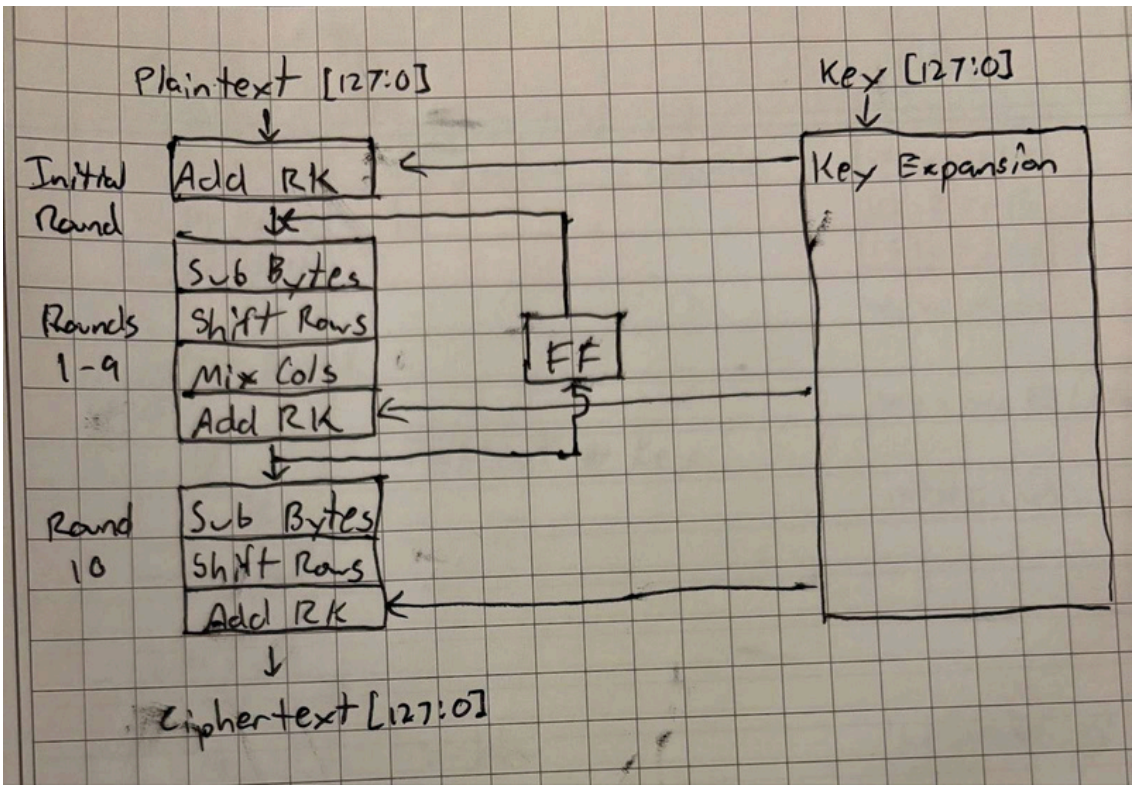
AES Encryption Core



Our AES encryption core design pipelines the data by round by registering the values after each round. This way multiple inputs can be processed in the pipeline at the same time to increase throughput. Additionally, registering intermediate data allows us to meet timing constraints for higher clock frequencies.

Plaintext

00	04	08	0c
01	05	09	0d
02	06	0a	0e
03	07	0b	0f

Only b_0, b_5, b_{10} and b_{15} are needed to calculate b_0

Key

00	02	04	06
08	0a	0c	0e
10	12	14	16
18	1a	1c	1e

w_0 w_1 w_2 w_3

Initial Add RK

00			
	0f		
		1e	
			11

Plaintext ⊕ Key

$w_4 = w_0 \oplus (rcon(sub(rotate(w3))))$

rotate $(w3)$ = 08, 10, 18, 00

Sub-Byte

63			
	76		
		72	
			82

S-box

sub(rotate(w3)) = 30, ca, ad, 63

Shift Rows

63			
76			
72			
82			

rcon ⊕ sub(rotate(w3)) = 01 ⊕ 30 = 31; 00 ⊕ ca = ca; 00 ⊕ ad = ad; 00 ⊕ 63 = 63

$w4 = w0 \oplus rcon(sub(rotate(w3)))$ = AA, C2, BD, 78

$2 \times h76 \oplus 76 = 9A$

Mix Cols

$b_0 = (2 \times h63) \oplus (3 \times h76) \oplus h72 \oplus h82 = h06 \oplus h9A \oplus h72 \oplus h82$

