Lab 2 g13_SIG_CH_MAJ

Group 13

Yongru Pan 261001758

Chenyi Xu 260948311

Description of Circuit Function:

The entity name is **g13_SIG_CH_MAJ.** The purpose of this lab is to work on the essential building blocks for SHA 256 hashing functions used in Bitcoin mining. The Maj function outputs the bit (either 0 or 1) that appears most frequently among its three input bits. The Ch function acts as a selector between two inputs, outputting one of them based on the value of a third bit. It is essentially a 2-input multiplexer. SIG functions xored the three inputs.

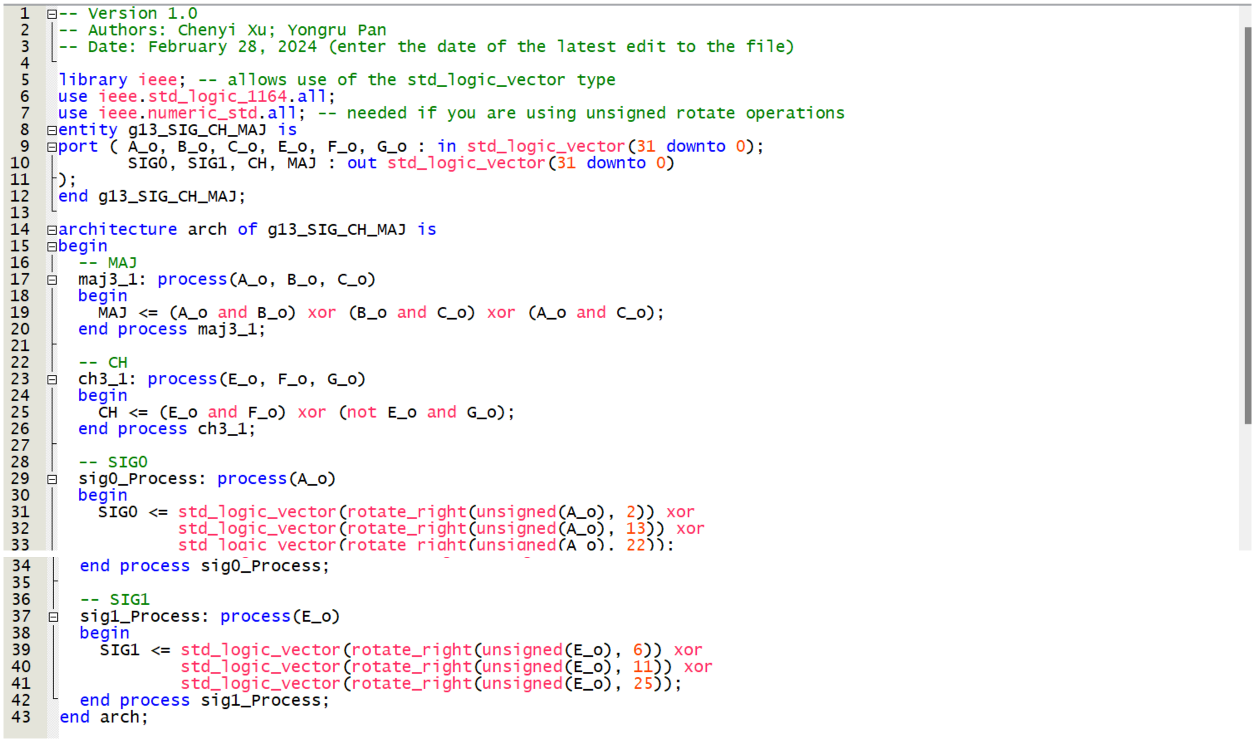
Inputs:

A_o: A 32-bit input signal (std_logic_vector of size 31 downto 0)
B_o: A 32-bit input signal (std_logic_vector of size 31 downto 0)
C_o: A 32-bit input signal (std_logic_vector of size 31 downto 0)
E_o: A 32-bit input signal (std_logic_vector of size 31 downto 0)
F_o: A 32-bit input signal (std_logic_vector of size 31 downto 0)
G_o: A 32-bit input signal (std_logic_vector of size 31 downto 0)

