

BẢN GIẢI TRÌNH CÂU HỎI PHẢN BIỆN ĐỒ ÁN TỐT NGHIỆP

1. SOURCE CODE THIẾT KẾ

Các source code yêu cầu đã được upload lên repo Github, truy cập tại địa chỉ https://github.com/tlatonf/thesis_defense, hoặc scan qr code bên dưới đây:



2. MODULE KECCAK-f

2.1. Verify

- Dùng tool Cadence Xcelium 2403:

```
51      initial begin
52          #10;

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS
bash - 20_sim + v [icon]

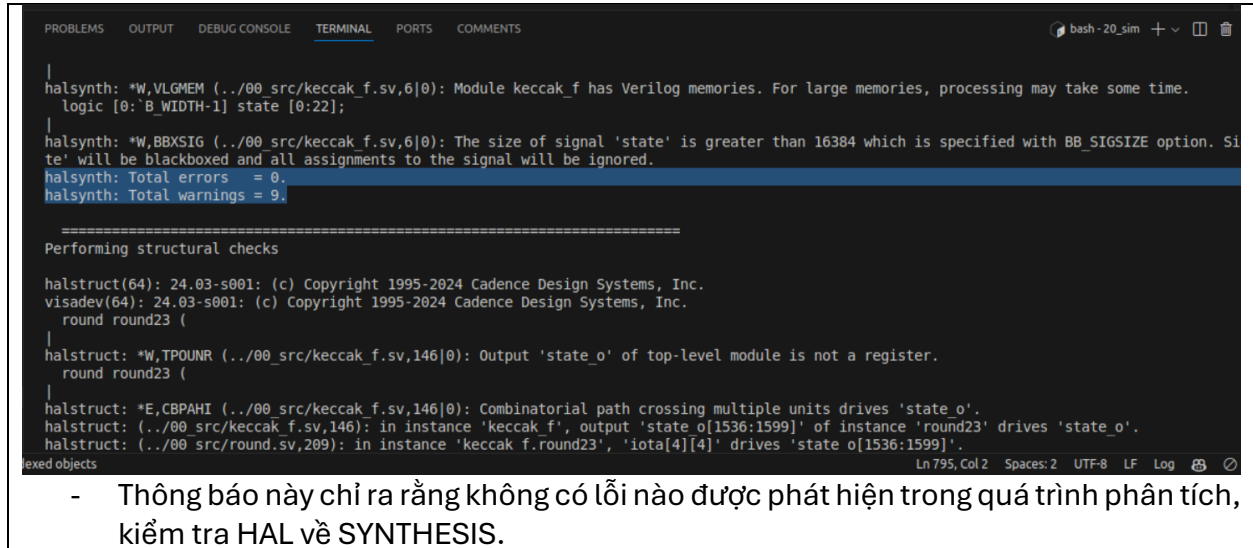
xcelium> run
round 0: OK
round 1: OK
round 2: OK
round 3: OK
round 4: OK
round 5: OK
round 6: OK
round 7: OK
round 8: OK
round 9: OK
round 10: OK
round 11: OK
round 12: OK
round 13: OK
round 14: OK
round 15: OK
round 16: OK
round 17: OK
round 18: OK
round 19: OK
round 20: OK
round 21: OK
round 22: OK
round 23: OK
Simulation complete via $finish(1) at time 250 NS + 0
../t0_tb/keccak_f1600_tb.sv:58      $finish;
xcelium> exit
T00L:  xrun(64)      24.03-s001: Exiting on Dec 11, 2024 at 08:08:50 +07 (total: 00:00:00)
o tlatonf@413ia: 20_sim$

lexed objects
Ln 52, Col 8 Spaces: 2 UTF-8 LF SystemVerilog [icon] [icon]
```

- Cách khởi chạy: \$ thesis_review/keccak-f/20_sim/testbench.sh
- Testcase lấy từ: [eXtended Keccak Code Package](#)

2.2. Synthesis

- Dùng tool Cadence Xcelium 2403:



The screenshot shows the terminal output of the synthesis process in Cadence Xcelium 2403. The output includes several messages from the halsynth tool, indicating that the module keccak_f has Verilog memories and that the size of the signal 'state' is greater than 16384, which is specified with the BB_SIGSIZE option. The synthesis process is performing structural checks, and the output shows that the module keccak_f is not a register. The synthesis process is completed with 0 errors and 9 warnings.