$b_1 = (2 \times h76) \oplus (3 \times h72) \oplus h82 \oplus h63$

$b_2 = (2 \times h72) \oplus (3 \times h82) \oplus h63 \oplus h76$

$b_3 = (2 \times h82) \oplus (3 \times h63) \oplus h76 \oplus h72$

Add Rk

06

$b_0 = h94 \oplus hAA$

$= h06$

Key (Round1)

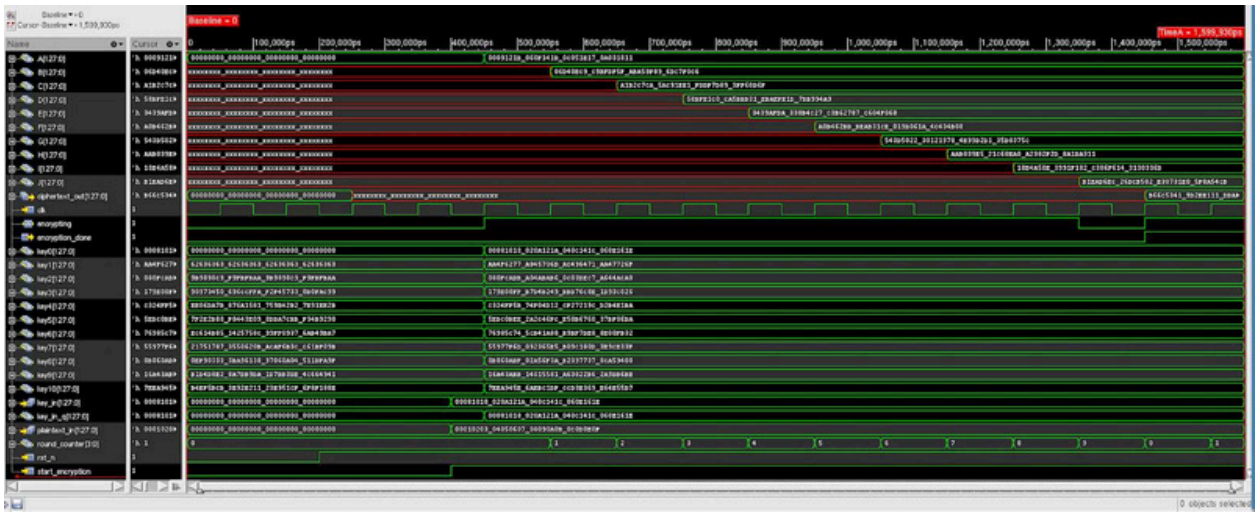
AA
C2
BD
78

$w4$ $w5$ $w6$ $w7$

The hardware complexity and area is slightly higher than expected, as is the minimum clock period. Otherwise, the hardware implementation is as expected.

Given a slack of 7.838 ns when simulating with a 10 ns clock, the maximum minimum clock period is 10 - 7.838 = 2.162 ns. Thus, the maximum clock frequency is 1/period = **462.5346 MHz.**