Outputs:

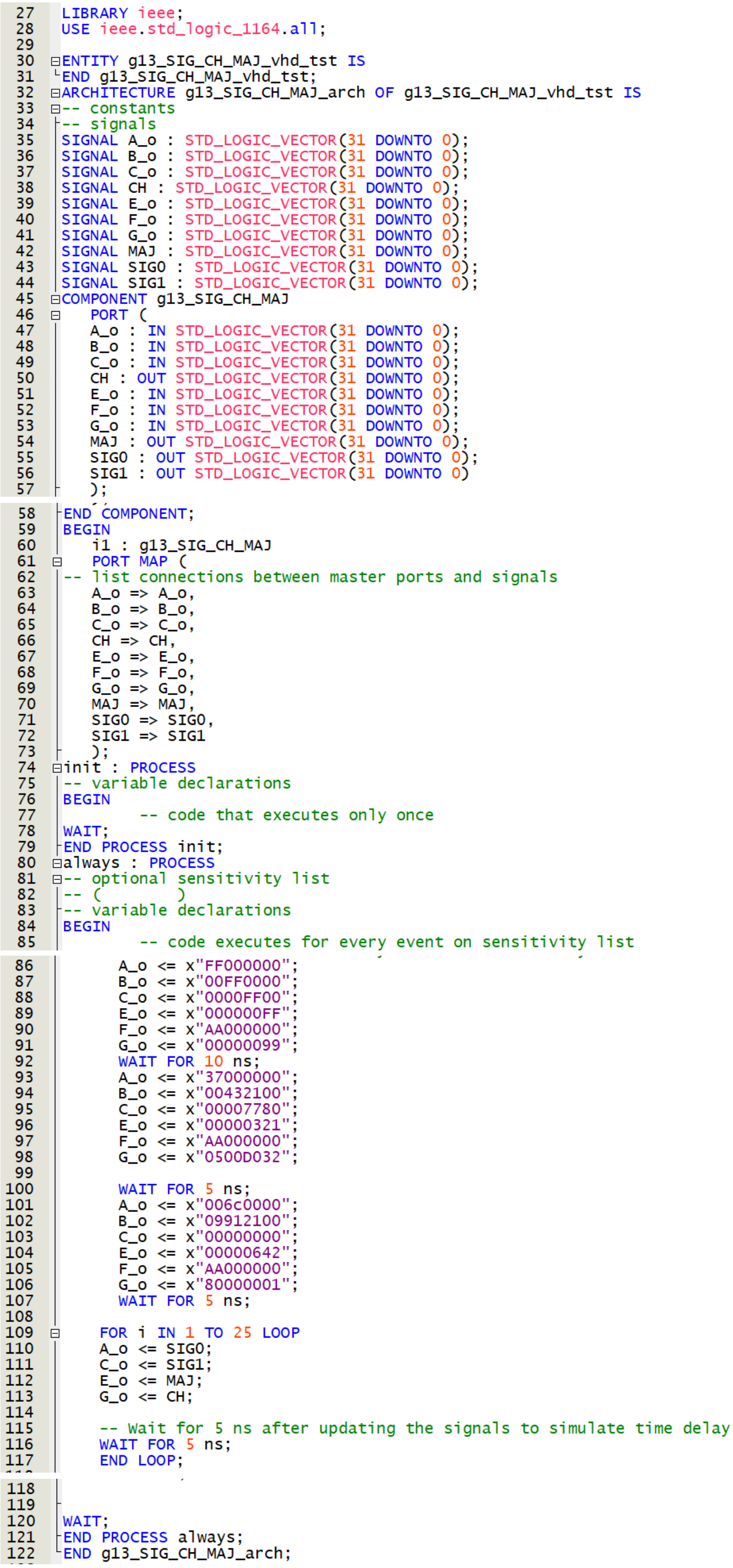
SIG0: A 32-bit output signal (std_logic_vector of size 31 downto 0)
SIG1: A 32-bit output signal (std_logic_vector of size 31 downto 0)
CH: A 32-bit output signal (std_logic_vector of size 31 downto 0)
MAJ: A 32-bit output signal (std_logic_vector of size 31 downto

