ECSE 325 Lab 3 Report

Group 06

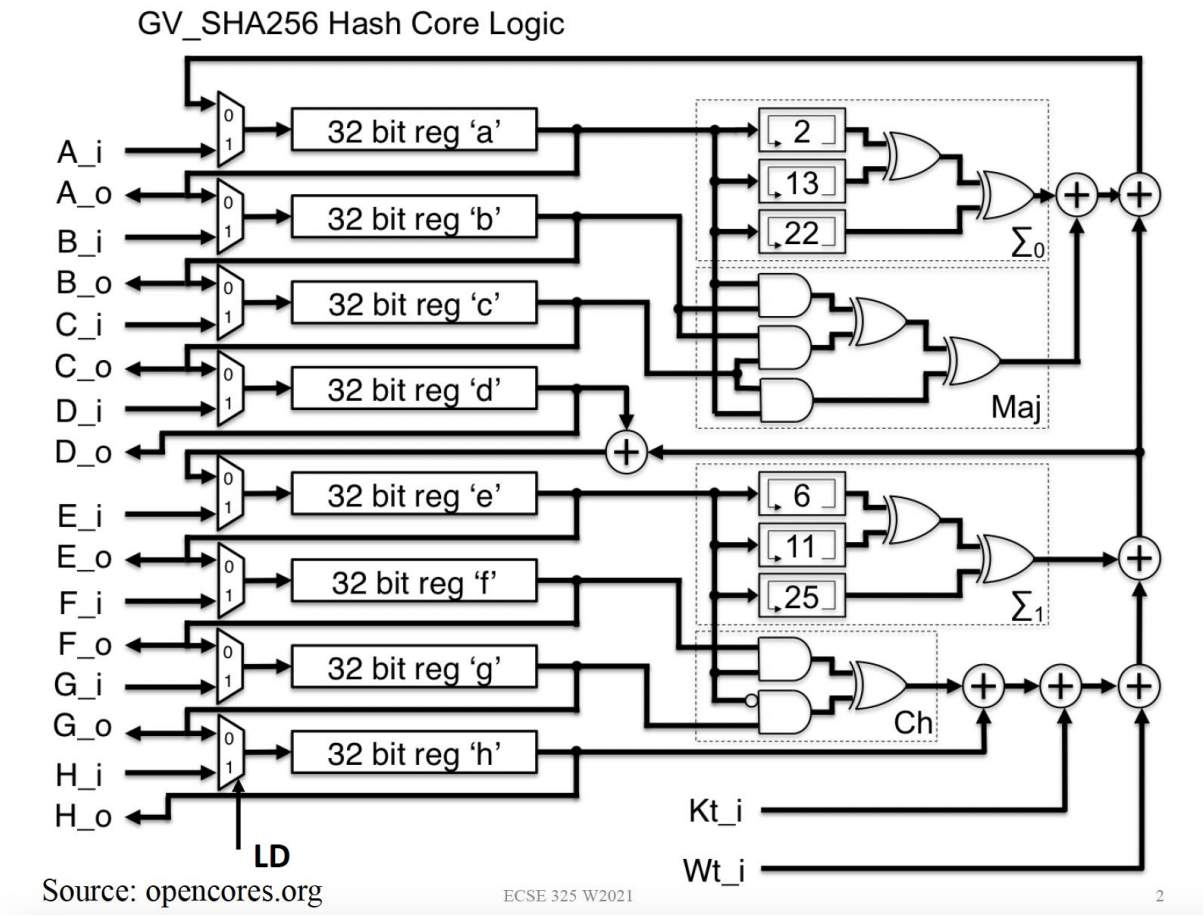
Adrian Wang	260769387
Irene Ma	260776283
Xiangyun Wang	260771591

1. Circuit Function Description

This circuit describes and analyses the remaining parts of the Hash Core Logic. The 2 to 1 multiplexers A, B, C with A_i, B_i, C_i are connected to registers A, B, C. Register A is connected to the SIG0 operation and B, C are connected to the MAJ operation. The 2 to 1 multiplexers E, F, G with E_i, F_i, G_i are connected to registers E, F, G. Register E is connected to SIG1 operation and E, F are connected to the CH operation. The output of SIG0, MAJ, register D, SIG1, CH, Kt_i, Wt_i and register H are summed together as a_0. The output of SIG1, CH, register D, register H and Kt_i, Wt_i are summed together as e_0. The next register state is updated according to LD. next_A <= unsigned(A_i) when LD = '1' else a_0; next_E <= unsigned(E_i) when LD = '1' else e_0; next_B <= unsigned(B_i) when LD = '1' else reg_A; and etc.