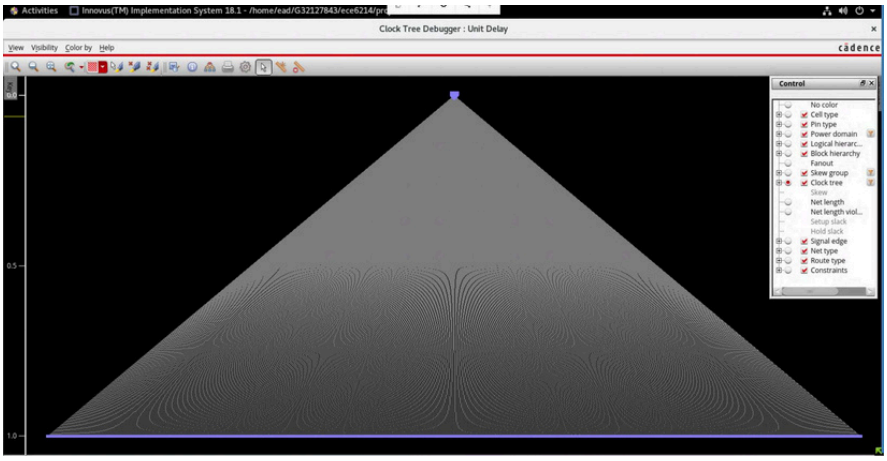
Simulation Waveform



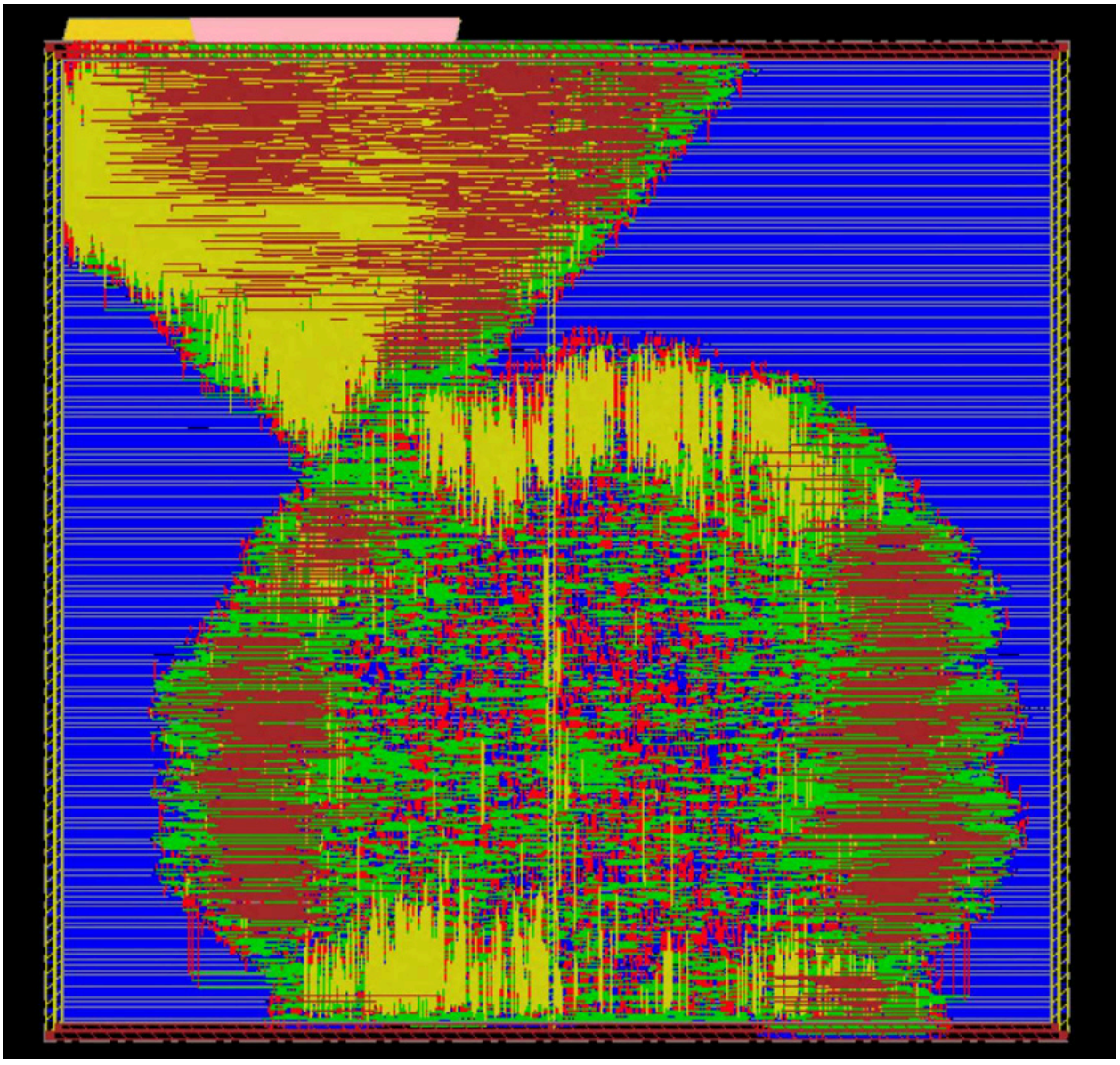
Log File

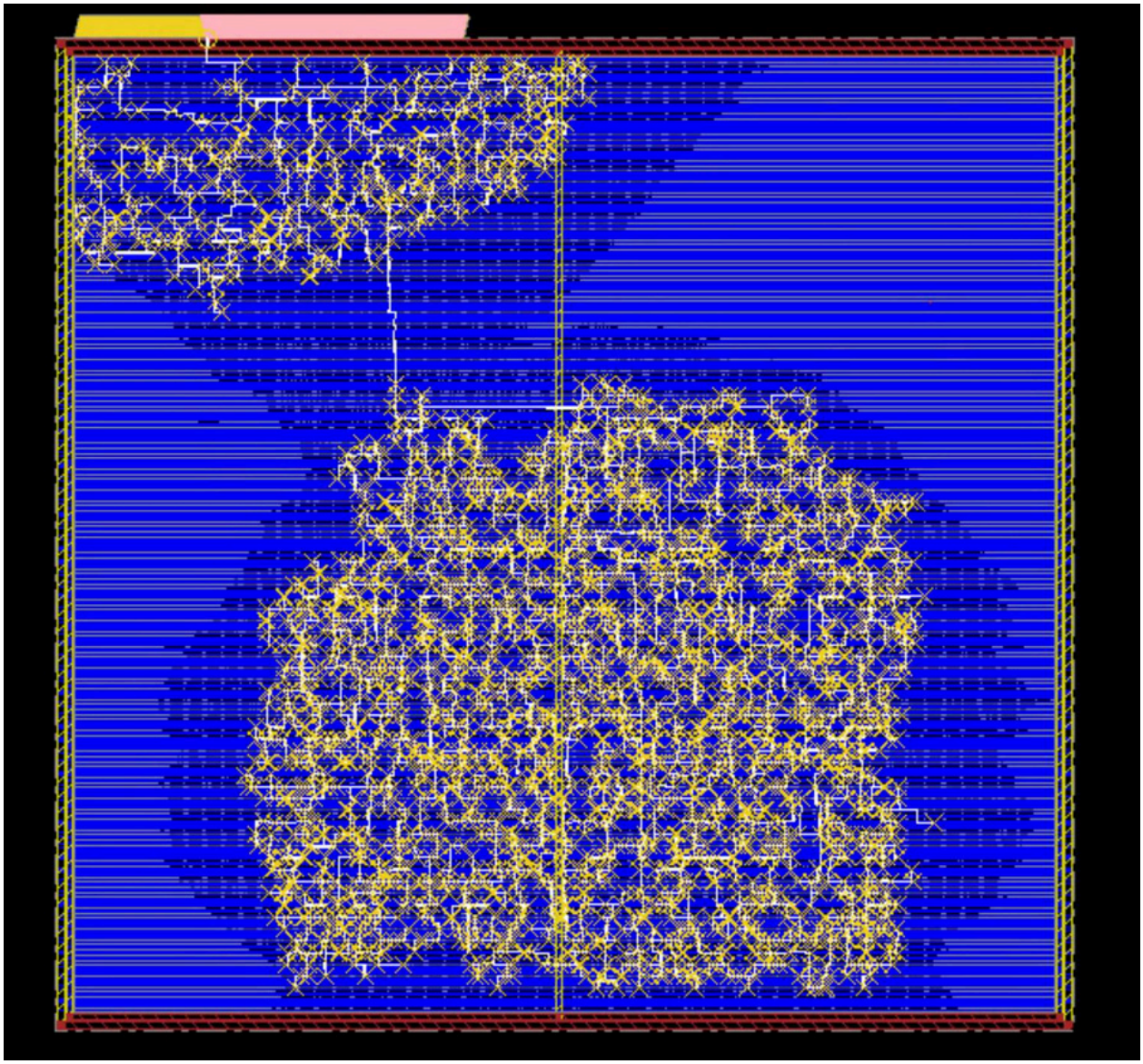
```
At time                   0, cipher = 00000000000000000000000000000000
Applying reset...
At time               25000, cipher = xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Starting Test 1: Apply given plaintext and key...
sub_bytes result = 6301c9af6f76faa4fe6b72f0677bad82
shift_rows result = 637672826f6badaffe7bc9a46701faf0
mix_cols result = ac9b6cbe61faaf3207ecfbf8c78082a9
sub_bytes result = 6f48abdddd089ecf6206dba73cc68cb4
shift_rows result = 6f08dbb4dd068cdd62c6abcf3c489ea7