VHDL Description of the Circuit



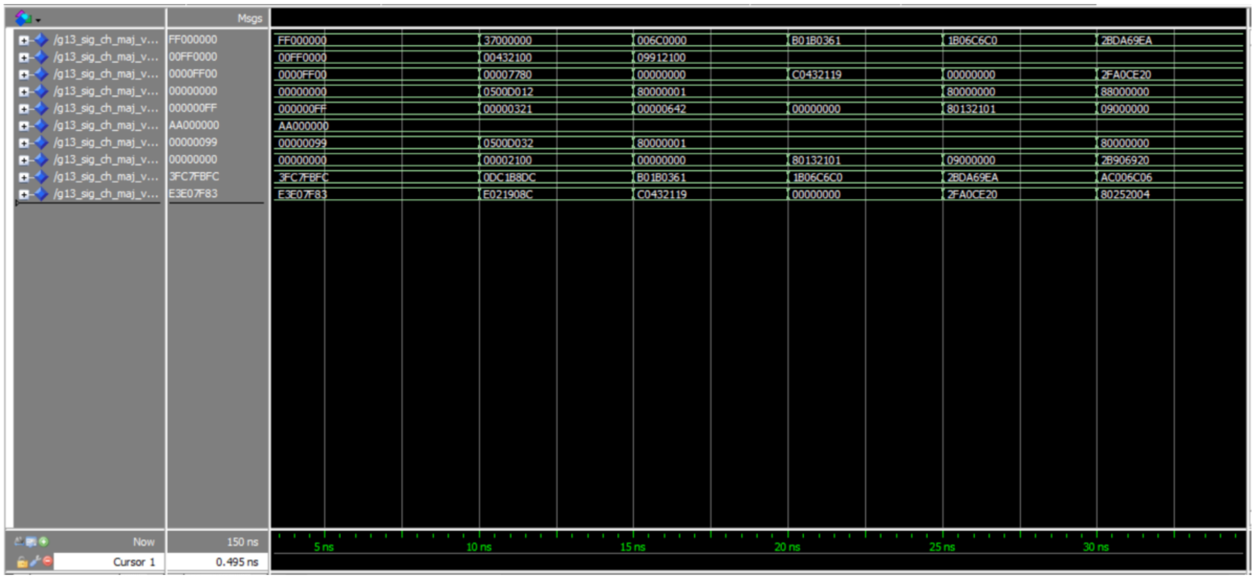
```
-- Version 1.0
-- Authors: Chenyi Xu; Yongru Pan
-- Date: February 28, 2024 (enter the date of the latest edit to the file)

library ieee; -- allows use of the std_logic_vector type
use ieee.std_logic_1164.all;
use ieee.numeric_std.all; -- needed if you are using unsigned rotate operations
entity g13_SIG_CH_MAJ is
port ( A_o, B_o, C_o, E_o, F_o, G_o : in std_logic_vector(31 downto 0);
       SIG0, SIG1, CH, MAJ : out std_logic_vector(31 downto 0)
);
end g13_SIG_CH_MAJ;

architecture arch of g13_SIG_CH_MAJ is
begin
  -- MAJ
  maj3_1: process(A_o, B_o, C_o)
  begin
    MAJ <= (A_o and B_o) xor (B_o and C_o) xor (A_o and C_o);
  end process maj3_1;

  -- CH
  ch3_1: process(E_o, F_o, G_o)
  begin
    CH <= (E_o and F_o) xor (not E_o and G_o);
  end process ch3_1;

  -- SIG0
  sig0_Process: process(A_o)
  begin
    SIG0 <= std_logic_vector(rotate_right(unsigned(A_o), 2)) xor
            std_logic_vector(rotate_right(unsigned(A_o), 13)) xor
            std_logic_vector(rotate_right(unsigned(A_o), 22));
  end process sig0_Process;

  -- SIG1
  sig1_Process: process(E_o)
  begin
    SIG1 <= std_logic_vector(rotate_right(unsigned(E_o), 6)) xor
            std_logic_vector(rotate_right(unsigned(E_o), 11)) xor
            std_logic_vector(rotate_right(unsigned(E_o), 25));
  end process sig1_Process;
end arch;
```