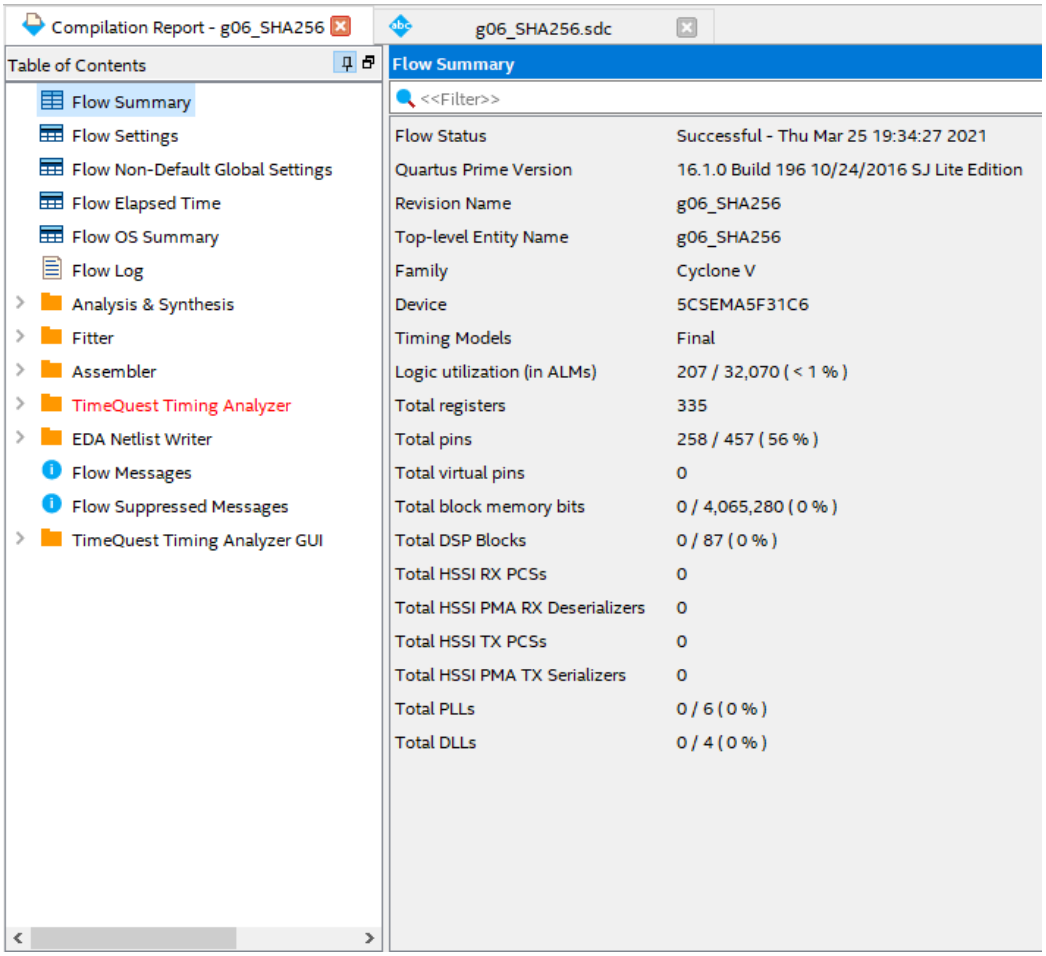
List of inputs: A_o, B_o, C_o, D_o, E_o, F_o, G_o, H_o
A_i, B_i, C_i, D_i, E_i, F_i, G_i, H_i
Kt_i, Wt_i
LD, CLK