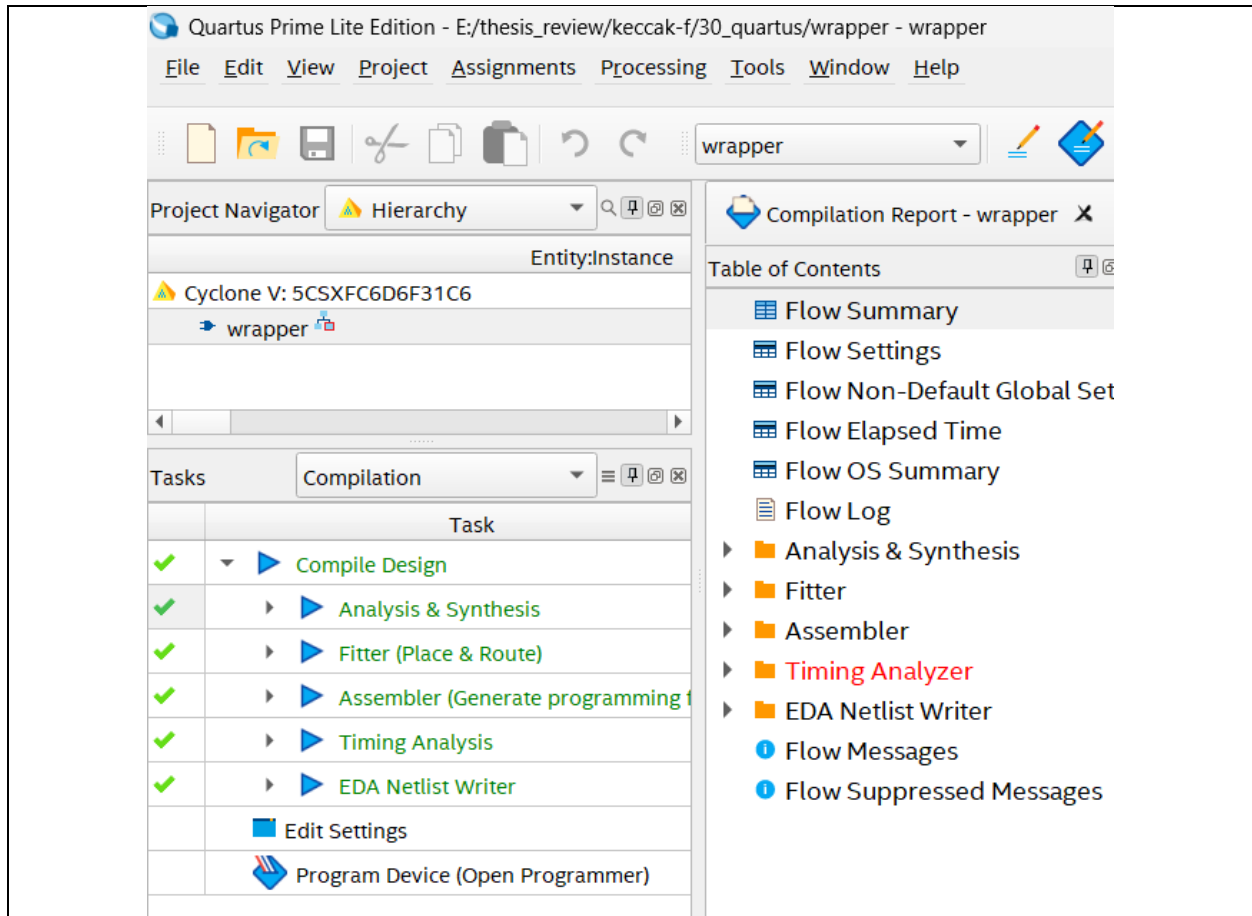
```
halsynth: *W,VLMEM (../00_src/keccak_f.sv,6|0): Module keccak_f has Verilog memories. For large memories, processing may take some time.
logic [0: B_WIDTH-1] state [0:22];
halsynth: *W,BBXSIG (../00_src/keccak_f.sv,6|0): The size of signal 'state' is greater than 16384 which is specified with BB_SIGSIZE option. Si
te' will be blackboxed and all assignments to the signal will be ignored.
halsynth: Total errors = 0.
halsynth: Total warnings = 9.

=====
Performing structural checks
halstruct(64): 24.03-s001: (c) Copyright 1995-2024 Cadence Design Systems, Inc.
visadev(64): 24.03-s001: (c) Copyright 1995-2024 Cadence Design Systems, Inc.
round round23 (
|
halstruct: *W,TPOUNR (../00_src/keccak_f.sv,146|0): Output 'state_o' of top-level module is not a register.
round round23 (
|
halstruct: *E,CBPAHI (../00_src/keccak_f.sv,146|0): Combinatorial path crossing multiple units drives 'state_o'.
halstruct: (../00_src/keccak_f.sv,146): in instance 'keccak_f', output 'state_o[1536:1599]' of instance 'round23' drives 'state_o'.
halstruct: (../00_src/round.sv,209): in instance 'keccak_f.round23', 'iota[4][4]' drives 'state_o[1536:1599]'.
lexed objects
```

