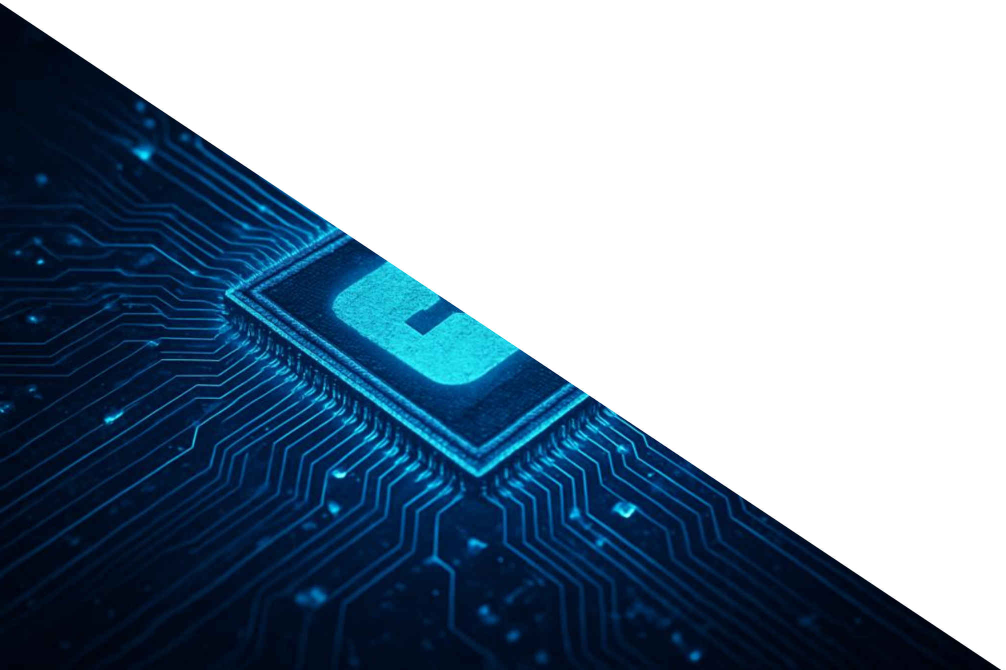
Design of Chip Security

Lab03 Report



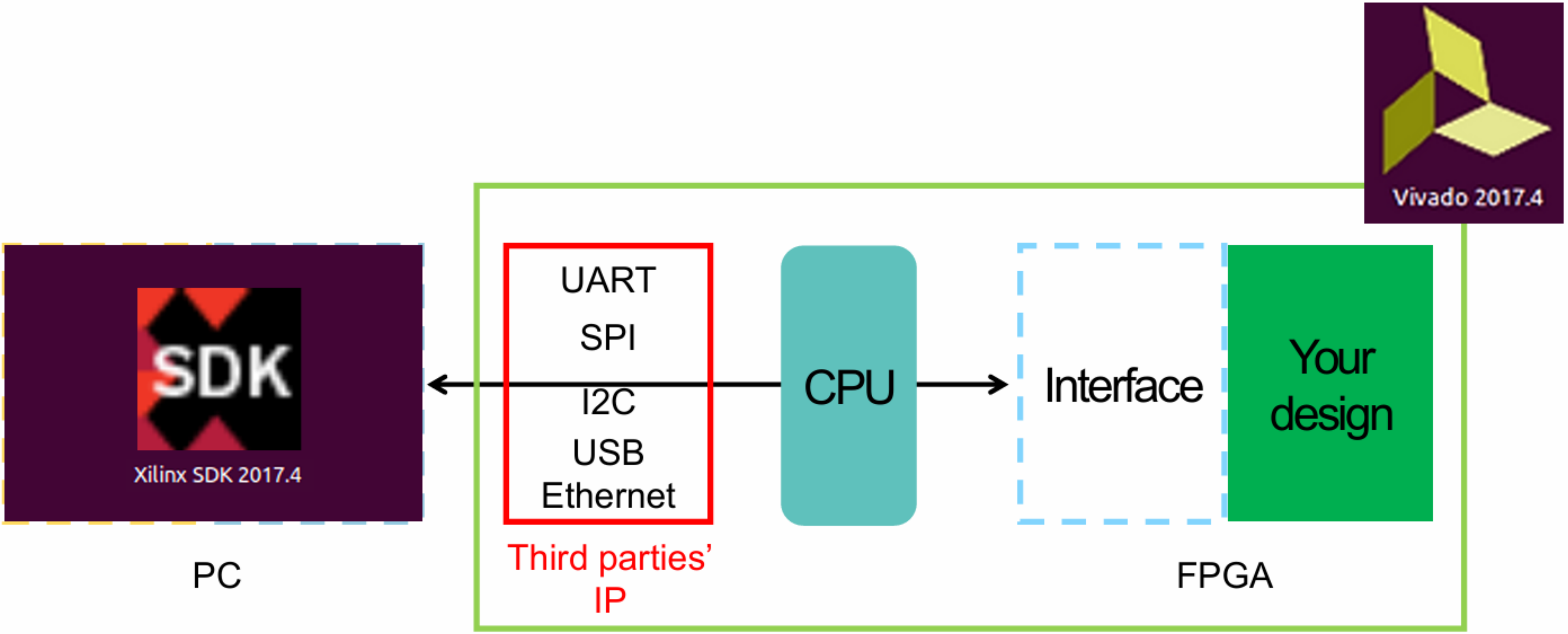
Name: 王品然

Student ID: 113063572

Outline

- Overview
- Pack sha2 into an AXI IP
- Build CPU system with packed IP
- Synthesis and implementation
- C program in SDK
- Result
- Review

Overview


Vivado 2017.4
SDK
Xilinx SDK 2017.4
UART
SPI
I2C
USB
Ethernet
CPU
Interface
Your design
PC
Third parties' IP
FPGA

Pack sha2 into an IP

AXI registers plan

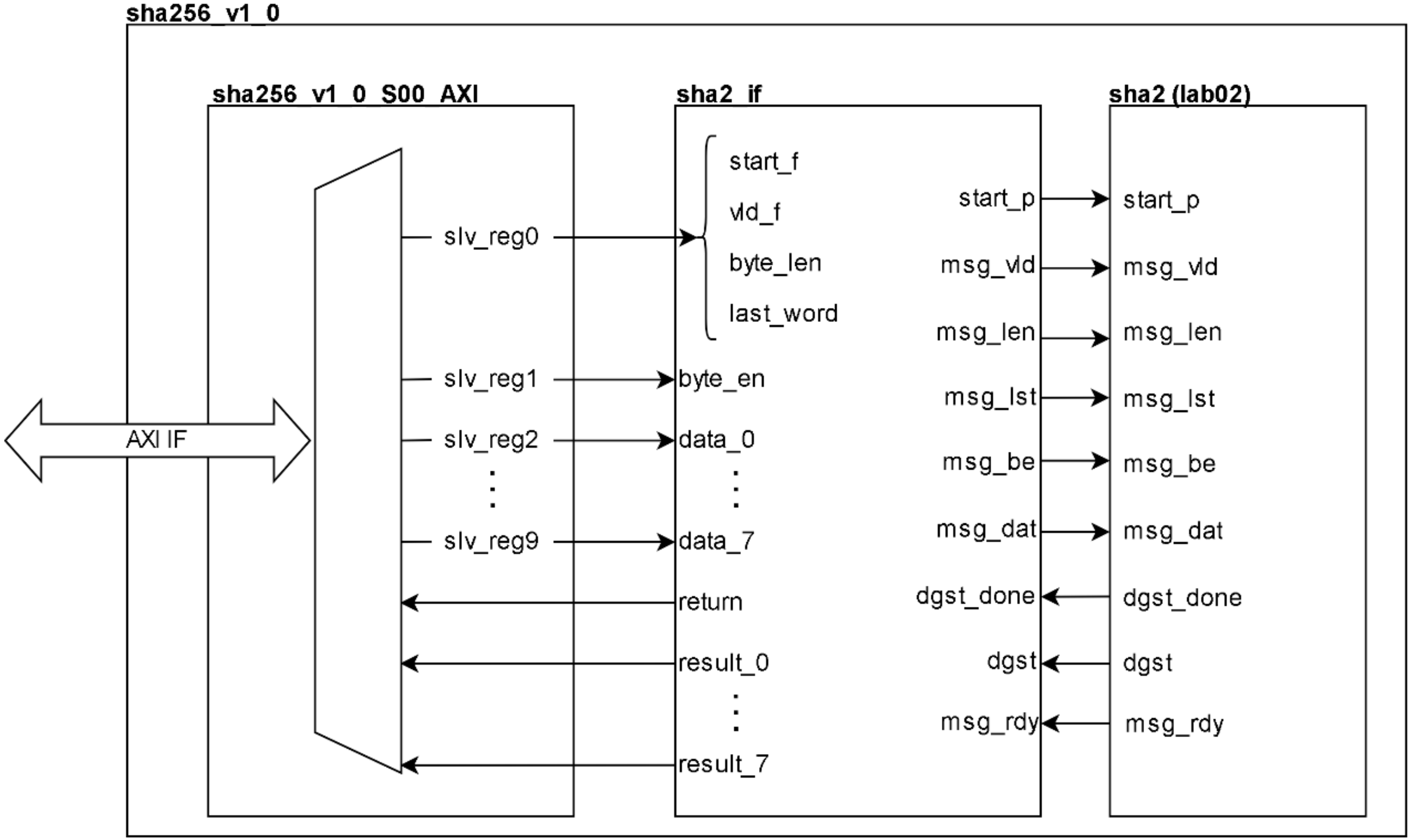
- **slv_reg0:** start_f, vld_f, byte_len, last_word

