

## Theta function:

Steps:

1. For all pairs  $(x, z)$  such that  $0 \leq x < 5$  and  $0 \leq z < w$ , let

$$C[x, z] = A[x, 0, z] \oplus A[x, 1, z] \oplus A[x, 2, z] \oplus A[x, 3, z] \oplus A[x, 4, z].$$

2. For all pairs  $(x, z)$  such that  $0 \leq x < 5$  and  $0 \leq z < w$  let

$$D[x, z] = C[(x-1) \bmod 5, z] \oplus C[(x+1) \bmod 5, (z-1) \bmod w].$$

3. For all triples  $(x, y, z)$  such that  $0 \leq x < 5$ ,  $0 \leq y < 5$ , and  $0 \leq z < w$ , let

$$A'[x, y, z] = A[x, y, z] \oplus D[x, z].$$

Let us consider the output as the following

**cf748aa5cd36e44be6659c8c35b35083f97cd7896c8403a800**

Step 1:

```
11001111 01110100 10001010 10100101 11001101
00110110 11100100 01001011 11100110 01100101
10011100 10001100 00110101 10110011 01010000
10000011 11111001 01111100 11010111 10001001
01101100 10000100 00000011 10101000 00000000
```

Inversing the above bits

```
11110011 00101110 01010001 10100101 10110011
01101100 00100111 11010010 01100111 10100110
00111001 00110001 10101100 11001101 00001010
11000001 10011111 00111110 11101011 10010001
00110110 00100001 11000000 00010101 00000000
```

Step 2:

Z=0

<b>2</b>	1	0	0	0	0
<b>1</b>	0	1	0	0	1
<b>0</b>	1	1	1	0	0
<b>4</b>	0	0	0	0	1
<b>3</b>	1	1	1	1	0
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=1

<b>2</b>	1	0	0	0	0
<b>1</b>	1	0	1	0	1
<b>0</b>	0	0	1	0	1
<b>4</b>	0	0	0	0	1
<b>3</b>	1	0	1	0	0
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=2

<b>2</b>	1	0	1	1	1
<b>1</b>	1	1	1	1	0
<b>0</b>	1	1	1	1	0
<b>4</b>	1	0	1	1	0
<b>3</b>	1	0	0	0	1
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=3

<b>2</b>	0	1	1	1	1
<b>1</b>	0	0	0	0	1
<b>0</b>	0	1	1	0	1
<b>4</b>	1	0	1	0	0
<b>3</b>	0	1	0	1	1
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=4

<b>2</b>	1	1	1	0	1
<b>1</b>	0	0	1	0	0
<b>0</b>	0	0	0	1	0
<b>4</b>	0	0	0	0	0
<b>3</b>	1	0	0	1	1
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=5

<b>2</b>	1	0	0	0	1
<b>1</b>	1	1	1	1	0
<b>0</b>	1	0	0	1	0
<b>4</b>	1	0	1	0	0
<b>3</b>	0	0	0	1	1
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=6

<b>2</b>	0	1	0	0	0
<b>1</b>	1	1	0	1	1
<b>0</b>	0	1	1	1	0
<b>4</b>	0	0	1	0	0
<b>3</b>	1	0	0	1	1
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=7

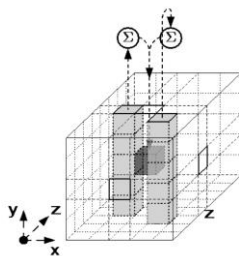
<b>2</b>	1	0	1	1	0
<b>1</b>	1	0	0	1	0
<b>0</b>	1	1	1	0	1
<b>4</b>	1	0	0	1	0
<b>3</b>	1	1	1	1	0
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

The below is the compression operation that has been done based on the equation 1

Y plane

<b>7</b>	1	0	1	0	1
<b>6</b>	0	1	0	1	0
<b>5</b>	0	1	0	1	0
<b>4</b>	0	1	0	0	0
<b>3</b>	1	1	1	0	0
<b>2</b>	1	0	0	0	0
<b>1</b>	1	0	1	0	1
<b>0</b>	1	1	0	1	0
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Xor the bits as shown in the figure:



Y plane:

<b>7</b>	0	1	1	1	1
<b>6</b>	1	0	0	0	1
<b>5</b>	1	0	1	0	1
<b>4</b>	1	1	1	0	1
<b>3</b>	0	1	1	1	1
<b>2</b>	0	0	0	1	1
<b>1</b>	0	1	1	1	1
<b>0</b>	0	0	1	1	0
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=0

<b>2</b>	0	0	1	1	1
<b>1</b>	1	1	1	1	1
<b>0</b>	0	1	0	1	0
<b>4</b>	1	0	1	1	1
<b>3</b>	0	1	0	0	0
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=1

<b>2</b>	1	0	0	0	0
<b>1</b>	1	0	1	0	1
<b>0</b>	0	0	1	0	1
<b>4</b>	0	0	0	0	1
<b>3</b>	1	0	1	0	0
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=2

<b>2</b>	1	1	0	1	0
<b>1</b>	0	0	0	1	1
<b>0</b>	0	0	0	1	1
<b>4</b>	1	1	0	1	1
<b>3</b>	0	1	1	0	0
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=3