Final Version of Testbench File



```
LIBRARY ieee;
USE ieee.std_logic_1164.all;

ENTITY g13_SIG_CH_MAJ_vhd_tst IS
END g13_SIG_CH_MAJ_vhd_tst;
ARCHITECTURE g13_SIG_CH_MAJ_arch OF g13_SIG_CH_MAJ_vhd_tst IS
-- constants
-- signals
SIGNAL A_o : STD_LOGIC_VECTOR(31 DOWNTO 0);
SIGNAL B_o : STD_LOGIC_VECTOR(31 DOWNTO 0);
SIGNAL C_o : STD_LOGIC_VECTOR(31 DOWNTO 0);
SIGNAL CH : STD_LOGIC_VECTOR(31 DOWNTO 0);
SIGNAL E_o : STD_LOGIC_VECTOR(31 DOWNTO 0);
SIGNAL F_o : STD_LOGIC_VECTOR(31 DOWNTO 0);
SIGNAL G_o : STD_LOGIC_VECTOR(31 DOWNTO 0);
SIGNAL MAJ : STD_LOGIC_VECTOR(31 DOWNTO 0);
SIGNAL SIG0 : STD_LOGIC_VECTOR(31 DOWNTO 0);
SIGNAL SIG1 : STD_LOGIC_VECTOR(31 DOWNTO 0);
COMPONENT g13_SIG_CH_MAJ
    PORT (
    A_o : IN STD_LOGIC_VECTOR(31 DOWNTO 0);
    B_o : IN STD_LOGIC_VECTOR(31 DOWNTO 0);
    C_o : IN STD_LOGIC_VECTOR(31 DOWNTO 0);
    CH : OUT STD_LOGIC_VECTOR(31 DOWNTO 0);
    E_o : IN STD_LOGIC_VECTOR(31 DOWNTO 0);
    F_o : IN STD_LOGIC_VECTOR(31 DOWNTO 0);
    G_o : IN STD_LOGIC_VECTOR(31 DOWNTO 0);
    MAJ : OUT STD_LOGIC_VECTOR(31 DOWNTO 0);
    SIG0 : OUT STD_LOGIC_VECTOR(31 DOWNTO 0);
    SIG1 : OUT STD_LOGIC_VECTOR(31 DOWNTO 0)
    );
END COMPONENT;
BEGIN
    i1 : g13_SIG_CH_MAJ
    PORT MAP (
-- list connections between master ports and signals
    A_o => A_o,
    B_o => B_o,
    C_o => C_o,
    CH => CH,
    E_o => E_o,
    F_o => F_o,
    G_o => G_o,
    MAJ => MAJ,
    SIG0 => SIG0,
    SIG1 => SIG1
    );
init : PROCESS
-- variable declarations
BEGIN
        -- code that executes only once
WAIT;
END PROCESS init;
always : PROCESS
-- optional sensitivity list
-- (        )
-- variable declarations
BEGIN
        -- code executes for every event on sensitivity list
      A_o <= x"FF000000";
      B_o <= x"00FF0000";
      C_o <= x"0000FF00";
      E_o <= x"000000FF";
      F_o <= x"AA000000";
      G_o <= x"00000099";
      WAIT FOR 10 ns;
      A_o <= x"37000000";
      B_o <= x"00432100";
      C_o <= x"00007780";
      E_o <= x"00000321";
      F_o <= x"AA000000";
      G_o <= x"0500D032";

      WAIT FOR 5 ns;
      A_o <= x"006c0000";
      B_o <= x"09912100";
      C_o <= x"00000000";
      E_o <= x"00000642";
      F_o <= x"AA000000";
      G_o <= x"80000001";
      WAIT FOR 5 ns;

    FOR i IN 1 TO 25 LOOP
    A_o <= SIG0;
    C_o <= SIG1;
    E_o <= MAJ;
    G_o <= CH;

    -- Wait for 5 ns after updating the signals to simulate time delay
    WAIT FOR 5 ns;
    END LOOP;


WAIT;
END PROCESS always;
END g13_SIG_CH_MAJ_arch;
```