…	last_word (8-bit)	byte_len (6-bit)	vld_f	start_f

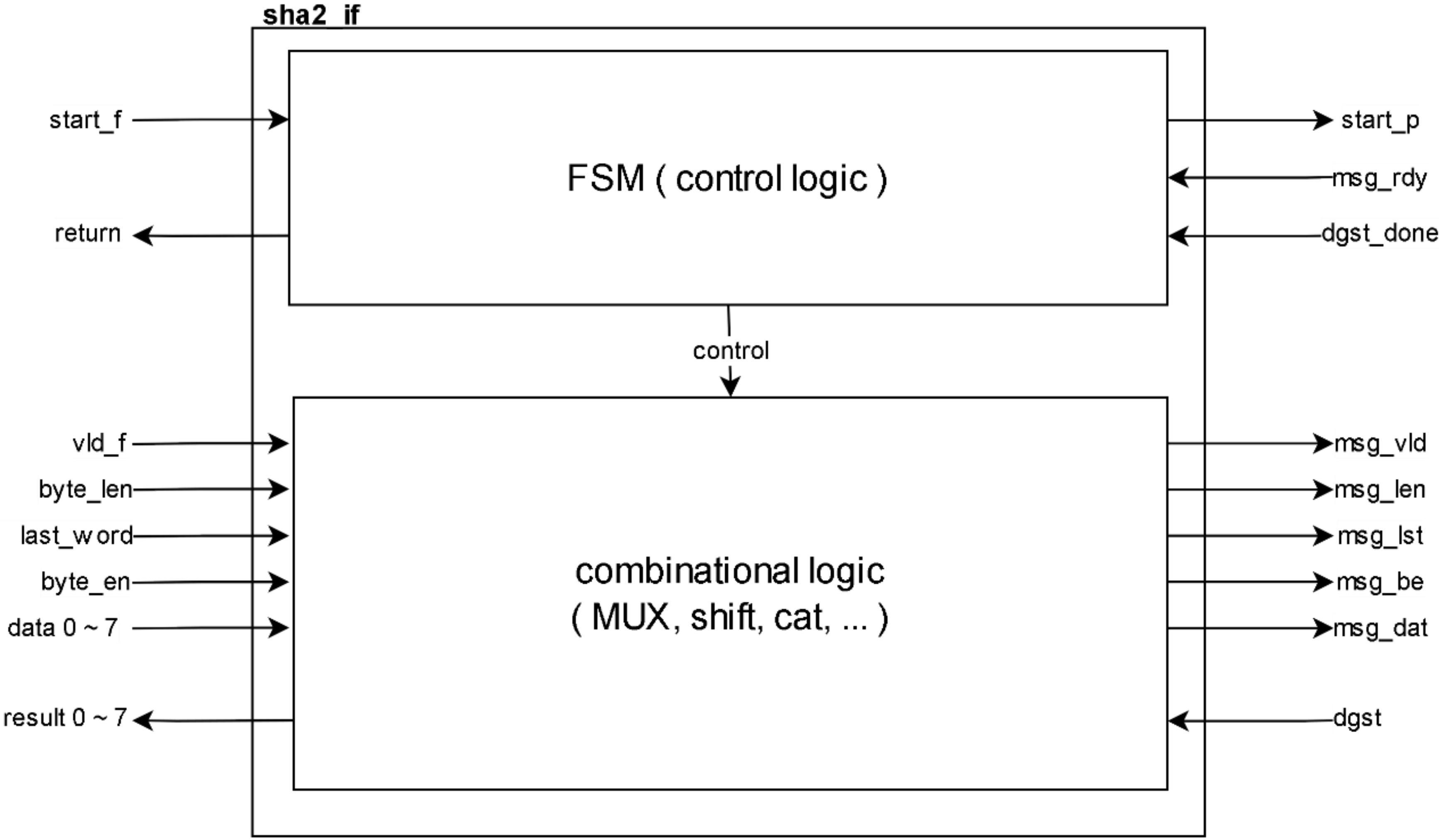
- **slv_reg1:** byte_en (32-bit)

- **slv_reg2 ~ slv_reg9:** message (8 word)