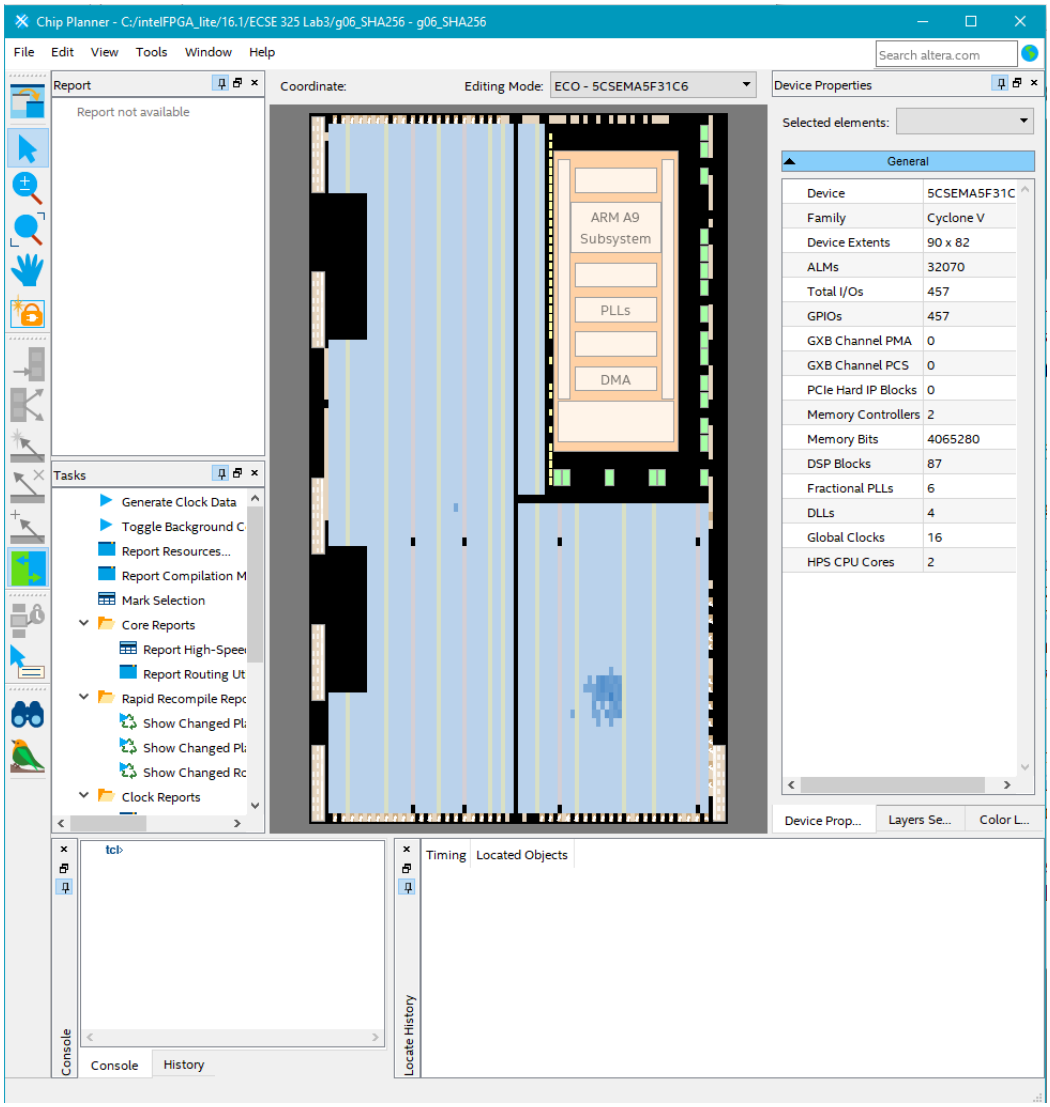
List of outputs: A_o, B_o, C_o, D_o, E_o, F_o, G_o, H_o