mix_cols result = a9bd0d11fa83a457f1dca34e99b2a1c7
sub_bytes result = 3237c674bedd72f8549effa77542d7a8
shift_rows result = 32ddffa8be9ed7745442c6f8753772a7
mix_cols result = 4f21e93f7d8f097850799293662a548f
sub_bytes result = 6a08f8ba7439eac7e9e4bba4215622d3
shift_rows result = 6a39bbd374e422bae956f8c72108eaa4
mix_cols result = f71d5081477b01350c91061b14b011d2
sub_bytes result = 18127957c33d29cc2e4ecc17b4f28c45
shift_rows result = 183dcc45c34e8c572ef279ccb4122917
mix_cols result = fe686953948777 32e496617a7bfccdd2
sub_bytes result = e08daa7aae62c78b7c5e6fa2291ab330
shift_rows result = e0626f30ae5eb37a7c1aaa8b298dc7a2
mix_cols result = 22a50c566ca603f0f726af39bbd8cc6e
sub_bytes result = 2027539304c9d4bc2feeb53e96619a4a
shift_rows result = 20c9b54a04ee9a932f6153bc9627d43e
mix_cols result = ff27468828e56b4512a43720b481402e
sub_bytes result = ace712d9fdb4abe03a0715d87ea40a82
shift_rows result = acb41582fd070ad93aa412e07ee7abd8
mix_cols result = 1362af513b349eb871bf8123bd95a765
sub_bytes result = ad6906191281a1132e4442fac704c33c
shift_rows result = ad81423c1244c3192e040613c769a1fa
mix_cols result = a74eec5732dde083453f13567517e275
At time              145000, cipher = b66c53419d2ee111ddad151e29c98036
Ciphertext: b66c53419d2ee111ddad151e29c98036
Simulation complete via $finish(1) at time 1600 NS + 0
../testbench/AES_tb.v:60        $finish;
xcelium> SS
```

