POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

DEPARTEMENT DE GENIE INFORMATIQUE ET GENIE LOGICIEL

INF8505E: Embedded Configurable Processors

Laboratory 2

Design of specialized instructions for the SHA256 application

Laboratory Instructor: Imad Benacer

imad.benacer@polymtl.ca

February 2019

Table of contents

1 Laboratory objectives 1
2 Part-1 SHA256 profiling 1
3 Part-2 custom instruction(s) for SHA256 acceleration 1
4 Laboratory report and evaluation 2
5 References 2

1 Laboratory objectives

Initially, the role of processors in a digital system was to control the proper functioning of the hardware components and to collect statistics. These processors were generic. When designers wanted to use more sophisticated processors, they had to design and implement them from scratch. In recent years, new technologies for automatic generation of processors have become available on the Electronic Design Automation (EDA) market. These tools make it possible to overcome the limitations of general purpose processors. Indeed, these tools for generating processors allow to design a processor that is better adapted to the application and that will make the most of the implementation technology.

In this lab, you will learn how to customize the TLX 32-bit reduced instruction set computing (RISC) processor (a variant of Hennessy and Patterson DLX RISC [1]) instruction set to accelerate the SHA256 application [2].

2 Part-1 SHA256 profiling

In the first part of this laboratory, you are asked to profile the SHA256 application under the TLX processor. Take a few minutes to study the SHA256 code and then do a profiling to identify the functions to accelerate. To do this, use the unmodified processor configuration while commenting #define custom_instruction. To use the example of the custom instruction, de-comment the latter #define.

It will be very important throughout the progress of your work to ensure that your modifications do not change the functionality of the SHA256 application (i.e., the footprint generated by the program, and console message always pass “SHA256 result is correct”).

You are asked to provide the following:

1. Profile the SHA256 code and determine the reduction of the number of cycles and of the number of instructions after the introduction of the custom instruction **[10 point]**.
2. Provide the profiling results and execution summary (screenshot both tabs in the ASIP Designer tool) for both processor configurations (with and without the custom instruction) **[10 points]**.

3 Part-2 custom instruction(s) for SHA256 acceleration

In the second part of this laboratory, you are asked to provide at least another custom instruction that accelerates the SHA256 application.

You are asked to provide the following:

1. Choice of the SHA256 function(s) to accelerate **[20 points]**.
2. Profiling results **[10 points]**.
3. The gain from each new custom instruction introduction in the processor either from the reduction of number of cycles or of the number of instructions **[10 points]**.

4. A discussion including processor architecture modifications, a comparison of the performances obtained with and without the specialized instruction(s) starting from the first part of this laboratory. Display the different results in a graph (configuration vs gain) **[20 points]**.
5. Provide the area (look-up tables, flip-flops, etc.), performance (clock period), and power consumption results of both default and customized TLX processor configurations under XCVU440-FLGB2377-3-E UltraScale FPGA device. In here you should use Vivado tool, the guide for this tool can be found in the Moodle of the INF3500 course in the lab section **[20 points]**.

4 Laboratory report and evaluation

For this laboratory, you are asked to provide a laboratory report file in word or pdf version by Friday the 1st of March at 12h00.

The laboratory report will be evaluated over 100 points. You have to adhere to the lab report format standard shown under Section 2 in the Moodle of the course. The evaluation will be as follows:

Part 1	**20**
• Code profiling with discussion	10
• Profiling results for both configurations	10
Part 2	**80**
• SHA256 function(s) choice of acceleration	20
• Profiling results per new custom instruction	10
• Custom instruction(s) gain	10
• Discussion	20
• Placement and routing results	20
Total	**100**

5 References

[1] John L. Hennessy and David A. Patterson. Computer Architecture: A Quantitative Approach, 2nd Edition. Morgan Kaufmann. 1996.

[2] Website online available: https://en.wikipedia.org/wiki/SHA-2

Synopsys document notice

EN : The documentation provided by Synopsys is clearly identified for this purpose and is provided as a courtesy to Polytechnique Montréal. This documentation must only be used for the purposes of the course. It must not be shared with people who are not enrolled in the course. It must not be published online. Students must not keep a copy of this documentation after the end of the course.