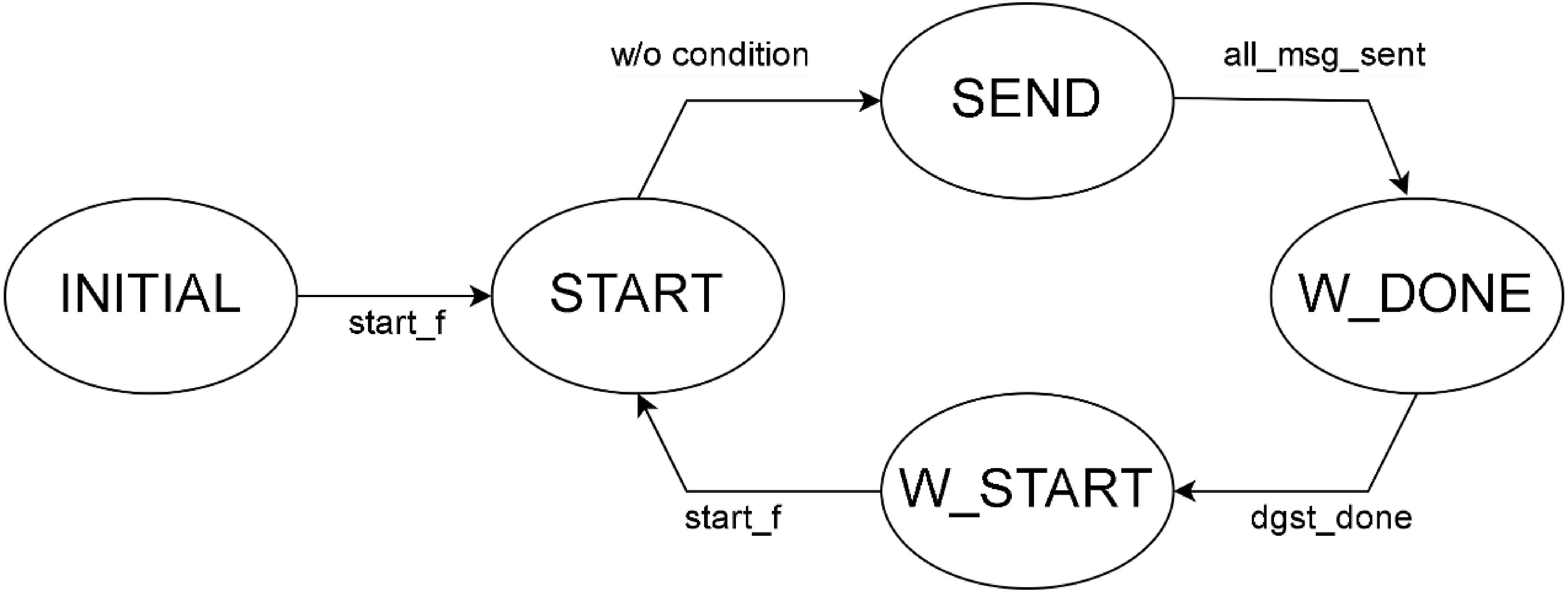
sha256_v1_0 module structure



sha2_if module structure

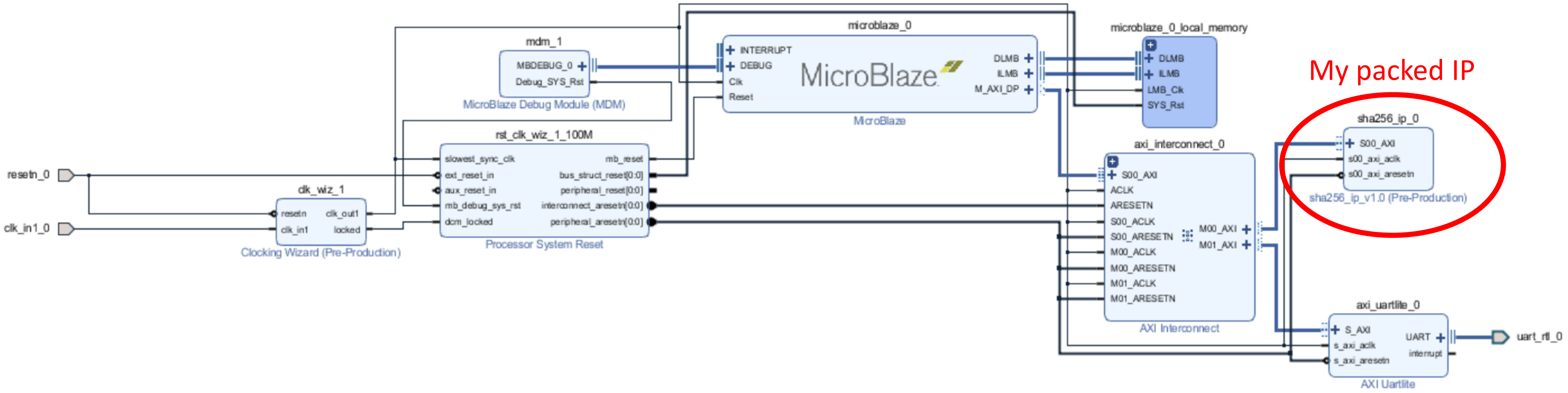


sha2_if module FSM



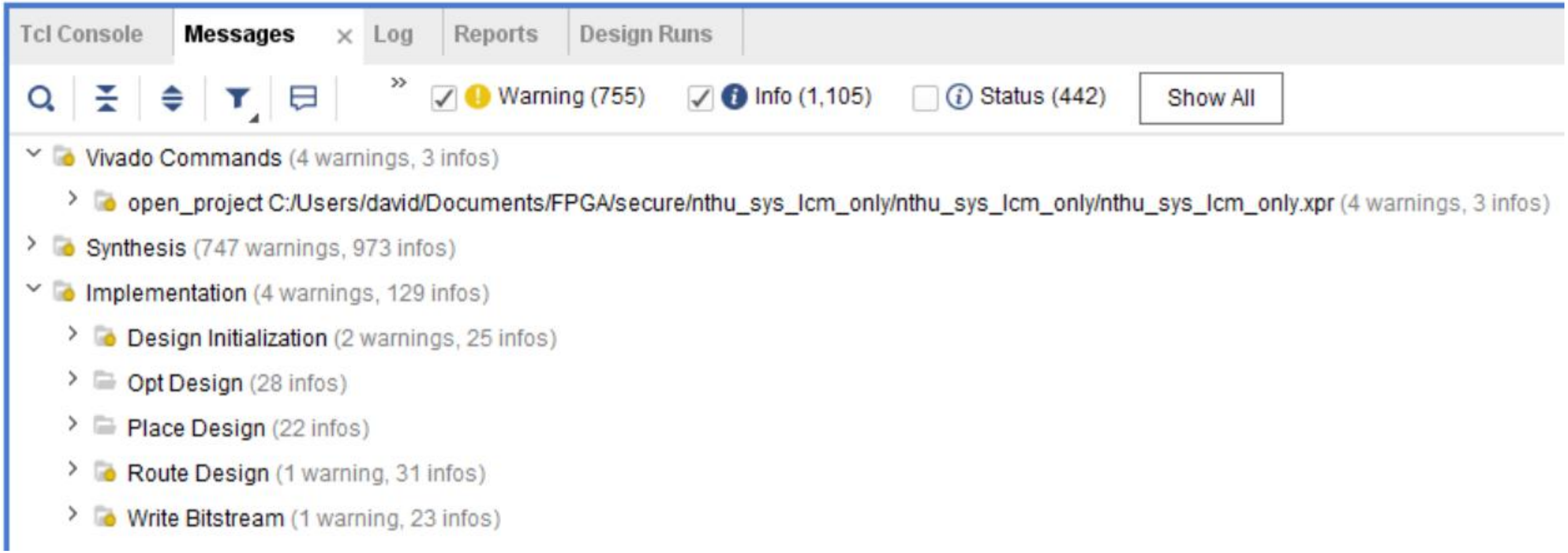
Build CPU system with packed IP

Replace default IP with my sha256 IP


My packed IP

Synthesis and Implementation

Check message

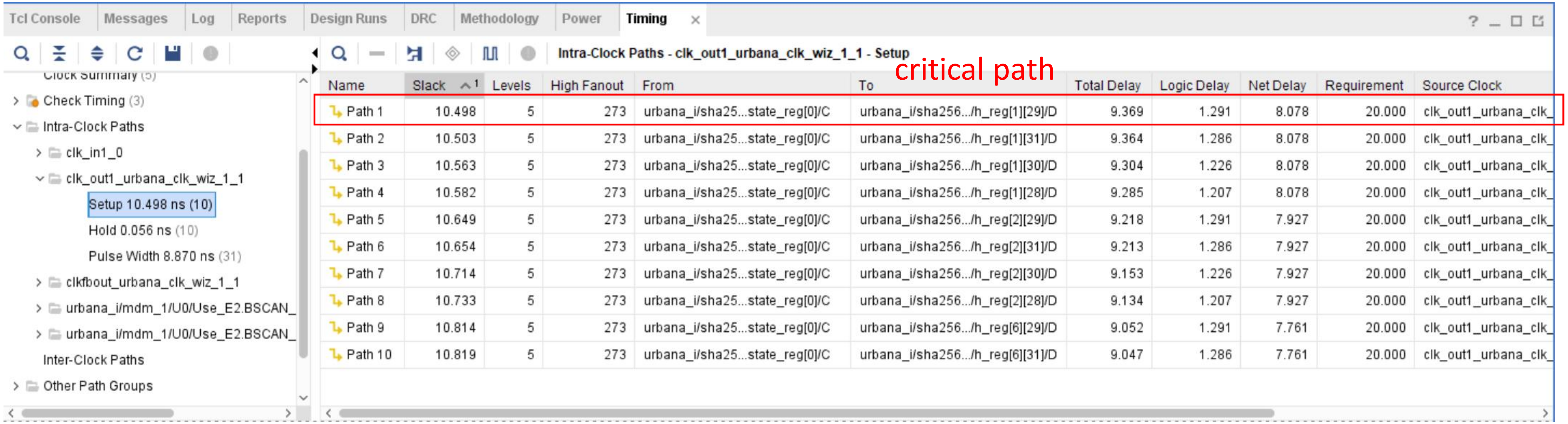


☑ Warning (755) ☑ Info (1,105) □ Status (442)

```
Vivado Commands (4 warnings, 3 infos)
    open_project C:/Users/david/Documents/FPGA/secure/nthu_sys_lcm_only/nthu_sys_lcm_only/nthu_sys_lcm_only.xpr (4 warnings, 3 infos)
Synthesis (747 warnings, 973 infos)
Implementation (4 warnings, 129 infos)
    Design Initialization (2 warnings, 25 infos)
    Opt Design (28 infos)
    Place Design (22 infos)
    Route Design (1 warning, 31 infos)
    Write Bitstream (1 warning, 23 infos)
```

