The Design of the SHA1 Co-Processor

ECE 111 Final Project

Winter Quarter 2016

Date:

Team Members: (or just Name: if you did the project on your own.)

**Introduction**

* Describe background information about what is the purpose of the SHA-1 algorithm.
* Give some example applications for the SHA-1 algorithm.
* Talk about the history of the SHA-1 algorithm.
* Talk about the importance of the SHA-1 algorithm, including security concerns.

**Description of the SHA-1 Algorithm**

* You can describe the algorithm using a combination of the description/figures shown in the PowerPoint presentation “finalprojectv2.ppt”, pseudo code, etc, to adequately describe how the SHA-1 algorithm works.
* You are free to borrow “figures” from “finalprojectv2.ppt”.
* You can also use the “bullet points” from “finalprojectv2.ppt”, but put them in your own words.
* You can also use other references like the Wikipedia page, other papers on SHA-1, but use your own words when writing the description. You can use figures from other sources (incl. pseudo-code) as long as you cite the source.

**Design Details**

* Describe the approach/strategy that you took for the design.
* Did you focus on getting the design to work and made the design simple by performing each SHA-1 round using combinational logic and by using separate states for reading the memory?
* Did you aim to reduce the clock period by breaking up the computation of each SHA-1 round into multiple states? e.g., computed F(B, C, D) and ( Wt-3 ^ Wt-8 ^ Wt-14 ^ Wt-16 ) <<< 1 in separate states?
* Did you aim to reduce the #cycles and clock period by breaking the SHA-1 round computations and memory reads into pipelined stages? Provide some explanation as to how you achieved it.
* If you did multiple versions of your design, what approach did you take initially? What did you learn from the earlier designs? What did you do differently in later versions of your design based on what you learned from earlier designs?
* Did you target your design for Delay, Area x Delay, or both?
* Provide block diagram(s) if appropriate – e.g., if you did a pipelined design, and the pipelined structure is amendable to a block diagram.

**Working in Teams** (only applies if you worked in a group)

* How were the work divided among the team members?
* How did you coordinate the work and communicate between the team members?
* In which ways do you think your team functioned well?
* What have you learned from this quarter’s experience about functioning in a team?
* What can the instructors do in future quarters to make this aspect of the course better?

**Summary of Results**

* If you are just turning in one design, summarize the results for this design in terms of #ALUTs, #Registers, Area = #ALUTs + #Registers, Clock period = 1/Fmax, #cycles for the SHA1\_hash\_testbench\_v6.v, Delay = Clock period x #cycles, Area\*Delay = Area x Delay.
* If you are turning in two designs, then say explicitly that you are turning in two designs and provide the same summary of results for:
  + Best Delay Design: …
  + Best Area x Delay Design: …

**References**

* What references did you research/read for this project? You can list the Wikipedia page, IETF specification, etc.
* But if you read other papers on SHA-1 implementation, please talk about them: what were their strategies, did you adopt some of their ideas, why not, etc?