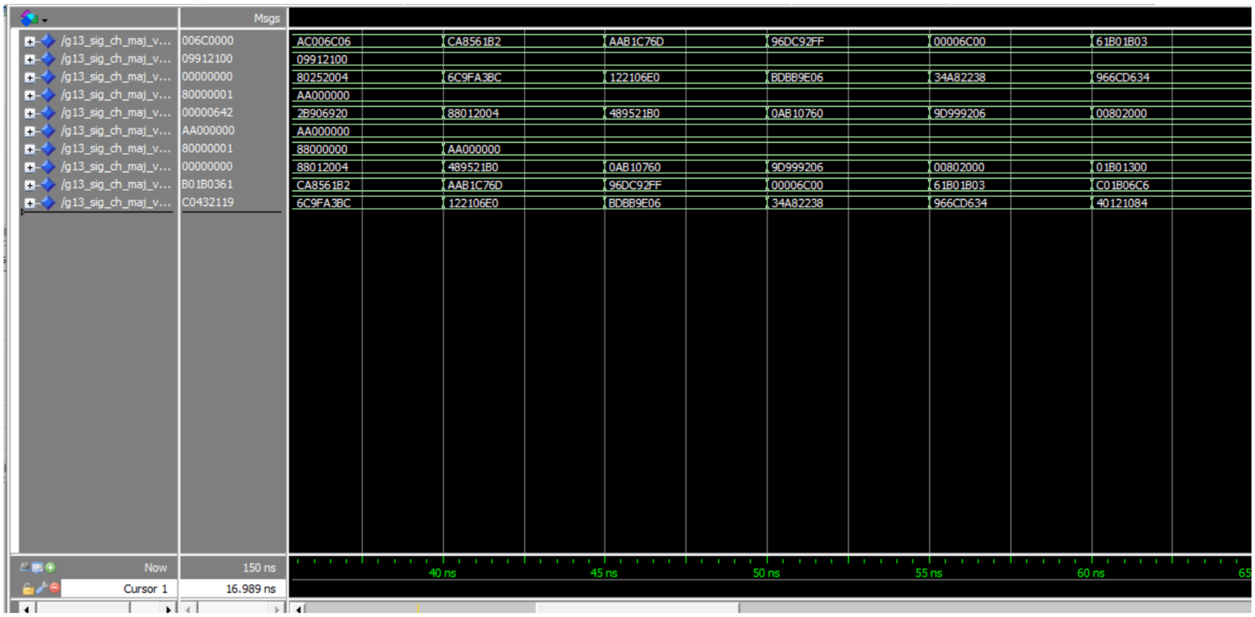
Screenshots of the simulation results for the final simulation run



	Msgs						
/g13_sig_ch_maj_v...	FF000000	FF000000	37000000	006C0000	B01B0361	1B06C6C0	2BDA69EA
/g13_sig_ch_maj_v...	00FF0000	00FF0000	00432100	09912100			
/g13_sig_ch_maj_v...	0000FF00	0000FF00	00007780	00000000	C0432119	00000000	2FA0CE20
/g13_sig_ch_maj_v...	00000000	00000000	0500D012	80000001		80000000	88000000
/g13_sig_ch_maj_v...	000000FF	000000FF	00000321	00000642	00000000	80132101	09000000
/g13_sig_ch_maj_v...	AA000000	AA000000					
/g13_sig_ch_maj_v...	00000099	00000099	0500D032	80000001			80000000
/g13_sig_ch_maj_v...	00000000	00000000	00002100	00000000	80132101	09000000	2B906920
/g13_sig_ch_maj_v...	3FC7FBFC	3FC7FBFC	0DC1B8DC	B01B0361	1B06C6C0	2BDA69EA	AC006C06
/g13_sig_ch_maj_v...	E3E07F83	E3E07F83	E021908C	C0432119	00000000	2FA0CE20	80252004