- Thông báo này chỉ ra rằng không có lỗi nào được phát hiện trong quá trình phân tích, kiểm tra HAL về SYNTHESIS.

2.3. Compile bằng Intel Quartus Prime, simulate on DE10 kit.

- Trong báo cáo, em có trình bày module Keccak-f thực hiện chỉ trong 1 chu kỳ (vì đây là mạch tổ hợp), tuy nhiên đó là trường hợp đặt module này nằm trong một thiết kế tổng thể.
- Còn khi tách ra chạy độc lập thì không thể đạt được, vì số lượng chân của FPGA bị giới hạn (mỗi input/output của module cần đến 1600bit).
- Nên trong bài test này, em sẽ chia nhỏ input/output thành từng đoạn, nên số chu kỳ thực hiện không còn được 1 chu kỳ.
- Minh chứng synthesis/fitter thành công:



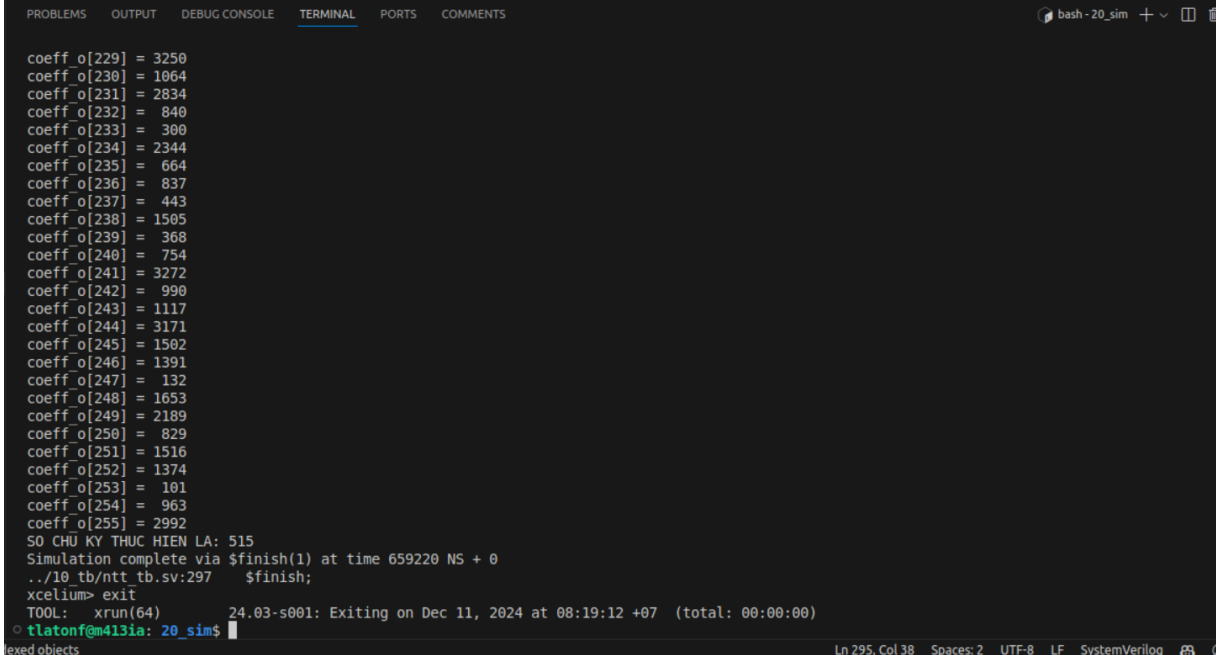
- Kết quả resource khi compile bằng quartus:

	Resource	Usage
1	Estimate of Logic utilization (ALMs needed)	13126
2		
3	▼ Combinational ALUT usage for logic	18951
1	-- 7 input functions	1806
2	-- 6 input functions	5494
3	-- 5 input functions	2461
4	-- 4 input functions	4204
5	-- <=3 input functions	4986
4		
5	Dedicated logic registers	3310
6		
7	I/O pins	203
8		
9	Total DSP Blocks	1
10		
11	Maximum fan-out node	Mult0~8
12	Maximum fan-out	10416
13	Total fan-out	91595
14	Average fan-out	4.04

3. MODULE BIẾN ĐỔI NTT

3.1. Verify

- Dùng tool Cadence Xcelium 2403:



```

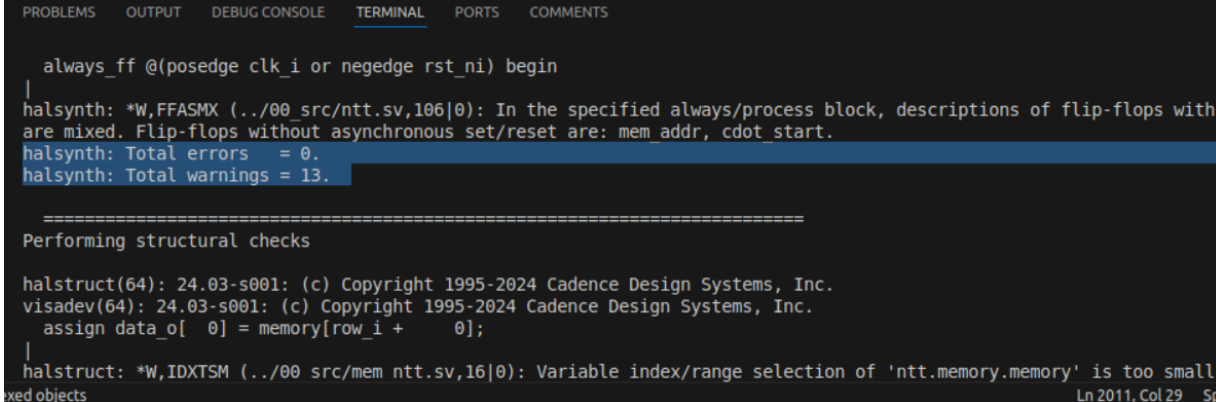
coeff_o[229] = 3250
coeff_o[230] = 1064
coeff_o[231] = 2834
coeff_o[232] = 840
coeff_o[233] = 300
coeff_o[234] = 2344
coeff_o[235] = 664
coeff_o[236] = 837
coeff_o[237] = 443
coeff_o[238] = 1505
coeff_o[239] = 368
coeff_o[240] = 754
coeff_o[241] = 3272
coeff_o[242] = 990
coeff_o[243] = 1117
coeff_o[244] = 3171
coeff_o[245] = 1502
coeff_o[246] = 1391
coeff_o[247] = 132
coeff_o[248] = 1653
coeff_o[249] = 2189
coeff_o[250] = 829
coeff_o[251] = 1516
coeff_o[252] = 1374
coeff_o[253] = 101
coeff_o[254] = 963
coeff_o[255] = 2992
SO CHU KY THUC HIEN LA: 515
Simulation complete via $finish(1) at time 659220 NS + 0
../10_tb/ntt_tb.sv:297 $finish;
xcelium> exit
T00L: xrun(64) 24.03-s001: Exiting on Dec 11, 2024 at 08:19:12 +07 (total: 00:00:00)
tlatonf@413ia: 20_sim$