<b>2</b>	0	0	1	1	0
<b>1</b>	0	0	0	0	1
<b>0</b>	0	1	1	0	1
<b>4</b>	1	0	1	0	0
<b>3</b>	0	1	0	1	
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=4

<b>2</b>	0	1	0	0	0
<b>1</b>	1	0	0	0	1
<b>0</b>	1	0	1	1	1
<b>4</b>	1	0	1	0	1
<b>3</b>	0	1	1	1	0
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=5

<b>2</b>	0	0	1	0	1
<b>1</b>	0	1	0	1	0
<b>0</b>	0	1	1	1	0
<b>4</b>	0	0	0	0	0
<b>3</b>	1	0	1	1	1
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z = 6

<b>2</b>	1	1	0	0	0
<b>1</b>	0	1	0	1	1
<b>0</b>	1	1	1	1	0
<b>4</b>	1	0	1	0	0
<b>3</b>	0	0	0	1	1
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

Z=7

<b>2</b>	0	0	0	1	1
<b>1</b>	0	0	1	1	0
<b>0</b>	0	1	0	0	0
<b>4</b>	0	0	1	1	1
<b>3</b>	0	1	0	1	1
	<b>3</b>	<b>4</b>	<b>0</b>	<b>1</b>	<b>2</b>

The binary bits are obtained from the above the slices :

01011110, 10101110, 01111000, 00001010, 10010011,  
11000001, 10100111, 11111011, 11001000, 10000110,  
10010100, 10110001, 10000101, 01100010, 00101010,  
01101100, 00011111, 00010111, 01000100, 10110001,  
10011011, 10100001, 11101001, 10111010, 00100000

The inverse function is performed for the above values :

01111010, 01110101, 00011110, 01010000, 11001001,  
10000011, 11100101, 11011111, 00010011, 01100001,  
00101001, 10001101, 10100001, 01000110, 01010100,  
00110110, 11111000, 11101000, 00100010, 10001101,  
11011001, 10000101, 10010111, 01011101, 00000100

When coverting the above binary bits into hexa, we get the below result

**7a751e50c983e5df1361298da1465436f8e8228dd985975d04**

$$C[(x-1) \bmod 5, z] = A[(x-1) \bmod 5, 0, z] \oplus A[(x-1) \bmod 5, 1, z] \oplus A[(x-1) \bmod 5, 2, z] \oplus A[(x-1) \bmod 5, 3, z] \oplus A[(x-1) \bmod 5, 4, z].$$

----- equation (1)

$$C[(x+1) \bmod 5, (z-1) \bmod 8] = A[(x+1) \bmod 5, 0, (z-1) \bmod 8] \oplus A[(x+1) \bmod 5, 1, (z-1) \bmod 8] \oplus A[(x+1) \bmod 5, 2, (z-1) \bmod 8] \oplus A[(x+1) \bmod 5, 3, (z-1) \bmod 8] \oplus A[(x+1) \bmod 5, 4, (z-1) \bmod 8].$$

-----equation (2)

$$D[x, z] = C[(x-1) \bmod 5, z] \oplus C[(x+1) \bmod 5, (z-1) \bmod w]. \quad \text{-----equation (3)}$$

Equation 1 and 2 in 3

$$D[x, z] = A[(x-1) \bmod 5, 0, z] \oplus A[(x-1) \bmod 5, 1, z] \oplus A[(x-1) \bmod 5, 2, z] \oplus A[(x-1) \bmod 5, 3, z] \oplus A[(x-1) \bmod 5, 4, z] \oplus A[(x+1) \bmod 5, 0, (z-1) \bmod 8] \oplus A[(x+1) \bmod 5, 1, (z-1) \bmod 8] \oplus A[(x+1) \bmod 5, 2, (z-1) \bmod 8] \oplus A[(x+1) \bmod 5, 3, (z-1) \bmod 8] \oplus A[(x+1) \bmod 5, 4, (z-1) \bmod 8]$$

We know that

$$A'[x, y, z] = A[x, y, z] \oplus D[x, z] \quad \text{-----equation (4)}$$

Equation 3 in 4

$$\begin{aligned} A'[x,y,z] = & A[x,y,z] \oplus A[(x-1) \bmod 5, 0, z] \oplus A[(x-1) \bmod 5, 1, z] \oplus A[(x-1) \bmod \\ & 5, 2, z] \oplus A[(x-1) \bmod 5, 3, z] \oplus A[(x-1) \bmod 5, 4, z] \oplus A[(x+1) \bmod 5, 0, (z-1) \\ & \bmod 8] \oplus A[(x+1) \bmod 5, 1, (z-1) \bmod 8] \oplus A[(x+1) \bmod 5, 2, (z-1) \bmod 8] \oplus \\ & A[(x+1) \bmod 5, 3, (z-1) \bmod 8] \oplus A[(x+1) \bmod 5, 4, (z-1) \bmod 8] \end{aligned}$$

We were trying to get a definite relationship between A and A` but we were able to get till the the above equation