→ No errors

Check timing



Clock Summary (5)
- Check Timing (3)
- Intra-Clock Paths
  - clk_in1_0
  - clk_out1_urbana_clk_wiz_1_1
    - Setup 10.498 ns (10)
    - Hold 0.056 ns (10)
    - Pulse Width 8.870 ns (31)
  - clkfbout_urbana_clk_wiz_1_1
  - urbana_i/mdm_1/U0/Use_E2.BSCAN_
  - urbana_i/mdm_1/U0/Use_E2.BSCAN_
- Inter-Clock Paths
- Other Path Groups

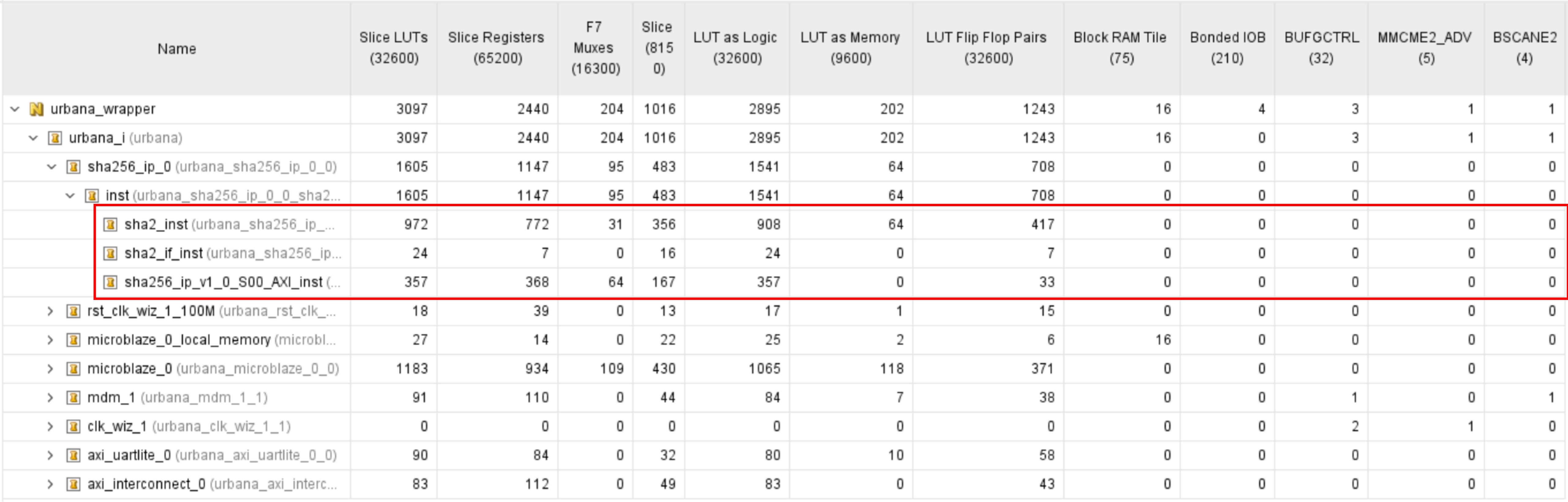
Intra-Clock Paths - clk_out1_urbana_clk_wiz_1_1 - Setup

critical path

Name	Slack ^1	Levels	High Fanout	From	To	Total Delay	Logic Delay	Net Delay	Requirement	Source Clock
Path 1	10.498	5	273	urbana_i/sha25...state_reg[0]/C	urbana_i/sha256.../h_reg[1][29]/D	9.369	1.291	8.078	20.000	clk_out1_urbana_clk_
Path 2	10.503	5	273	urbana_i/sha25...state_reg[0]/C	urbana_i/sha256.../h_reg[1][31]/D	9.364	1.286	8.078	20.000	clk_out1_urbana_clk_
Path 3	10.563	5	273	urbana_i/sha25...state_reg[0]/C	urbana_i/sha256.../h_reg[1][30]/D	9.304	1.226	8.078	20.000	clk_out1_urbana_clk_
Path 4	10.582	5	273	urbana_i/sha25...state_reg[0]/C	urbana_i/sha256.../h_reg[1][28]/D	9.285	1.207	8.078	20.000	clk_out1_urbana_clk_
Path 5	10.649	5	273	urbana_i/sha25...state_reg[0]/C	urbana_i/sha256.../h_reg[2][29]/D	9.218	1.291	7.927	20.000	clk_out1_urbana_clk_
Path 6	10.654	5	273	urbana_i/sha25...state_reg[0]/C	urbana_i/sha256.../h_reg[2][31]/D	9.213	1.286	7.927	20.000	clk_out1_urbana_clk_
Path 7	10.714	5	273	urbana_i/sha25...state_reg[0]/C	urbana_i/sha256.../h_reg[2][30]/D	9.153	1.226	7.927	20.000	clk_out1_urbana_clk_
Path 8	10.733	5	273	urbana_i/sha25...state_reg[0]/C	urbana_i/sha256.../h_reg[2][28]/D	9.134	1.207	7.927	20.000	clk_out1_urbana_clk_
Path 9	10.814	5	273	urbana_i/sha25...state_reg[0]/C	urbana_i/sha256.../h_reg[6][29]/D	9.052	1.291	7.761	20.000	clk_out1_urbana_clk_
Path 10	10.819	5	273	urbana_i/sha25...state_reg[0]/C	urbana_i/sha256.../h_reg[6][31]/D	9.047	1.286	7.761	20.000	clk_out1_urbana_clk_

