097E
7B1AC4D5091B6870 D2A8B82F257D7316

D9FECCE372F03428 E453BD502784CBAB 784591079D2C6EAE
B2FA3C872D7DB3AE 142C82E2F6CB94EF

8E5A4343FA1AA22E 36AC7750BB407C7F 1302E5279000DC09
40CA3C520D304DC7 2C4B051EABF34D8C

086952F883BF3DF5 884A97C621DEB52E DC60EB56BF3E8B8C
D616AC8887B0C207 CC8122A86EB2048F

Applying χ (Chi) transformation:

Lane (0, 0): D11DE7D7DAD666DC -> CD00FB558A56E2DC

Lane (0, 1): 107D4ABB2456FAA2 -> 143DEABBA45CF3E2

Lane (0, 2): D9FECCE372F03428 -> C1FACCE4EAD8102C

Lane (0, 3): 8E5A4343FA1AA22E -> 8F58C364FA1A222E

Lane (0, 4): 086952F883BF3DF5 -> 5C493AE81D9F3775

Lane (1, 0): 61E0615D861913C0 -> 60E0C0798F1843CA

Lane (1, 1): 71BD5A7C0CA5B43E -> 3BAF5EED0DB4D43E

Lane (1, 2): E453BD502784CBAB -> 66E991D007D55AAB

Lane (1, 3): 36AC7750BB407C7F -> 76646F00B6707DB9

Lane (1, 4): 884A97C621DEB52E -> 8A5C934E215EF52D

Lane (2, 0): 7CFD5CD3D49884C0 -> DCD64EC1F0B82EF1

Lane (2, 1): 3549FA648C2A097E -> B5E9C24EA84E1A78

Lane (2, 2): 784591079D2C6EAE -> 7C4113674FAE6AEF

Lane (2, 3): 1302E5279000DC09 -> 3F03E42B32C3DC01

Lane (2, 4): DC60EB56BF3E8B8C -> D4E1E976D73C8F04

Lane (3, 0): 1914E9A4D981548A -> 58002DE1835710C6

Lane (3, 1): 7B1AC4D5091B6870 -> 7B4F86450919E0D0

Lane (3, 2): B2FA3C872D7DB3AE -> 7B2870862D4D93AE

Lane (3, 3): 40CA3C520D304DC7 -> C2DA7E135D38EFE5

Lane (3, 4): D616AC8887B0C207 -> D67EFCD806BDFB77

Lane (4, 0): B02B3BB2A521BAB1 -> 90CB3BBAA128ABB1

Lane (4, 1): D2A8B82F257D7316 -> B328A86B2DDC770A

Lane (4, 2): 142C82E2F6CB94EF -> 302DB3F2F3CF5F6C

Lane (4, 3): 2C4B051EABF34D8C -> 1CEF310EAAB311DD

Lane (4, 4): CC8122A86EB2048F -> 4C83A7AE4EF28485

State AFTER χ (Chi):

CD00FB558A56E2DC 60E0C0798F1843CA DCD64EC1F0B82EF1
58002DE1835710C6 90CB3BBAA128ABB1

143DEABBA45CF3E2 3BAF5EED0DB4D43E B5E9C24EA84E1A78
7B4F86450919E0D0 B328A86B2DDC770A

C1FACCE4EAD8102C 66E991D007D55AAB 7C4113674FAE6AEF
7B2870862D4D93AE 302DB3F2F3CF5F6C

8F58C364FA1A222E 76646F00B6707DB9 3F03E42B32C3DC01
C2DA7E135D38EFE5 1CEF310EAAB311DD

5C493AE81D9F3775 8A5C934E215EF52D D4E1E976D73C8F04
D67EFCD806BDFB77 4C83A7AE4EF28485

Applying ι (Iota) transformation:

Lane (0, 0): CD00FB558A56E2DC -> 4D00FB558A566256 (XOR with RC[2] =
800000000000808A)

State AFTER ι (Iota):

4D00FB558A566256 60E0C0798F1843CA DCD64EC1F0B82EF1
58002DE1835710C6 90CB3BBAA128ABB1

143DEABBA45CF3E2 3BAF5EED0DB4D43E B5E9C24EA84E1A78
7B4F86450919E0D0 B328A86B2DDC770A

C1FACCE4EAD8102C 66E991D007D55AAB 7C4113674FAE6AEF
7B2870862D4D93AE 302DB3F2F3CF5F6C

8F58C364FA1A222E 76646F00B6707DB9 3F03E42B32C3DC01
C2DA7E135D38EFE5 1CEF310EAAB311DD

5C493AE81D9F3775 8A5C934E215EF52D D4E1E976D73C8F04
D67EFCD806BDFB77 4C83A7AE4EF28485

State AFTER Round 2:

4D00FB558A566256 60E0C0798F1843CA DCD64EC1F0B82EF1
58002DE1835710C6 90CB3BBAA128ABB1

143DEABBA45CF3E2 3BAF5EED0DB4D43E B5E9C24EA84E1A78
7B4F86450919E0D0 B328A86B2DDC770A

C1FACCE4EAD8102C 66E991D007D55AAB 7C4113674FAE6AEF
7B2870862D4D93AE 302DB3F2F3CF5F6C

8F58C364FA1A222E 76646F00B6707DB9 3F03E42B32C3DC01 C2DA7E135D38EFE5 1CEF310EAAB311DD

5C493AE81D9F3775 8A5C934E215EF52D D4E1E976D73C8F04 D67EFCD806BDFB77 4C83A7AE4EF28485

Computing C[x] (Column parity):

C[0] = state[0][0] XOR state[0][1] XOR state[0][2] XOR state[0][3] XOR state[0][4] = 4BD62486235794C3

C[1] = state[1][0] XOR state[1][1] XOR state[1][2] XOR state[1][3] XOR state[1][4] = C19EF30A125745CB

C[2] = state[2][0] XOR state[2][1] XOR state[2][2] XOR state[2][3] XOR state[2][4] = FE9C92B5F2A70D63

C[3] = state[3][0] XOR state[3][1] XOR state[3][2] XOR state[3][3] XOR state[3][4] = 4CC359E9FC86772A

C[4] = state[4][0] XOR state[4][1] XOR state[4][2] XOR state[4][3] XOR state[4][4] = 43A2B6839B7A168F

Computing D[x]:

D[0] = C[4] XOR ROTL(C[1], 1) = 43A2B6839B7A168F XOR 833DE61424AE8B97 = C09F5097BFD49D18

D[1] = C[0] XOR ROTL(C[2], 1) = 4BD62486235794C3 XOR FD39256BE54E1AC7 = B6EF01EDC6198E04

D[2] = C[1] XOR ROTL(C[3], 1) = C19EF30A125745CB XOR 9986B3D3F90CEE54 = 581840D9EB5BAB9F

D[3] = C[2] XOR ROTL(C[4], 1) = FE9C92B5F2A70D63 XOR 87456D0736F42D1E = 79D9FFB2C453207D

D[4] = C[3] XOR ROTL(C[0], 1) = 4CC359E9FC86772A XOR 97AC490C46AF2986 = DB6F10E5BA295EAC

Updating State with θ (Theta) transformation:

