Recommended
LWC Project Schedule

1

Recommended Project Tasks (1)

Week 1 [10/17-10/23]

Understanding
a. specification (without security analysis)
b. reference implementation in C
c. interface of the CryptoCore and LWC.

Formulating assumptions, e.g.,
- supported variant(s).

Week 2 [10/24-10/30]

Drawing
a. detailed block diagram of the Datapath
b. interface with the division into the Datapath and Controller.

2

Recommended Project Tasks (2)

Week 3 [10/31-11/06]

Developing RTL VHDL code of the Datapath.
Timing Analysis (with all execution times expressed in clock cycles).

Week 4 [11/07-11/13]

Developing a testbench for the Datapath.
Debugging the Datapath.
Verifying execution times in clock cycles using simulation.

3

Recommended Project Tasks (3)

Week 5 [11/14-11/20]

Drawing ASM chart of the Controller.

Week 6 [11/21-11/27]

Developing RTL VHDL code of the Controller.
Generating test vectors using cryptotvgen.
Debugging the entire code using LWC_TB.

4

Recommended Project Tasks (4)

Week 7 [11/28-12/04]

Generating preliminary results using Xilinx Vivado.
Optimizing the design and code.
Writing the verification report.
Final timing analysis [with throughputs in Mbits/s]

Week 8 [12/05-12/11]

Benchmarking.
Finalizing project deliverables.

5

Important Comments

- **If you fall behind in the first weeks of the project, you can still catch up by doing more in the later weeks.**
- **You can pass the course with a grade B or better even if you do not manage to complete all project tasks.**
- **You will have an opportunity to discuss your progress with me at least once per two weeks by scheduling a meeting with me using Doodle.**
- **You also can request additional meetings with me in the periods between two consecutive progress reports.**
- **Please feel free to post your questions on Piazza.**

6