```

- Cách khởi chạy: \$ thesis_review/ntt/20_sim/testbench.sh
- Testcase lấy từ: Tài liệu trích dẫn: [9] CFRG. Kyber: Post-Quantum Key Encapsulation Mechanism

3.2. Synthesis

- HAL Check bằng tool Cadence Xcelium (Version 2024):



```

always_ff @(posedge clk_i or negedge rst_ni) begin
|
halsynth: *W,FFASM (*W,FFASM (../00_src/ntt.sv,106|0): In the specified always/process block, descriptions of flip-flops with
are mixed. Flip-flops without asynchronous set/reset are: mem_addr, cdot_start.
halsynth: Total errors = 0.
halsynth: Total warnings = 13.

=====
Performing structural checks

halstruct(64): 24.03-s001: (c) Copyright 1995-2024 Cadence Design Systems, Inc.
visadev(64): 24.03-s001: (c) Copyright 1995-2024 Cadence Design Systems, Inc.
assign data_o[ 0] = memory[row_i + 0];
|
halstruct: *W,IDXSM (*W,IDXSM (../00_src/mem ntt.sv,16|0): Variable index/range selection of 'ntt.memory.memory' is too small

```

- Mặc dù vẫn còn một số cảnh báo (chủ yếu đến từ thông báo initial block không được synthesis, cảnh báo gán đa chiều, cảnh báo tải không đồng bộ, cảnh cáo rom lớn), nhưng thông báo này chỉ ra rằng không có lỗi nào được phát hiện trong quá trình phân tích, kiểm tra HAL về SYNTHESIS.

3.3. Compile bằng Intel Quartus Prime, simulate on DE10 kit.

- Kết quả resource khi compile bằng quartus:

	Resource	Usage
1	Estimate of Logic utilization (ALMs needed)	4466
2		
3	▼ Combinational ALUT usage for logic	6467
1	-- 7 input functions	0
2	-- 6 input functions	2121
3	-- 5 input functions	14
4	-- 4 input functions	3648
5	-- <=3 input functions	684
4		
5	Dedicated logic registers	6418
6		
7	I/O pins	28
8	Total MLAB memory bits	0
9	Total block memory bits	1536
10		
11	Total DSP Blocks	8
12		
13	Maximum fan-out node	rst_ni~input
14	Maximum fan-out	6556
15	Total fan-out	51693
16	Average fan-out	3.99

	Compilation Hierarchy Node	Combinational ALUTs	Dedicated Logic Registers	Block Memory Bits	DSP Blocks	Pins	Virtual Pins
1	▼ wrapper	6467 (1320)	6418 (3093)	1536	8	28	0
1	▼ ntt:utt	5147 (3410)	3325 (3092)	1536	8	0	0
1	▼ cdot:cdot0	885 (600)	125 (49)	0	4	0	0
1	divide...ivider	212 (212)	76 (76)	0	1	0	0
2	karatsu...tiplier	73 (73)	0 (0)	0	3	0	0
2	▼ cdot:cdot1	852 (577)	108 (36)	0	4	0	0
1	divide...ivider	209 (209)	72 (72)	0	1	0	0
2	karatsu...tiplier	66 (66)	0 (0)	0	3	0	0
3	▼ mem_ntt:memory	0 (0)	0 (0)	1536	0	0	0
1	▼ rom:memory	0 (0)	0 (0)	1536	0	0	0
1	▼ alts...nent	0 (0)	0 (0)	1536	0	0	0
1	al...ed	0 (0)	0 (0)	1536	0	0	0