state[0][0] XOR = D[0]: 4D00FB558A566256 -> 8D9FABC23582FF4E

state[0][1] XOR = D[0]: 143DEABBA45CF3E2 -> D4A2BA2C1B886EFA

state[0][2] XOR = D[0]: C1FACCE4EAD8102C -> 01659C73550C8D34

state[0][3] XOR = D[0]: 8F58C364FA1A222E -> 4FC793F345CEBF36

state[0][4] XOR = D[0]: 5C493AE81D9F3775 -> 9CD66A7FA24BAA6D

state[1][0] XOR = D[1]: 60E0C0798F1843CA -> D60FC1944901CDCE

state[1][1] XOR = D[1]: 3BAF5EED0DB4D43E -> 8D405F00CBAD5A3A

state[1][2] XOR = D[1]: 66E991D007D55AAB -> D006903DC1CCD4AF

state[1][3] XOR = D[1]: 76646F00B6707DB9 -> C08B6EED7069F3BD

state[1][4] XOR = D[1]: 8A5C934E215EF52D -> 3CB392A3E7477B29

state[2][0] XOR = D[2]: DCD64EC1F0B82EF1 -> 84CE0E181BE3856E

state[2][1] XOR = D[2]: B5E9C24EA84E1A78 -> EDF182974315B1E7

state[2][2] XOR = D[2]: 7C4113674FAE6AEF -> 245953BEA4F5C170

state[2][3] XOR = D[2]: 3F03E42B32C3DC01 -> 671BA4F2D998779E

state[2][4] XOR = D[2]: D4E1E976D73C8F04 -> 8CF9A9AF3C67249B

state[3][0] XOR = D[3]: 58002DE1835710C6 -> 21D9D253470430BB

state[3][1] XOR = D[3]: 7B4F86450919E0D0 -> 029679F7CD4AC0AD

state[3][2] XOR = D[3]: 7B2870862D4D93AE -> 02F18F34E91EB3D3

state[3][3] XOR = D[3]: C2DA7E135D38EFE5 -> BB0381A1996BCF98

state[3][4] XOR = D[3]: D67EFCD806BDFB77 -> AFA7036AC2EEDB0A

state[4][0] XOR = D[4]: 90CB3BBAA128ABB1 -> 4BA42B5F1B01F51D

state[4][1] XOR = D[4]: B328A86B2DDC770A -> 6847B88E97F529A6

state[4][2] XOR = D[4]: 302DB3F2F3CF5F6C -> EB42A31749E601C0

state[4][3] XOR = D[4]: 1CEF310EAAB311DD -> C78021EB109A4F71

state[4][4] XOR = D[4]: 4C83A7AE4EF28485 -> 97ECB74BF4DBDA29

State AFTER θ (Theta):

8D9FABC23582FF4E D60FC1944901CDCE 84CE0E181BE3856E
21D9D253470430BB 4BA42B5F1B01F51D

D4A2BA2C1B886EFA 8D405F00CBAD5A3A EDF182974315B1E7
029679F7CD4AC0AD 6847B88E97F529A6

01659C73550C8D34 D006903DC1CCD4AF 245953BEA4F5C170
02F18F34E91EB3D3 EB42A31749E601C0

4FC793F345CEBF36 C08B6EED7069F3BD 671BA4F2D998779E
BB0381A1996BCF98 C78021EB109A4F71

9CD66A7FA24BAA6D 3CB392A3E7477B29 8CF9A9AF3C67249B
AFA7036AC2EEDB0A 97ECB74BF4DBDA29

ρ (Rho) Transformation

Each lane is rotated by a specific offset based on its (x, y) position:

Lane (0, 0): Original = 8D9FABC23582FF4E, Offset = 0, Rotated = 8D9FABC23582FF4E

Lane (0, 1): Original = D4A2BA2C1B886EFA, Offset = 36, Rotated = B886EFAD4A2BA2C1

Lane (0, 2): Original = 01659C73550C8D34, Offset = 3, Rotated = 0B2CE39AA86469A0

Lane (0, 3): Original = 4FC793F345CEBF36, Offset = 41, Rotated = 9D7E6C9F8F27E68B

Lane (0, 4): Original = 9CD66A7FA24BAA6D, Offset = 18, Rotated = A9FE892EA9B67359

Lane (1, 0): Original = D60FC1944901CDCE, Offset = 1, Rotated = AC1F832892039B9D

Lane (1, 1): Original = 8D405F00CBAD5A3A, Offset = 44, Rotated = D5A3A8D405F00CBA

Lane (1, 2): Original = D006903DC1CCD4AF, Offset = 10, Rotated = 1A40F7073352BF40

Lane (1, 3): Original = C08B6EED7069F3BD, Offset = 45, Rotated = 3E77B8116DDDAE0D

Lane (1, 4): Original = 3CB392A3E7477B29, Offset = 2, Rotated = F2CE4A8F9D1DECA4

Lane (2, 0): Original = 84CE0E181BE3856E, Offset = 62, Rotated = A133838606F8E15B

Lane (2, 1): Original = EDF182974315B1E7, Offset = 6, Rotated = 7C60A5D0C56C79FB

Lane (2, 2): Original = 245953BEA4F5C170, Offset = 43, Rotated = AE0B8122CA9DF527

Lane (2, 3): Original = 671BA4F2D998779E, Offset = 15, Rotated = D2796CCC3BCF338D

Lane (2, 4): Original = 8CF9A9AF3C67249B, Offset = 61, Rotated = 719F3535E78CE493

Lane (3, 0): Original = 21D9D253470430BB, Offset = 28, Rotated = 3470430BB21D9D25

Lane (3, 1): Original = 029679F7CD4AC0AD, Offset = 55, Rotated = 56814B3CFBE6A560

Lane (3, 2): Original = 02F18F34E91EB3D3, Offset = 25, Rotated = 69D23D67A605E31E