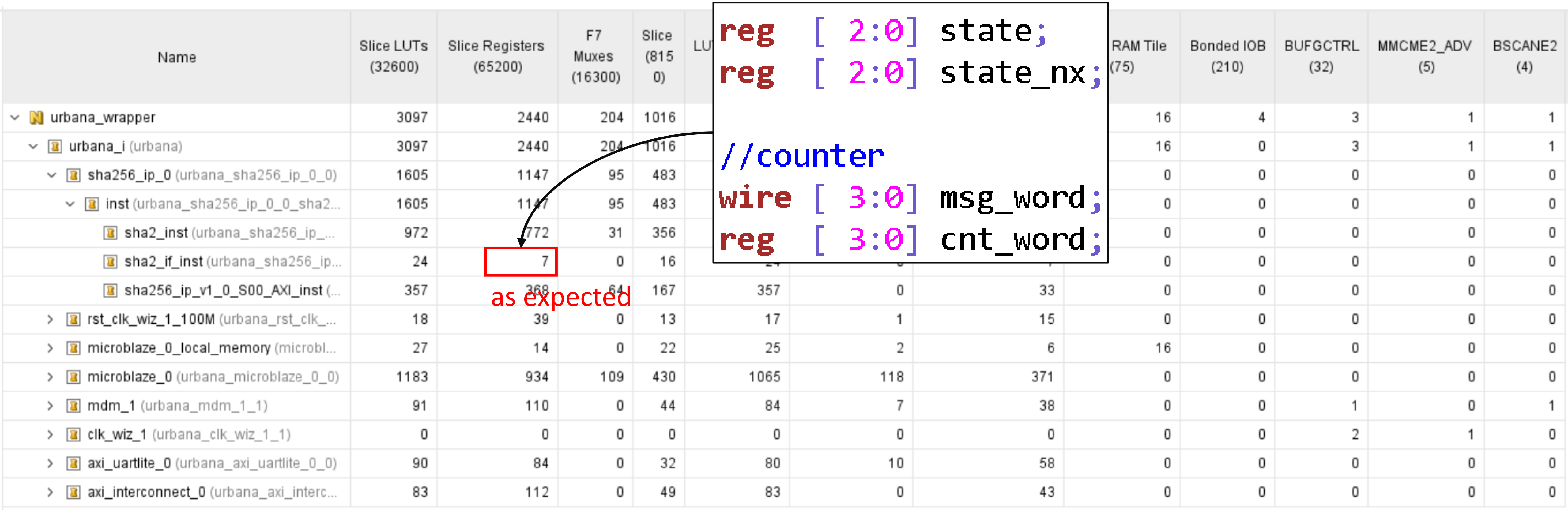
→ No setup time violate

Check utilization - hierarchy table



Name	Slice LUTs (32600)	Slice Registers (65200)	F7 Muxes (16300)	Slice (8150)	LUT as Logic (32600)	LUT as Memory (9600)	LUT Flip Flop Pairs (32600)	Block RAM Tile (75)	Bonded IOB (210)	BUFGCTRL (32)	MMCME2_ADV (5)	BSCANE2 (4)
urbana_wrapper	3097	2440	204	1016	2895	202	1243	16	4	3	1	1
urbana_i (urbana)	3097	2440	204	1016	2895	202	1243	16	0	3	1	1
sha256_ip_0 (urbana_sha256_ip_0_0)	1605	1147	95	483	1541	64	708	0	0	0	0	0
inst (urbana_sha256_ip_0_0_sha2...	1605	1147	95	483	1541	64	708	0	0	0	0	0
sha2_inst (urbana_sha256_ip_...	972	772	31	356	908	64	417	0	0	0	0	0
sha2_if_inst (urbana_sha256_ip...	24	7	0	16	24	0	7	0	0	0	0	0
sha256_ip_v1_0_S00_AXI_inst (...	357	368	64	167	357	0	33	0	0	0	0	0
rst_clk_wiz_1_100M (urbana_rst_clk_...	18	39	0	13	17	1	15	0	0	0	0	0
microblaze_0_local_memory (microbl...	27	14	0	22	25	2	6	16	0	0	0	0
microblaze_0 (urbana_microblaze_0_0)	1183	934	109	430	1065	118	371	0	0	0	0	0
mdm_1 (urbana_mdm_1_1)	91	110	0	44	84	7	38	0	0	1	0	1
clk_wiz_1 (urbana_clk_wiz_1_1)	0	0	0	0	0	0	0	0	0	2	1	0
axi_uartlite_0 (urbana_axi_uartlite_0_0)	90	84	0	32	80	10	58	0	0	0	0	0
axi_interconnect_0 (urbana_axi_interc...	83	112	0	49	83	0	43	0	0	0	0	0

Check utilization - hierarchy table



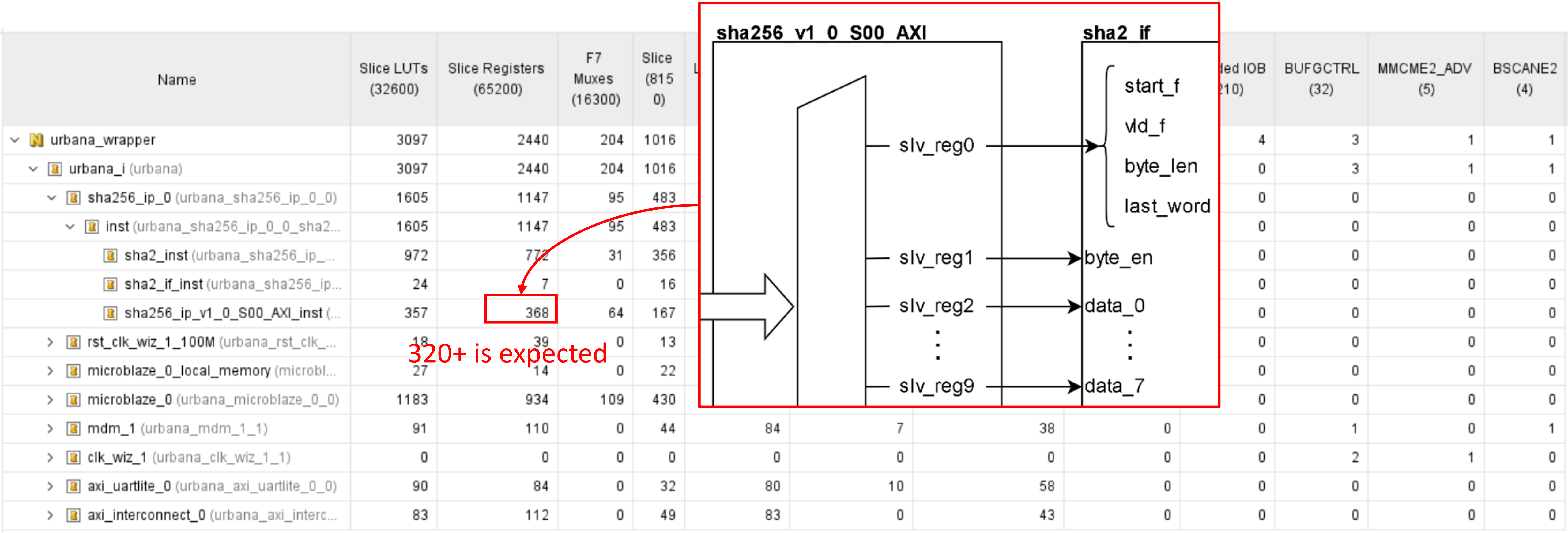
Name	Slice LUTs (32600)	Slice Registers (65200)	F7 Muxes (16300)	Slice (8150)	LU			RAM Tile (75)	Bonded IOB (210)	BUFGCTRL (32)	MMCME2_ADV (5)	BSCANE2 (4)
urbana_wrapper	3097	2440	204	1016				16	4	3	1	1
urbana_i (urbana)	3097	2440	204	1016				16	0	3	1	1
sha256_ip_0 (urbana_sha256_ip_0_0)	1605	1147	95	483				0	0	0	0	0
inst (urbana_sha256_ip_0_0_sha2...	1605	1147	95	483				0	0	0	0	0
sha2_inst (urbana_sha256_ip_...	972	772	31	356				0	0	0	0	0
sha2_if_inst (urbana_sha256_ip...	24	7	0	16	24	0	7	0	0	0	0	0
sha256_ip_v1_0_S00_AXI_inst (...	357	368	64	167	357	0	33	0	0	0	0	0
rst_clk_wiz_1_100M (urbana_rst_clk_...	18	39	0	13	17	1	15	0	0	0	0	0
microblaze_0_local_memory (microbl...	27	14	0	22	25	2	6	16	0	0	0	0
microblaze_0 (urbana_microblaze_0_0)	1183	934	109	430	1065	118	371	0	0	0	0	0
mdm_1 (urbana_mdm_1_1)	91	110	0	44	84	7	38	0	0	1	0	1
clk_wiz_1 (urbana_clk_wiz_1_1)	0	0	0	0	0	0	0	0	0	2	1	0
axi_uartlite_0 (urbana_axi_uartlite_0_0)	90	84	0	32	80	10	58	0	0	0	0	0
axi_interconnect_0 (urbana_axi_interc...	83	112	0	49	83	0	43	0	0	0	0	0

```
reg  [ 2:0] state;
reg  [ 2:0] state_nx;

//counter
wire [ 3:0] msg_word;
reg  [ 3:0] cnt_word;
```