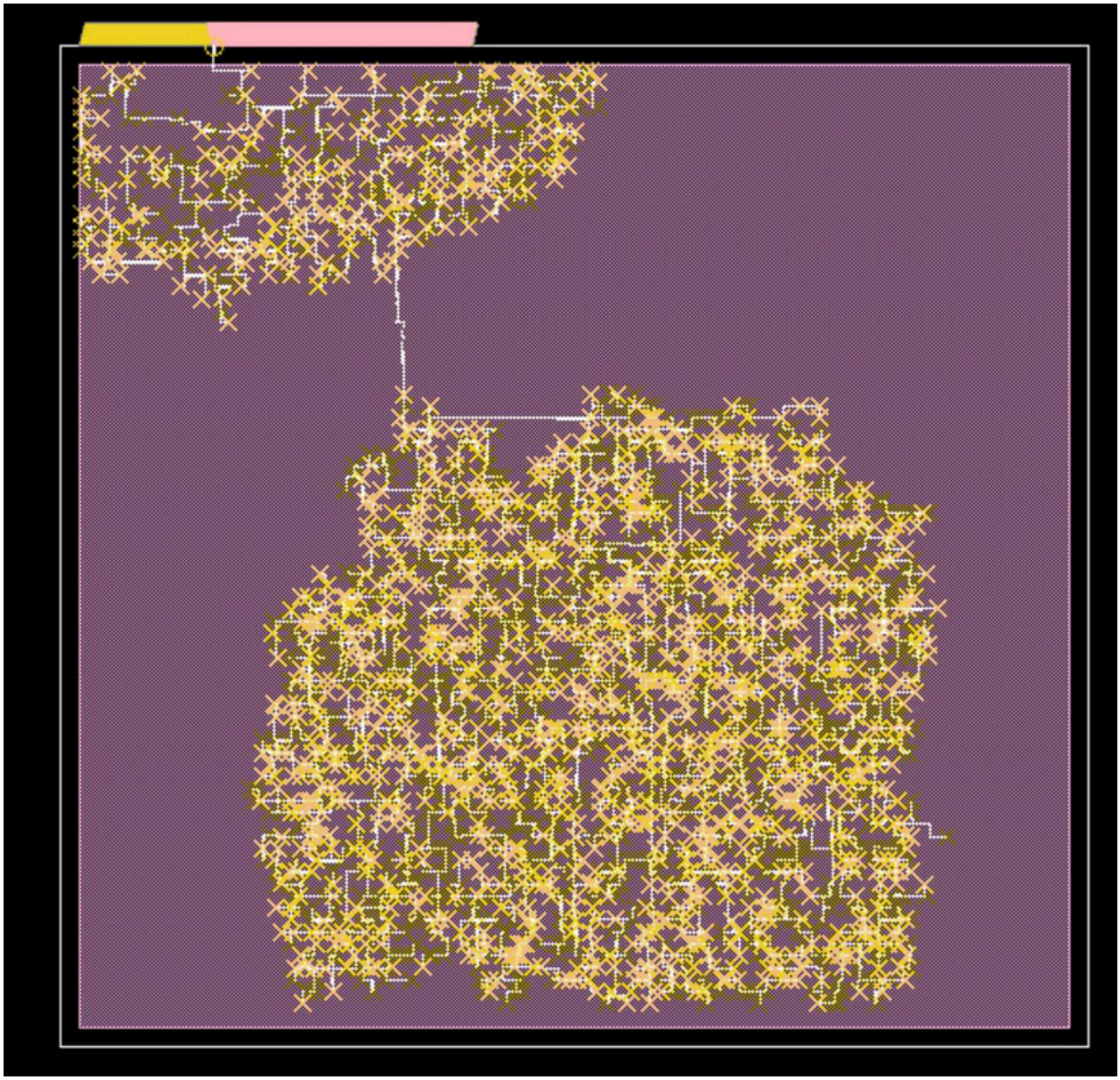
Layout Clock Tree debugger showing final clock tree