Now 150 ns

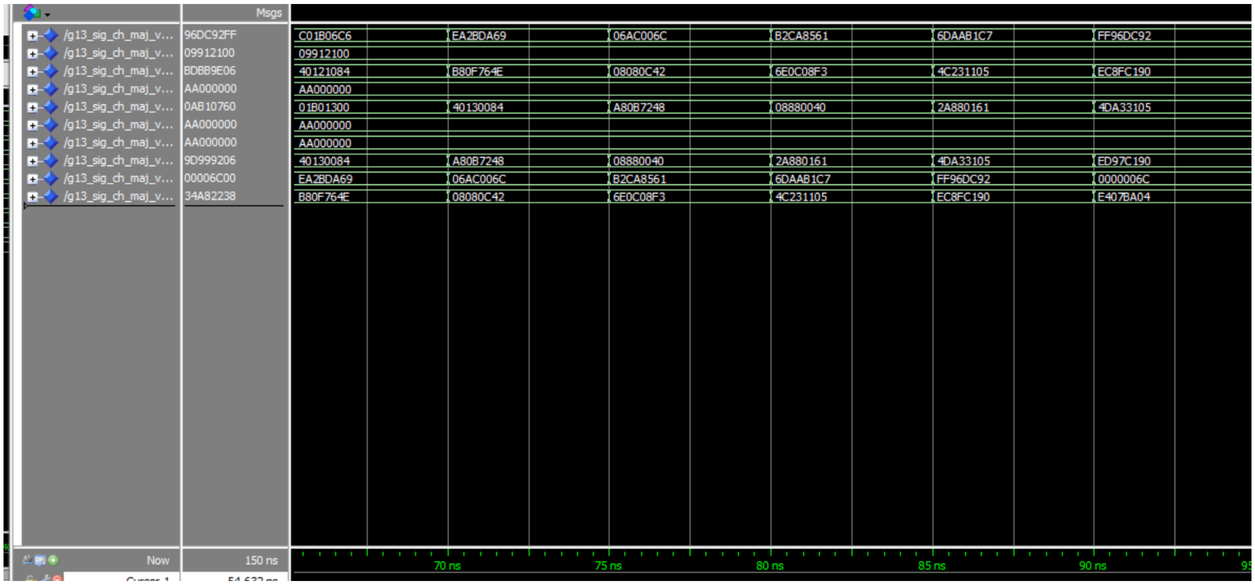
Cursor 1 0.495 ns

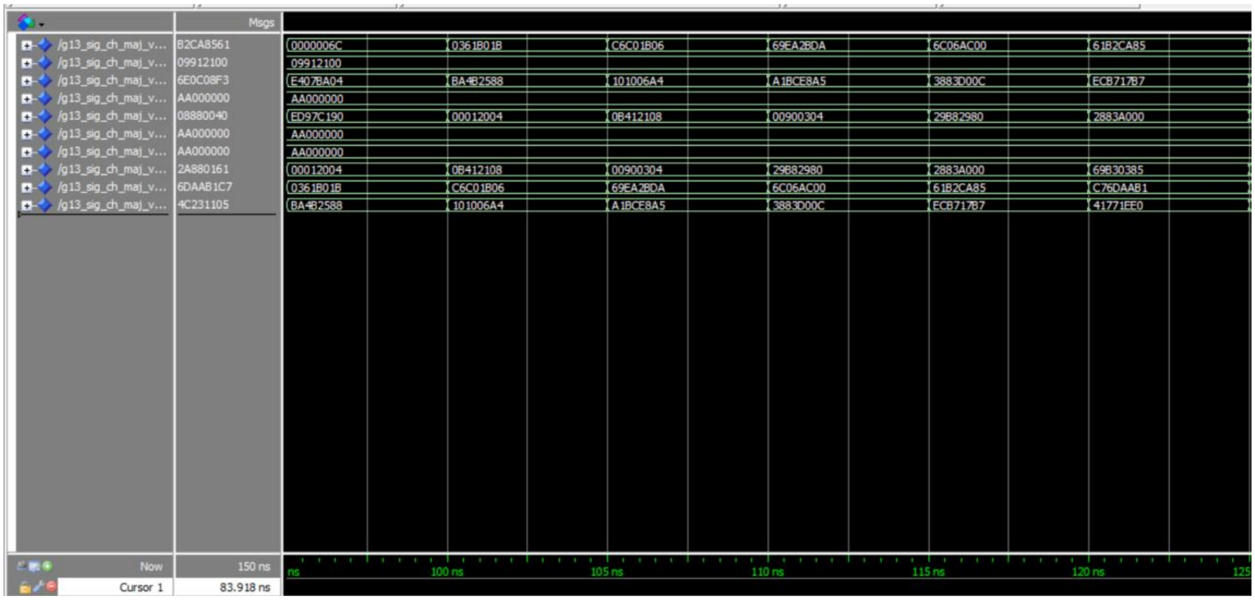


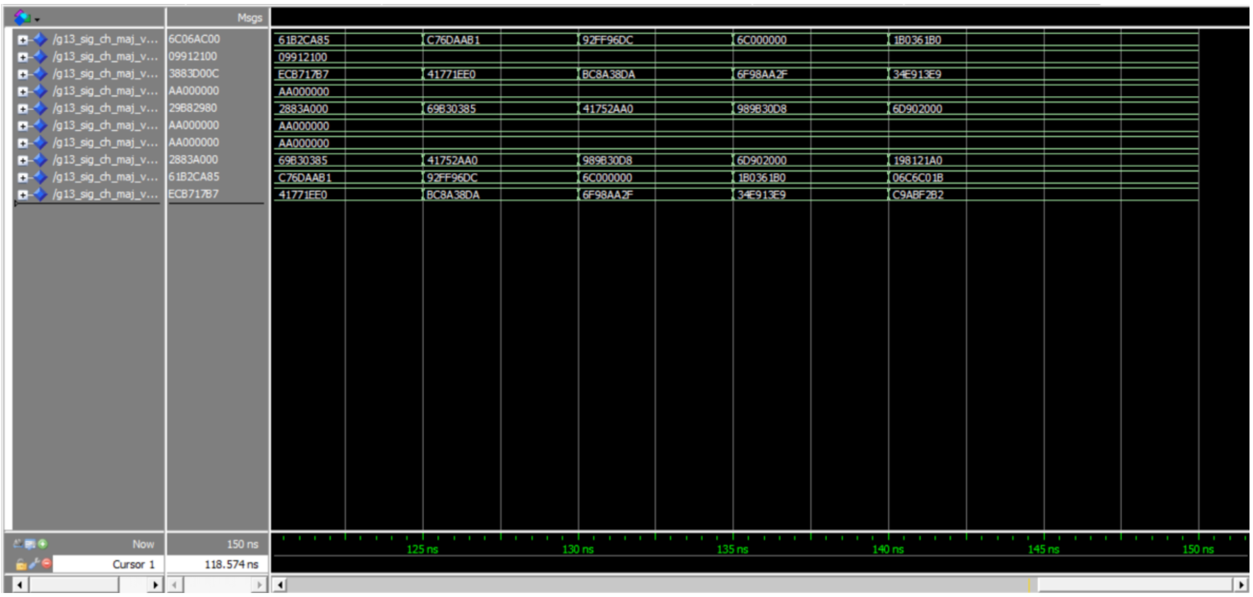
	Msgs						
/g13_sig_ch_maj_v...	006C0000	AC006C06	CA8561B2	AAB1C76D	96DC92FF	00006C00	61B01B03
/g13_sig_ch_maj_v...	09912100	09912100					
/g13_sig_ch_maj_v...	00000000	80252004	6C9FA3BC	122106E0	BDBB9E06	34A82238	966CD634
/g13_sig_ch_maj_v...	80000001	AA000000					
/g13_sig_ch_maj_v...	00000642	2B906920	88012004	489521B0	0AB10760	9D999206	00802000
/g13_sig_ch_maj_v...	AA000000	AA000000					
/g13_sig_ch_maj_v...	80000001	88000000	AA000000				
/g13_sig_ch_maj_v...	00000000	88012004	489521B0	0AB10760	9D999206	00802000	01B01300
/g13_sig_ch_maj_v...	B01B0361	CA8561B2	AAB1C76D	96DC92FF	00006C00	61B01B03	C01B06C6
/g13_sig_ch_maj_v...	C0432119	6C9FA3BC	122106E0	BDBB9E06	34A82238	966CD634	40121084