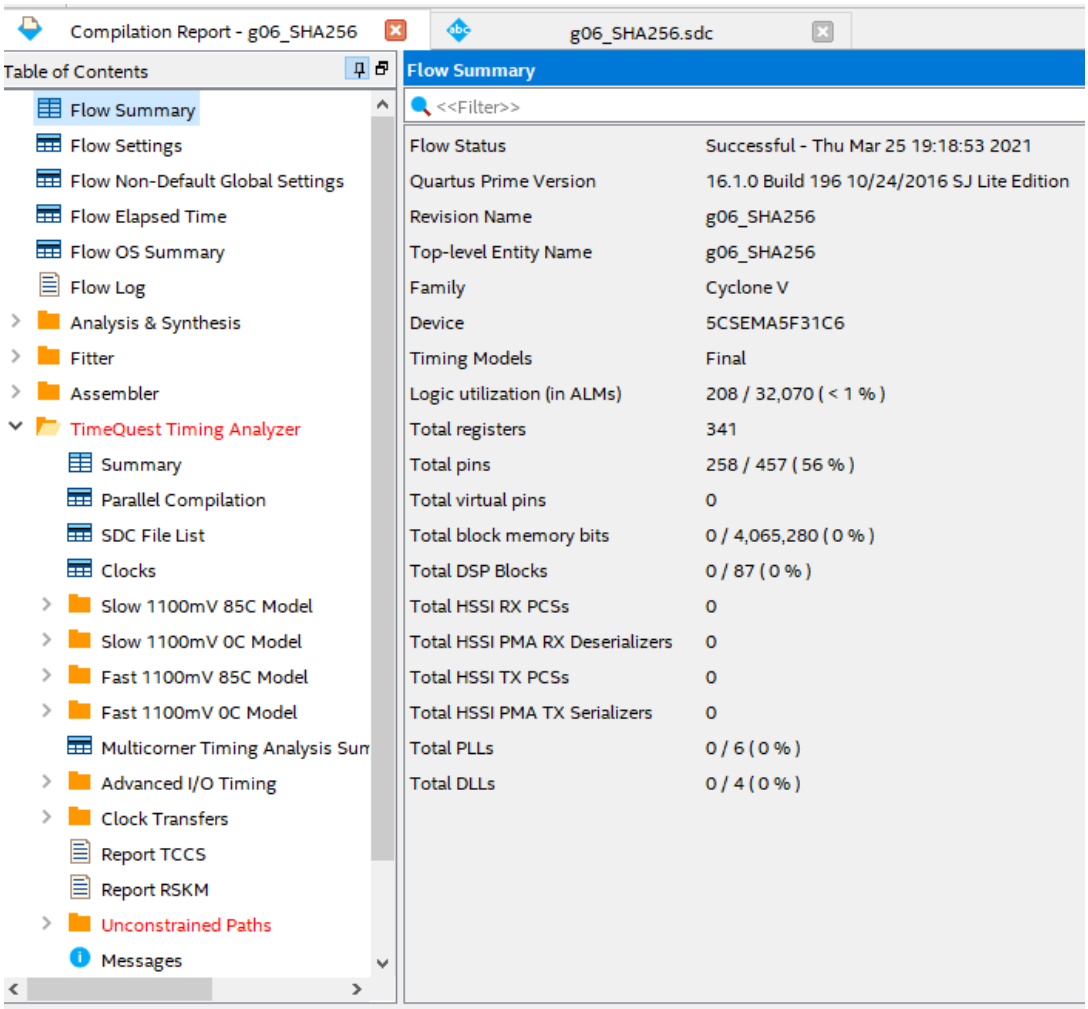
2. Flow Summary and Chip Planner Layout

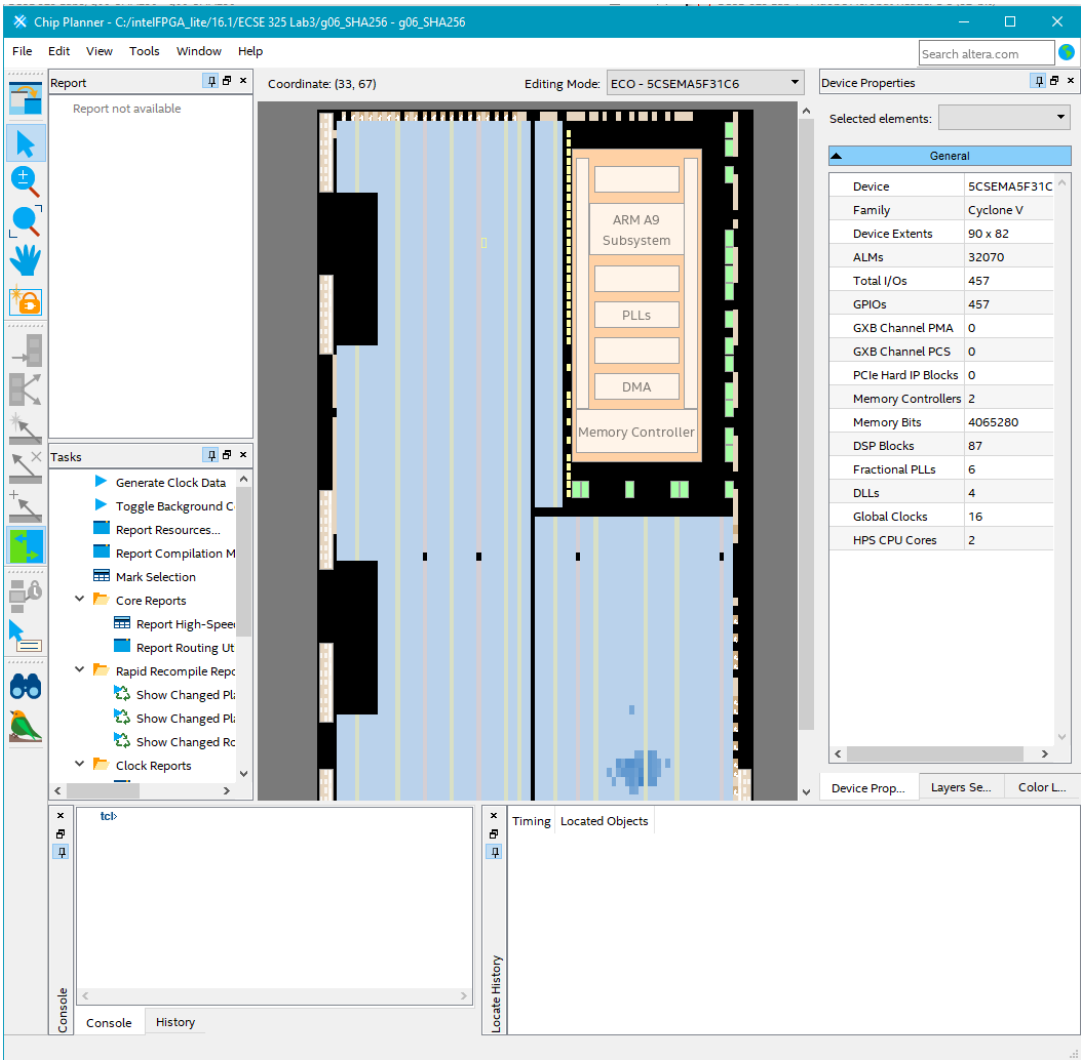
2.1. Compilation result with 6 ns period


Compilation Report - g06_SHA256
g06_SHA256.sdc
Table of Contents
Flow Summary
Flow Settings
Flow Non-Default Global Settings
Flow Elapsed Time
Flow OS Summary
Flow Log
Analysis & Synthesis
Fitter
Assembler
TimeQuest Timing Analyzer
EDA Netlist Writer
Flow Messages
Flow Suppressed Messages
TimeQuest Timing Analyzer GUI
Flow Summary
<<Filter>>
Flow Status Successful - Thu Mar 25 19:34:27 2021
Quartus Prime Version 16.1.0 Build 196 10/24/2016 SJ Lite Edition
Revision Name g06_SHA256
Top-level Entity Name g06_SHA256
Family Cyclone V
Device 5CSEMA5F31C6
Timing Models Final
Logic utilization (in ALMs) 207 / 32,070 (< 1 %)
Total registers 335
Total pins 258 / 457 (56 %)
Total virtual pins 0
Total block memory bits 0 / 4,065,280 (0 %)
Total DSP Blocks 0 / 87 (0 %)
Total HSSI RX PCSs 0
Total HSSI PMA RX Deserializers 0
Total HSSI TX PCSs 0
Total HSSI PMA TX Serializers 0
Total PLLs 0 / 6 (0 %)
Total DLLs 0 / 4 (0 %)