as expected

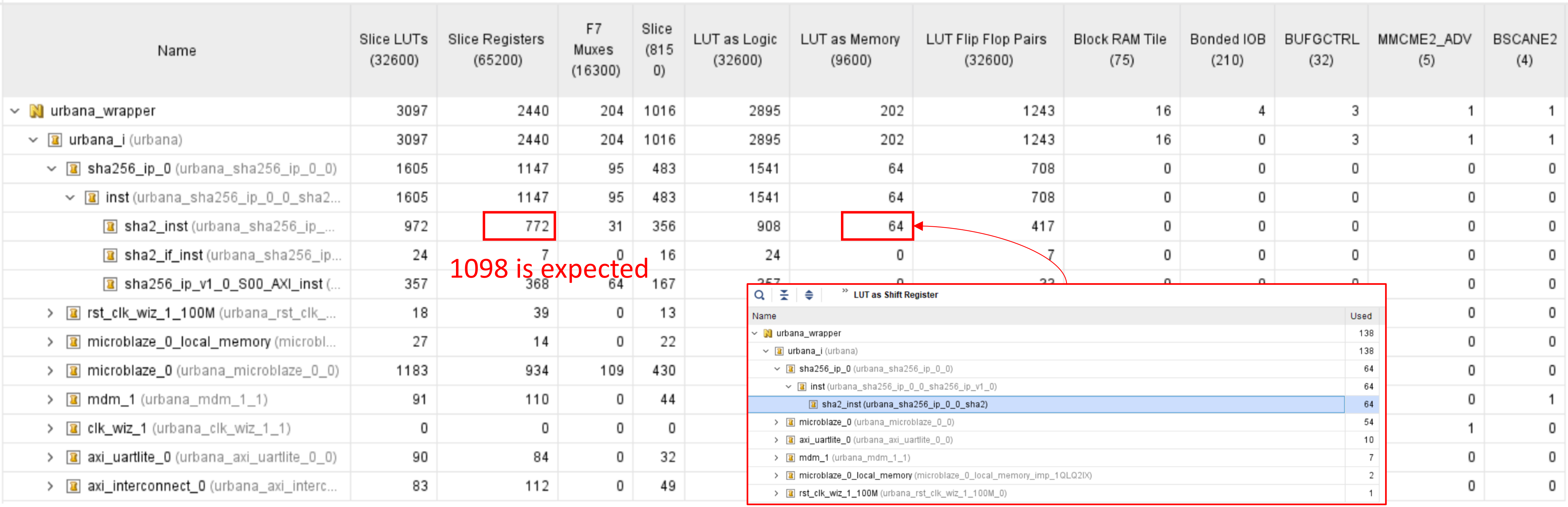
Check utilization - hierarchy table



Name	Slice LUTs (32600)	Slice Registers (65200)	F7 Muxes (16300)	Slice (8150)	L				ded IOB 210)	BUFGCTRL (32)	MMCME2_ADV (5)	BSCANE2 (4)
urbana_wrapper	3097	2440	204	1016					4	3	1	1
urbana_i (urbana)	3097	2440	204	1016					0	3	1	1
sha256_ip_0 (urbana_sha256_ip_0_0)	1605	1147	95	483					0	0	0	0
inst (urbana_sha256_ip_0_0_sha2...	1605	1147	95	483					0	0	0	0
sha2_inst (urbana_sha256_ip_...	972	772	31	356					0	0	0	0
sha2_if_inst (urbana_sha256_ip...	24	7	0	16					0	0	0	0
sha256_ip_v1_0_S00_AXI_inst (...	357	368	64	167					0	0	0	0
rst_clk_wiz_1_100M (urbana_rst_clk_...	18	39	0	13					0	0	0	0
microblaze_0_local_memory (microbl...	27	14	0	22					0	0	0	0
microblaze_0 (urbana_microblaze_0_0)	1183	934	109	430					0	0	0	0
mdm_1 (urbana_mdm_1_1)	91	110	0	44	84	7	38	0	0	1	0	1
clk_wiz_1 (urbana_clk_wiz_1_1)	0	0	0	0	0	0	0	0	0	2	1	0
axi_uartlite_0 (urbana_axi_uartlite_0_0)	90	84	0	32	80	10	58	0	0	0	0	0
axi_interconnect_0 (urbana_axi_interc...	83	112	0	49	83	0	43	0	0	0	0	0

320+ is expected

Check utilization - hierarchy table

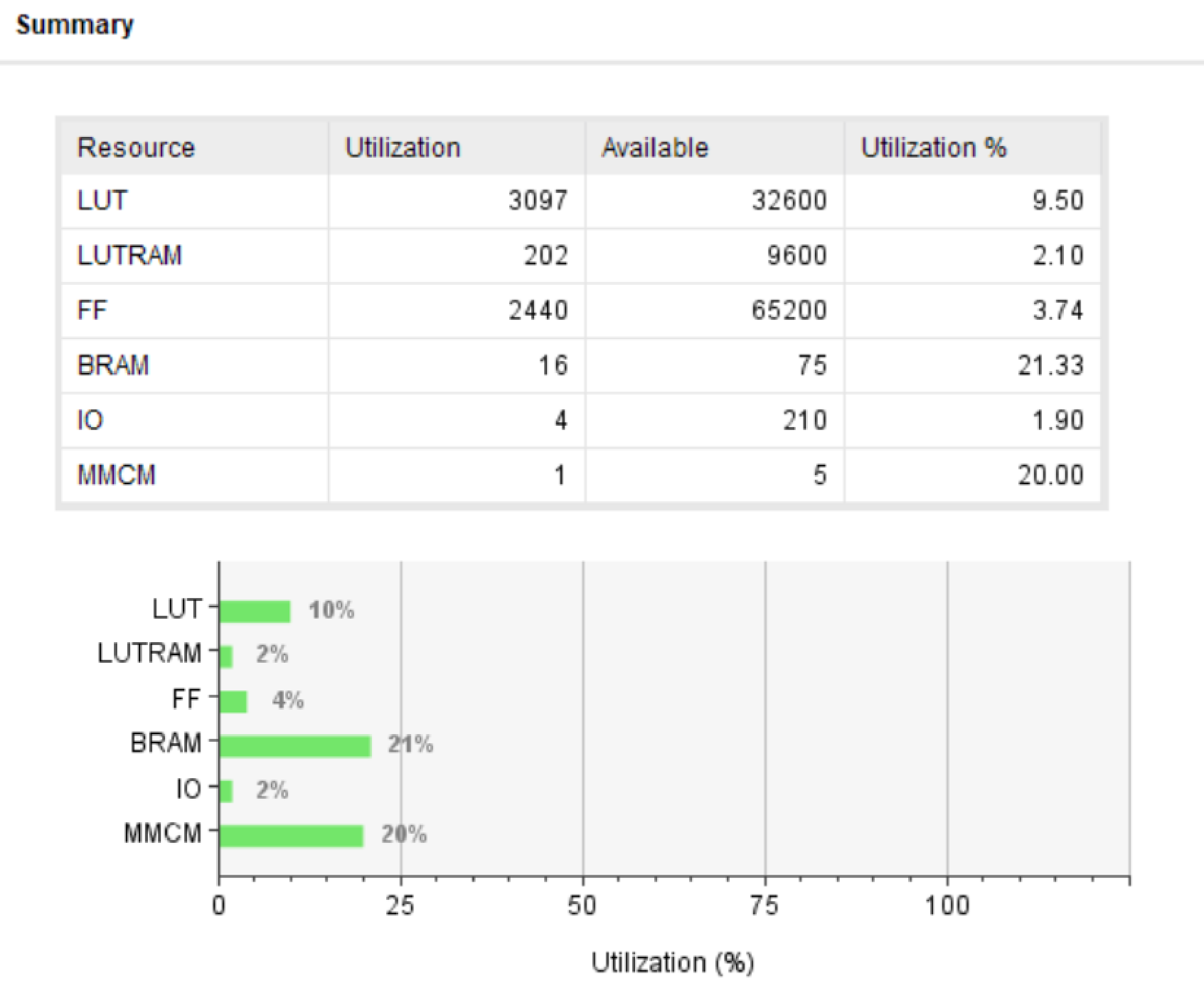


Name	Slice LUTs (32600)	Slice Registers (65200)	F7 Muxes (16300)	Slice (8150)	LUT as Logic (32600)	LUT as Memory (9600)	LUT Flip Flop Pairs (32600)	Block RAM Tile (75)	Bonded IOB (210)	BUFGCTRL (32)	MMCME2_ADV (5)	BSCANE2 (4)
urbana_wrapper	3097	2440	204	1016	2895	202	1243	16	4	3	1	1
urbana_i (urbana)	3097	2440	204	1016	2895	202	1243	16	0	3	1	1
sha256_ip_0 (urbana_sha256_ip_0_0)	1605	1147	95	483	1541	64	708	0	0	0	0	0
inst (urbana_sha256_ip_0_0_sha2...	1605	1147	95	483	1541	64	708	0	0	0	0	0
sha2_inst (urbana_sha256_ip_...	972	772	31	356	908	64	417	0	0	0	0	0
sha2_if_inst (urbana_sha256_ip...	24	7	0	16	24	0	7	0	0	0	0	0
sha256_ip_v1_0_S00_AXI_inst (...	357	368	64	167	357	0	33	0	0	0	0	0
rst_clk_wiz_1_100M (urbana_rst_clk_...	18	39	0	13							0	0
microblaze_0_local_memory (microbl...	27	14	0	22							0	0
microblaze_0 (urbana_microblaze_0_0)	1183	934	109	430							0	0
mdm_1 (urbana_mdm_1_1)	91	110	0	44							0	1
clk_wiz_1 (urbana_clk_wiz_1_1)	0	0	0	0							1	0
axi_uartlite_0 (urbana_axi_uartlite_0_0)	90	84	0	32							0	0
axi_interconnect_0 (urbana_axi_interc...	83	112	0	49							0	0

