

Points	Grade

Team: 6

01228774 Constantin SCHIEBER #1
0122576 Petar KOSIC #2

Digital Integrated Circuits Lab (LDIS)

384.088, Summer Term 2018

Supervisors:

Christian Krieg, Martin Mosbeck, Axel Jantsch

Task 2: Implementing Argon2

Abstract

1 Problem statement and motivation

2 Implementation (proposed solution)

2.1 Top Module State Machine

For the main implementation we used a state machine for all the logic.

STATE_UART_WELCOME:

The Logic starts in STATE_UART_WELCOME, which sends an welcome message to the user via UART. Afterwards it goes into STATE_IDLE and waits for new receiving data.

STATE_IDLE:

When it receives new data the state moves forward to STATE_PROD_RN.

STATE_TEST_RN:

Dummy State

STATE_PROD_RN:

In this state the state machine waits until the TRNG is ready to create next random number and then goes into STATE_PROD_RCV.

STATE_PROD_RCV:

In this state it saves the random number and switches into STATE_UART_RN.

STATE_UART_RN:

The STATE_UART_RN sends the random number over UART and then switch the state to STATE_SSEG_RN.

STATE_SSEG_RN:

The STATE_SSEG_RN state sends the random number data to the seven segment module, which shows the lower 8 nibbles of the random number in hex on the display.

2.2 UART

For the UART we used the given UART IP and slightly modified it for our purposes.

2.3 Seven Segment Display

3 Results (verification plan)

4 Discussion

5 Conclusions

The has a better understanding on how constraints in vhdl and vivado work. Sadly we couldn't provide a working solution.

6 Assessment

This is the place for the teaching staff to add notes for team assessment.

#	Issue	Yes	No
1 Implementation			
1.1	Does the implementation conform to the specification?		
1.2	Is the implementation resource-efficient?		
1.3	Is the implementation's hardware description language (HDL) complexity low?		
1.4	Is the implementation well-documented?		
1.5	Is the file structure's complexity low?		
2 Coding style			
2.1	Is the line width of code limited to 80 characters?		
2.2	Is white space appropriately used?		
2.3	Are tabs used for indentation?		
2.4	Are separators used to logically divide the file contents?		
2.5	Are meaningful comments given?		
3 Code reuse			
3.1	Is publicly available code re-used?		
3.2	Is non-publicly available code re-used?		
3.3	Are the sources of re-used code cited?		
4 Interaction			
4.1	Was the specification unclear to the team?		
4.2	If yes, did the team contact the teaching staff to make the specification clear?		
5 Report			
5.1	Are there typos?		
5.2	Is the report grammatically correct?		
5.3	Is there redundant information?		
5.4	Is the report's format consistent?		
5.5	Are captions properly used and numbered? Page numbers?		
5.6	Are figures and tables properly referenced in the body text?		
5.7	Are resources properly referenced?		