2.2. Compilation result with 8 ns period


Compilation Report - g06_SHA256
g06_SHA256.sdc
Table of Contents
Flow Summary
Flow Settings
Flow Non-Default Global Settings
Flow Elapsed Time
Flow OS Summary
Flow Log
Analysis & Synthesis
Fitter
Assembler
TimeQuest Timing Analyzer
Summary
Parallel Compilation
SDC File List
Clocks
Slow 1100mV 85C Model
Slow 1100mV 0C Model
Fast 1100mV 85C Model
Fast 1100mV 0C Model
Multicorner Timing Analysis Sum
Advanced I/O Timing
Clock Transfers
Report TCCS
Report RSKM
Unconstrained Paths
Messages
Flow Summary
<<Filter>>
Flow Status Successful - Thu Mar 25 19:18:53 2021
Quartus Prime Version 16.1.0 Build 196 10/24/2016 SJ Lite Edition
Revision Name g06_SHA256
Top-level Entity Name g06_SHA256
Family Cyclone V
Device 5CSEMA5F31C6
Timing Models Final
Logic utilization (in ALMs) 208 / 32,070 (< 1 %)
Total registers 341
Total pins 258 / 457 (56 %)
Total virtual pins 0
Total block memory bits 0 / 4,065,280 (0 %)
Total DSP Blocks 0 / 87 (0 %)
Total HSSI RX PCSs 0
Total HSSI PMA RX Deserializers 0
Total HSSI TX PCSs 0
Total HSSI PMA TX Serializers 0
Total PLLs 0 / 6 (0 %)
Total DLLs 0 / 4 (0 %)



3. Timing analyses Summary

When setting the clock period at 6 ns, as shown in the figure below, two slow models did not pass. The worst-case setup time slack happens with the slow 1100 mV 0C Model which is -1.252. The other timing analyses results are filled in the figure below.

- Slow 1100mV 85C Model
- Slow 1100mV 0C Model
- Fast 1100mV 85C Model
- Fast 1100mV 0C Model

Requested ***Fmax*** = ___166 MHz_____

Fast 1100mV 0C Model ***Hold*** Slack Value = 0.125

Slow 1100mV 85C Model ***Setup*** Slack Value = -1.070

Slow 1100mV 85C Model ***Fmax*** = 141.44 MHz

The worst failing paths are listed in the figure below.

Timing Closure Recommendations

Summary [hide details]

This design contains failing setup paths with a worst-case slack of -1.070 ns. Run Report Timing Closure Recommendations for recommendations on how to close setup timing. For recommendations for any particular path, click the appropriate link in the table below.

Top Failing Paths [hide details]

	Slack	From	To	Recommendations
1	-1.070	g06_Hash_Core:i1|reg_H[0]	g06_Hash_Core:i1|reg_A[29]	Report recommendations for this path
2	-1.066	g06_Hash_Core:i1|reg_H[0]	g06_Hash_Core:i1|..._A[29]~DUPLICATE	Report recommendations for this path
3	-1.045	g06_Hash_Core:i1|reg_H[2]	g06_Hash_Core:i1|reg_A[29]	Report recommendations for this path
4	-1.041	g06_Hash_Core:i1|reg_H[2]	g06_Hash_Core:i1|..._A[29]~DUPLICATE	Report recommendations for this path
5	-1.034	g06_Hash_Core:i1|reg_H[0]	g06_Hash_Core:i1|reg_A[29]	Report recommendations for this path

At the beginning, the worst-case slack is even as low as -40, and the code is optimized by defining more temp signals and separating the additions. This is because the codes outside the process happen concurrently, and multilayers of addition or multiplication could add timing delay a lot. By avoiding additional dependencies in the code logic, the maximum parallelism can be ensured and when the constraint is loosening a little, all tests are expected to pass.

When the clock period is set to 8 ns, all models pass, and the critical information is filled in the figure below.

Requested ***Fmax*** = ___125 MHz_____

Fast 1100mV 0C Model ***Hold*** Slack Value = 0.123

Slow 1100mV 85C Model ***Setup*** Slack Value = 0.655

Slow 1100mV 85C Model ***Fmax*** = 136.15 MHz

4. Further Discussion about Hashes

The maximum clock rate achieved in the simulation is 136.15 MHz Since a 256-bit hash is created every 65 clock cycles, there are about 136.15 MHz / 65 = 2E6 hashes performed per second. For a single core the logic utilization is 208/32070 as shown in the flow summary before. This means that in theory, we could put around 32070/208 = 154 cores onto the FPGA. Assuming all of them could run at the same maximum clock rate, the total number of 308E6

hashes per second could be achieved with this FPGA. However, we should also notice that with only one core, the total pins utilization is already more than 50%. Besides, considering the physical and timing constraints such as memory of the FPGA, it is very unlikely that this number could be reached.