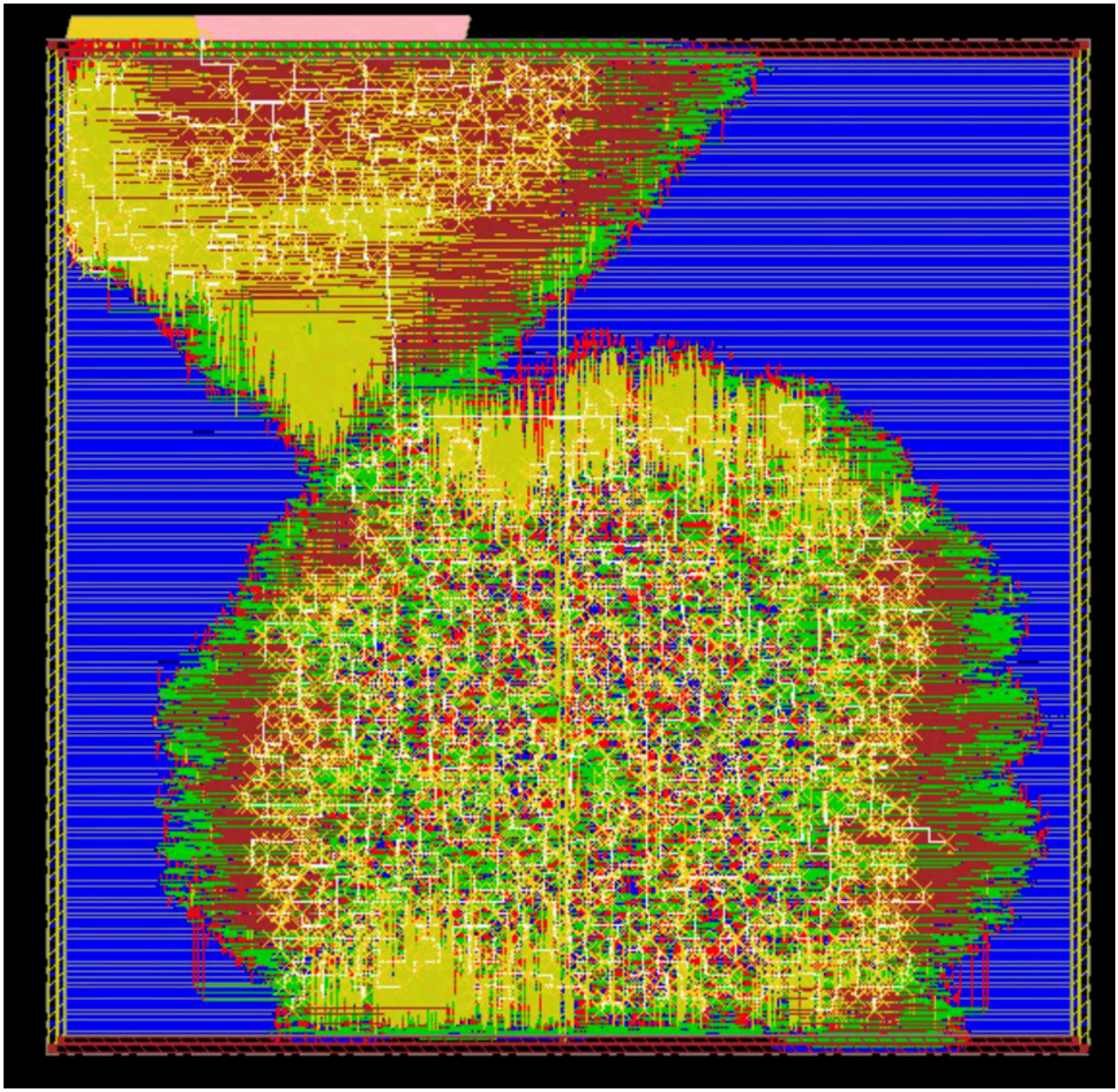


Layout

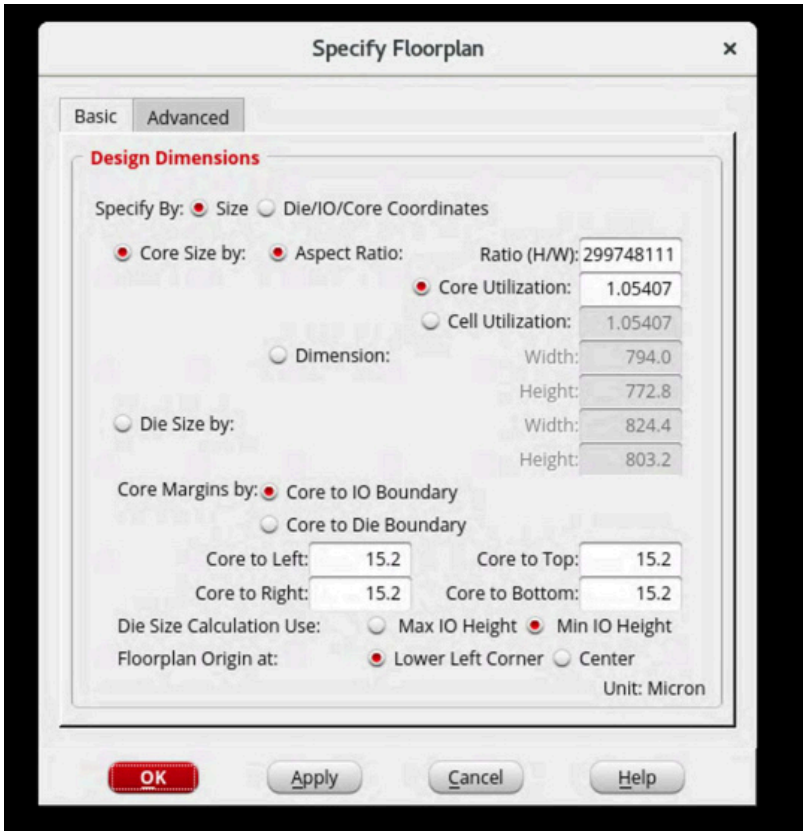








Given a slack of 7.838 ns when simulating with a 10 ns clock, the maximum minimum clock period is 10 - 7.838 = 2.162 ns. Thus, the maximum clock frequency is 1/period = **462.5346 MHz.**


Specify Floorplan
Basic
Advanced
Design Dimensions
Specify By: Size Die/IO/Core Coordinates
Core Size by: Aspect Ratio: Ratio (H/W): 299748111
Core Utilization: 1.05407
Cell Utilization: 1.05407
Dimension: Width: 794.0
Height: 772.8
Die Size by: Width: 824.4
Height: 803.2
Core Margins by: Core to IO Boundary
Core to Die Boundary
Core to Left: 15.2
Core to Top: 15.2
Core to Right: 15.2
Core to Bottom: 15.2
Die Size Calculation Use: Max IO Height Min IO Height
Floorplan Origin at: Lower Left Corner Center
Unit: Micron
OK
Apply
Cancel
Help