Lane (3, 3): Original = BB0381A1996BCF98, Offset = 21, Rotated = 34332D79F3176070

Lane (3, 4): Original = AFA7036AC2EEDB0A, Offset = 56, Rotated = 0AAFA7036AC2EEDB

Lane (4, 0): Original = 4BA42B5F1B01F51D, Offset = 27, Rotated = F8D80FA8EA5D215A

Lane (4, 1): Original = 6847B88E97F529A6, Offset = 20, Rotated = 88E97F529A66847B

Lane (4, 2): Original = EB42A31749E601C0, Offset = 39, Rotated = F300E075A1518BA4

Lane (4, 3): Original = C78021EB109A4F71, Offset = 8, Rotated = 8021EB109A4F71C7

Lane (4, 4): Original = 97ECB74BF4DBDA29, Offset = 14, Rotated = 2DD2FD36F68A65FB

State AFTER ρ (Rho):

8D9FABC23582FF4E AC1F832892039B9D A133838606F8E15B
3470430BB21D9D25 F8D80FA8EA5D215A

B886EFAD4A2BA2C1 D5A3A8D405F00CBA 7C60A5D0C56C79FB
56814B3CFBE6A560 88E97F529A66847B

0B2CE39AA86469A0 1A40F7073352BF40 AE0B8122CA9DF527
69D23D67A605E31E F300E075A1518BA4

9D7E6C9F8F27E68B 3E77B8116DDDAE0D D2796CCC3BCF338D
34332D79F3176070 8021EB109A4F71C7

A9FE892EA9B67359 F2CE4A8F9D1DECA4 719F3535E78CE493
0AAFA7036AC2EEDB 2DD2FD36F68A65FB

Applying π (Pi) transformation:

Moving lane (0, 0) -> (0, 0)

Moving lane (0, 1) -> (1, 3)

Moving lane (0, 2) -> (2, 1)

Moving lane (0, 3) -> (3, 4)

Moving lane (0, 4) -> (4, 2)

Moving lane (1, 0) -> (0, 2)

Moving lane (1, 1) -> (1, 0)

Moving lane (1, 2) -> (2, 3)

Moving lane (1, 3) -> (3, 1)

Moving lane (1, 4) -> (4, 4)

Moving lane (2, 0) -> (0, 4)

Moving lane (2, 1) -> (1, 2)

Moving lane (2, 2) -> (2, 0)

Moving lane (2, 3) -> (3, 3)

Moving lane (2, 4) -> (4, 1)

Moving lane (3, 0) -> (0, 1)

Moving lane (3, 1) -> (1, 4)

Moving lane (3, 2) -> (2, 2)

Moving lane (3, 3) -> (3, 0)

Moving lane (3, 4) -> (4, 3)

Moving lane (4, 0) -> (0, 3)

Moving lane (4, 1) -> (1, 1)

Moving lane (4, 2) -> (2, 4)

Moving lane (4, 3) -> (3, 2)

Moving lane (4, 4) -> (4, 0)

State AFTER π (Pi):

8D9FABC23582FF4E D5A3A8D405F00CBA AE0B8122CA9DF527
34332D79F3176070 2DD2FD36F68A65FB

3470430BB21D9D25 88E97F529A66847B 0B2CE39AA86469A0
3E77B8116DDDAE0D 719F3535E78CE493

AC1F832892039B9D 7C60A5D0C56C79FB 69D23D67A605E31E
8021EB109A4F71C7 A9FE892EA9B67359

F8D80FA8EA5D215A B886EFAD4A2BA2C1 1A40F7073352BF40
D2796CCC3BCF338D 0AAFA7036AC2EEDB

A133838606F8E15B 56814B3CFBE6A560 F300E075A1518BA4
9D7E6C9F8F27E68B F2CE4A8F9D1DECA4

Applying χ (Chi) transformation:

Lane (0, 0): 8D9FABC23582FF4E -> A797AAE0FF8F0E4B

Lane (0, 1): 3470430BB21D9D25 -> 3774C383921DF4A5

Lane (0, 2): AC1F832892039B9D -> AD8D9B0FB0021999

Lane (0, 3): F8D80FA8EA5D215A -> FA981FAADB0D3C5A

Lane (0, 4): A133838606F8E15B -> 003323C706E9EBDF

Lane (1, 0): D5A3A8D405F00CBA -> C593848D34F20CEA

Lane (1, 1): 88E97F529A66847B -> BCBA6753DFFF0276

Lane (1, 2): 7C60A5D0C56C79FB -> FC4167C0DD26693A

Lane (1, 3): B886EFAD4A2BA2C1 -> 78BFE76542A6A24C

Lane (1, 4): 56814B3CFBE6A560 -> 5AFF47B6F5C0C16B

Lane (2, 0): AE0B8122CA9DF527 -> A7CB5124CE15F0AC

Lane (2, 1): 0B2CE39AA86469A0 -> 4AA4E6BE2A642932

Lane (2, 2): 69D23D67A605E31E -> 400C3D4987B5E106

Lane (2, 3): 1A40F7073352BF40 -> 12C6740473527312

Lane (2, 4): F300E075A1518BA4 -> 9180E275B1498380

Lane (3, 0): 34332D79F3176070 -> B43E2FB9F217FA74

Lane (3, 1): 3E77B8116DDDAE0D -> 3A17FA1B7DCCB729

Lane (3, 2): 8021EB109A4F71C7 -> 8420E910884EF943

Lane (3, 3): D2796CCC3BCF338D -> 22296464BBD2328D

Lane (3, 4): 9D7E6C9F8F27E68B -> 9C4FED9F8DC7E7D0

Lane (4, 0): 2DD2FD36F68A65FB -> 7DF2FD22F6FA654B

Lane (4, 1): 719F3535E78CE493 -> F9160965EFEEE4C9

Lane (4, 2): A9FE892EA9B67359 -> F99EADFEECDA133B

Lane (4, 3): 0AAFA7036AC2EEDB -> 0AA947066AE06C5A

Lane (4, 4): F2CE4A8F9D1DECA4 -> A44E02B7641BE884

State AFTER χ (Chi):

A797AAE0FF8F0E4B C593848D34F20CEA A7CB5124CE15F0AC B43E2FB9F217FA74 7DF2FD22F6FA654B

3774C383921DF4A5 BCBA6753DFFF0276 4AA4E6BE2A642932 3A17FA1B7DCCB729 F9160965EFEEE4C9

AD8D9B0FB0021999 FC4167C0DD26693A 400C3D4987B5E106 8420E910884EF943 F99EADFEECDA133B

FA981FAADB0D3C5A 78BFE76542A6A24C 12C6740473527312 22296464BBD2328D 0AA947066AE06C5A

003323C706E9EBDF 5AFF47B6F5C0C16B 9180E275B1498380 9C4FED9F8DC7E7D0 A44E02B7641BE884

Applying ι (Iota) transformation:

Lane (0, 0): A797AAE0FF8F0E4B -> 2797AAE07F8F8E4B (XOR with RC[3] = 8000000080008000)

State AFTER ι (Iota):

2797AAE07F8F8E4B C593848D34F20CEA A7CB5124CE15F0AC
B43E2FB9F217FA74 7DF2FD22F6FA654B

3774C383921DF4A5 BCBA6753DFFF0276 4AA4E6BE2A642932
3A17FA1B7DCCB729 F9160965EFEEE4C9

AD8D9B0FB0021999 FC4167C0DD26693A 400C3D4987B5E106
8420E910884EF943 F99EADFEECDA133B

FA981FAADB0D3C5A 78BFE76542A6A24C 12C6740473527312
22296464BBD2328D 0AA947066AE06C5A

003323C706E9EBDF 5AFF47B6F5C0C16B 9180E275B1498380
9C4FED9F8DC7E7D0 A44E02B7641BE884

State AFTER Round 3:

2797AAE07F8F8E4B C593848D34F20CEA A7CB5124CE15F0AC
B43E2FB9F217FA74 7DF2FD22F6FA654B

3774C383921DF4A5 BCBA6753DFFF0276 4AA4E6BE2A642932
3A17FA1B7DCCB729 F9160965EFEEE4C9

AD8D9B0FB0021999 FC4167C0DD26693A 400C3D4987B5E106
8420E910884EF943 F99EADFEECDA133B

FA981FAADB0D3C5A 78BFE76542A6A24C 12C6740473527312
22296464BBD2328D 0AA947066AE06C5A

003323C706E9EBDF 5AFF47B6F5C0C16B 9180E275B1498380
9C4FED9F8DC7E7D0 A44E02B7641BE884