1098 is expected

Name	Used
urbana_wrapper	138
urbana_i (urbana)	138
sha256_ip_0 (urbana_sha256_ip_0_0)	64
inst (urbana_sha256_ip_0_0_sha256_ip_v1_0)	64
sha2_inst (urbana_sha256_ip_0_0_sha2)	64
microblaze_0 (urbana_microblaze_0_0)	54
axi_uartlite_0 (urbana_axi_uartlite_0_0)	10
mdm_1 (urbana_mdm_1_1)	7
microblaze_0_local_memory (microblaze_0_local_memory_imp_1QLQ2IX)	2
rst_clk_wiz_1_100M (urbana_rst_clk_wiz_1_100M_0)	1

Check utilization - summary table

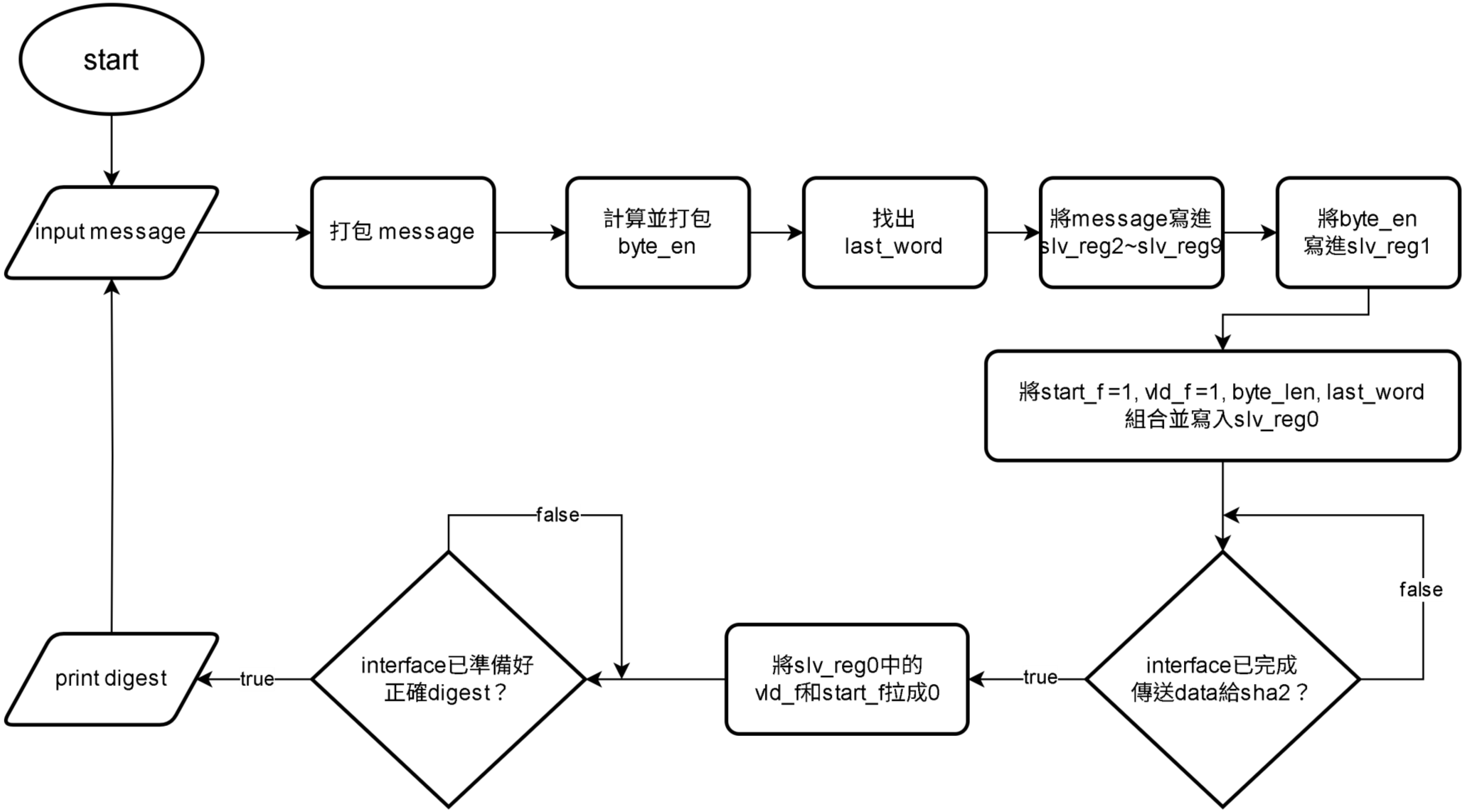


Summary

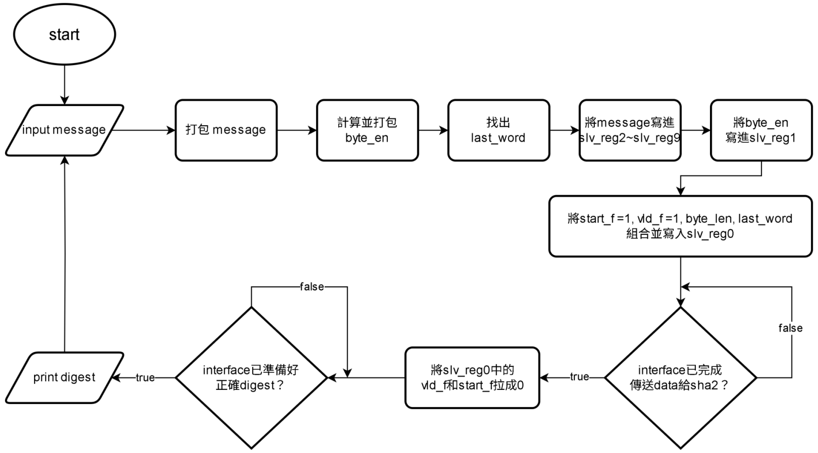
Resource	Utilization	Available	Utilization %
LUT	3097	32600	9.50
LUTRAM	202	9600	2.10
FF	2440	65200	3.74
BRAM	16	75	21.33
IO	4	210	1.90
MMCM	1	5	20.00

C program in SDK

Flow chart


start
input message
打包 message
計算並打包
byte_en
找出
last_word
將message寫進
slv_reg2~slv_reg9
將byte_en
寫進slv_reg1
將start_f =1, vld_f =1, byte_len, last_word
組合並寫入slv_reg0
interface已完成
傳送data給sha2？
false
true
將slv_reg0中的
vld_f和start_f拉成0
interface已準備好
正確digest？
false
true
print digest

Flow chart - explanation



input message

- 印出“message: ”
- 逐byte接收message，直到enter或是已接收32 byte
- 記下接收了幾個byte，並當作byte_len

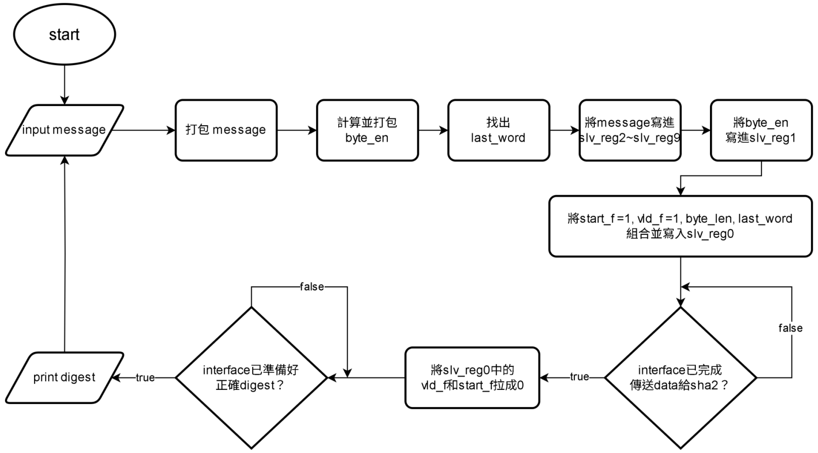
打包message

- 將message分裝成8個word

計算並打包
byte_en

- 計算每個word分別對應的msg_be
- 將結果彙整為32-bit的byte_en訊號

Flow chart - explanation

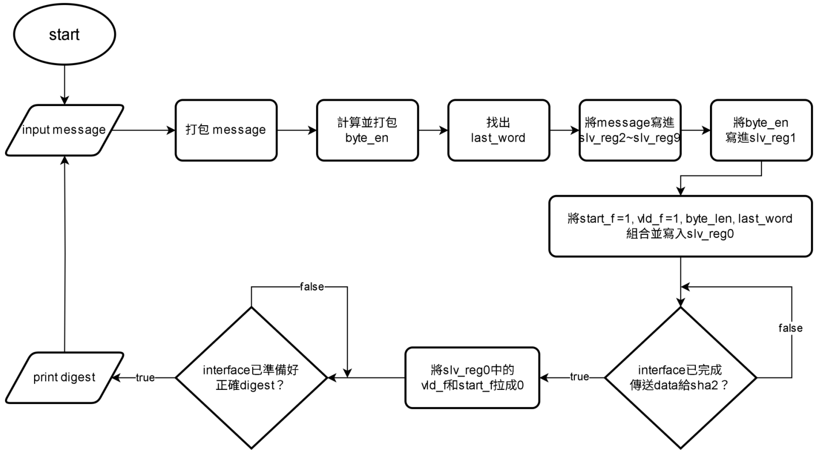


找出last_word → 計算每個word分別對應的msg_lst

將message寫進 slv_reg2 ~ slv_reg9 → 使用Xil_Out32將打包好的message word寫入AXI的slv_reg2 ~ slv_reg9