Now 150 ns

Cursor 1 16.989 ns


Msgs
/g13_sig_ch_maj_v... 96DC92FF
/g13_sig_ch_maj_v... 09912100
/g13_sig_ch_maj_v... BDBB9E06
/g13_sig_ch_maj_v... AA000000
/g13_sig_ch_maj_v... 0AB10760
/g13_sig_ch_maj_v... AA000000
/g13_sig_ch_maj_v... AA000000
/g13_sig_ch_maj_v... 9D999206
/g13_sig_ch_maj_v... 00006C00
/g13_sig_ch_maj_v... 34A82238
C01B06C6 EA2BDA69 06AC006C B2CA8561 6DAAB1C7 FF96DC92
09912100
40121084 B80F764E 08080C42 6E0C08F3 4C231105 EC8FC190
AA000000
01B01300 40130084 A80B7248 08880040 2A880161 4DA33105
AA000000
AA000000
40130084 A80B7248 08880040 2A880161 4DA33105 ED97C190
EA2BDA69 06AC006C B2CA8561 6DAAB1C7 FF96DC92 0000006C
B80F764E 08080C42 6E0C08F3 4C231105 EC8FC190 E407BA04
Now 150 ns
Cursor 1 54.632 ns
70 ns
75 ns
80 ns
85 ns
90 ns
95


Msgs
/g13_sig_ch_maj_v... B2CA8561
/g13_sig_ch_maj_v... 09912100
/g13_sig_ch_maj_v... 6E0C08F3
/g13_sig_ch_maj_v... AA000000
/g13_sig_ch_maj_v... 08880040
/g13_sig_ch_maj_v... AA000000
/g13_sig_ch_maj_v... AA000000
/g13_sig_ch_maj_v... 2A880161
/g13_sig_ch_maj_v... 6DAAB1C7
/g13_sig_ch_maj_v... 4C231105
0000006C 0361B01B C6C01B06 69EA2BDA 6C06AC00 61B2CA85
09912100
E407BA04 BA4B2588 101006A4 A1BCE8A5 3883D00C ECB717B7
AA000000
ED97C190 00012004 0B412108 00900304 29B82980 2883A000
AA000000
AA000000
00012004 0B412108 00900304 29B82980 2883A000 69B30385
0361B01B C6C01B06 69EA2BDA 6C06AC00 61B2CA85 C76DAAB1
BA4B2588 101006A4 A1BCE8A5 3883D00C ECB717B7 41771EE0
Now 150 ns
Cursor 1 83.918 ns
ns
100 ns
105 ns
110 ns
115 ns
120 ns
125



	Msgs					
/g13_sig_ch_maj_v...	6C06AC00	61B2CA85	C76DAAB1	92FF96DC	6C000000	1B0361B0
/g13_sig_ch_maj_v...	09912100	09912100				
/g13_sig_ch_maj_v...	3883D00C	ECB717B7	41771EE0	BC8A38DA	6F98AA2F	34E913E9
/g13_sig_ch_maj_v...	AA000000	AA000000				
/g13_sig_ch_maj_v...	29B82980	2883A000	69B30385	41752AA0	989B30D8	6D902000
/g13_sig_ch_maj_v...	AA000000	AA000000				
/g13_sig_ch_maj_v...	AA000000	AA000000				
/g13_sig_ch_maj_v...	2883A000	69B30385	41752AA0	989B30D8	6D902000	198121A0
/g13_sig_ch_maj_v...	61B2CA85	C76DAAB1	92FF96DC	6C000000	1B0361B0	06C6C01B
/g13_sig_ch_maj_v...	ECB717B7	41771EE0	BC8A38DA	6F98AA2F	34E913E9	C9ABF2B2

Now	150 ns	
Cursor 1	118.574 ns	