將byte_en寫進 slv_reg1 → 使用Xil_Out32將打包好的byte_en寫入AXI的slv_reg1

Flow chart - explanation



將start_f =1, vld_f =1, byte_len, last_word
組合並寫入slv_reg0

→ 使用Xil_Out32將start_f =1, vld_f =1, byte_len, last_word組合並寫入slv_reg0。

Interface已完成
傳送data給sha2？

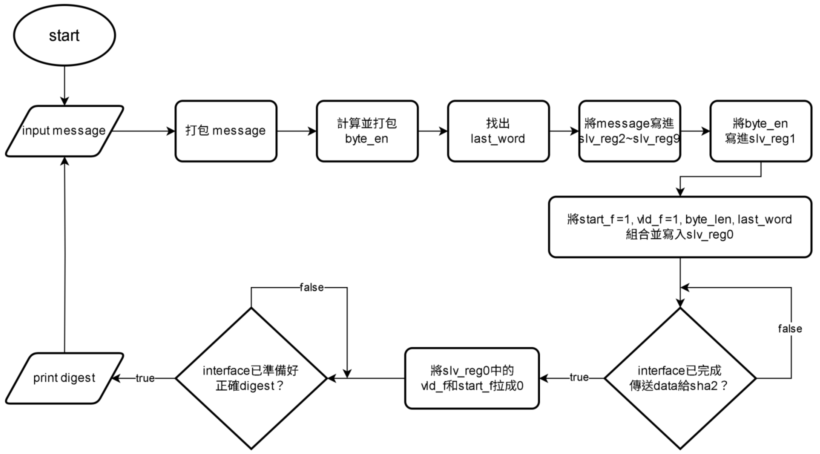
→ 使用Xil_In32讀取return[30]的訊號作為判斷條件，

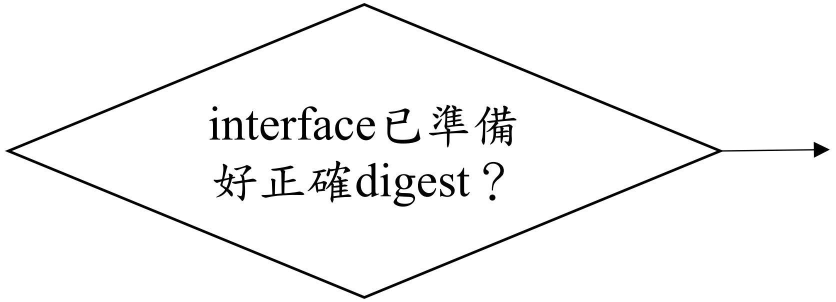
當為1時，繼續進行程式，否則繼續等待。

將slv_reg0中的
vld_f, start_f拉成0

→ 使用Xil_Out32將slv_reg0中代表vld_f和start_f的bit改成0。

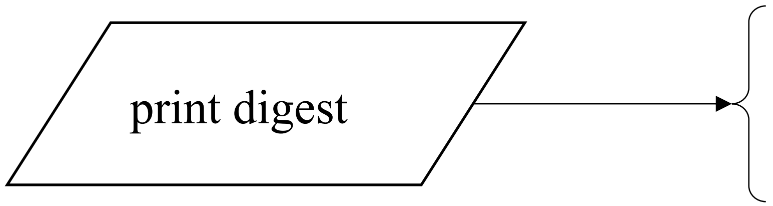
Flow chart - explanation





interface已準備
好正確digest？

使用Xil_In32讀取return[31]的訊號 作為判斷條件，當為1時，繼續進行程式，否則繼續等待。



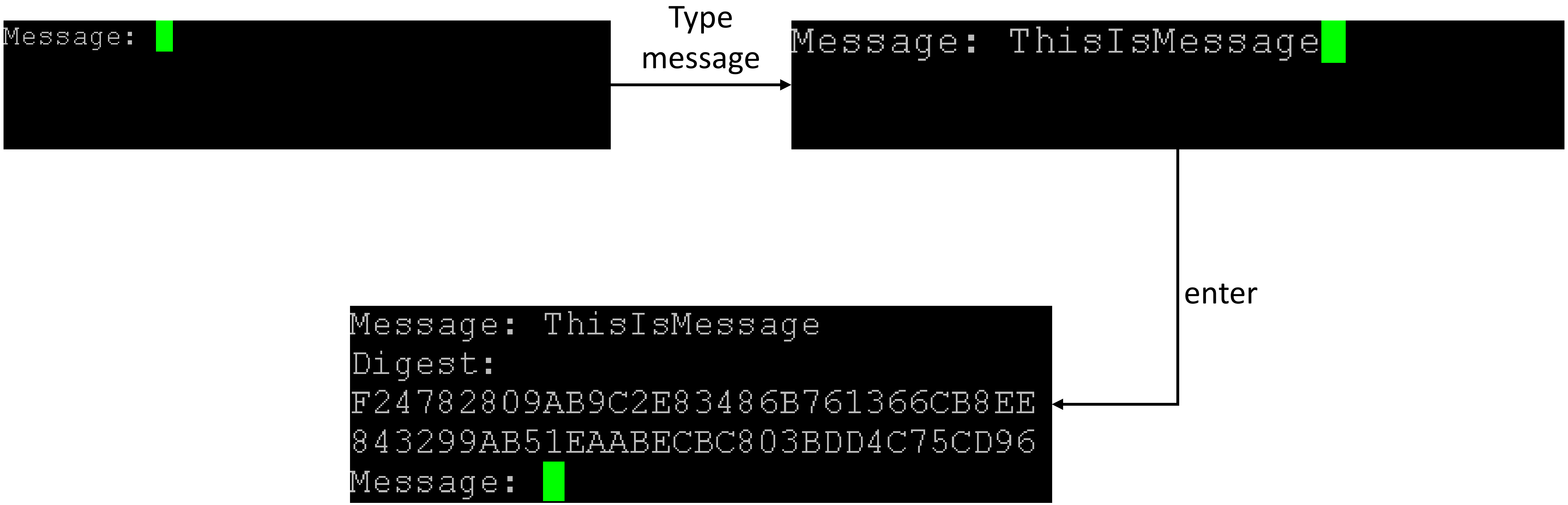
print digest

印出“Digest: ”並換行

分段讀取並接續分2行印出result 0～7的值

Result

Demonstration



```
Message:
```

Type message

```
Message: ThisIsMessage
```

enter

```
Message: ThisIsMessage
Digest:
F24782809AB9C2E83486B761366CB8EE
843299AB51EAABECBC803BDD4C75CD96
Message:
```

Review

Problem encounter

問題：不理解FPGA demo的流程

解決方法：在助教時間時，問清楚我的問題(非常感謝助教)

問題：C program等不到digest

過程：發現是C program有成功寫入slv_reg但等不到return訊號

解決方法：寫testbench驗證sha2_if，但發現沒有問題。重新下載nthu_sys_lcm_only並重燒板子，問題就不見了。

心得

- 初次接觸FPGA
- 沒有寫過C code

⟶ 花時間與心力學習並熟悉陌生領域，結果是愉快充實的

Thanks for listening