

ECE 646
PROJECT SPECIFICATION

Hardware Implementation of IDEA

by

Onur Tigli

tigli@gwu.edu

1. Design Entry Method:

The design entry will be completed in Verilog HDL. The design will be targeted for an ASIC implementation. The logic synthesis will be completed in Synopsys Design Compiler. Separate Synopsys scripts will be developed for applying advanced optimization techniques to the blocks as well as the overall design. Signalscan waveform editor will be employed for verification purposes. Verilog simulator will be used for simulating the testbenches which are written in Verilog.

2. Additional Libraries

Synopsys design compiler will be set to use the LSI_10K libraries as target and link library for synthesis. This library would be sufficient to contain all the necessary basic blocks at this stage.

3. I/O Specification

Inputs: 1. A 64-bit plaintext block
2. A 128-bit key

Output: 1. A 64-bit ciphertext

4. Algorithm Description

The main idea behind IDEA algorithm is one of “mixing operations from different algebraic groups” [1]. There are three algebraic groups whose operations are being mixed, namely:

- XOR
- Addition Modulo 2^{16} (addition, ignoring any overflow)
- Multiplication Modulo 2^{16} (multiplication, ignoring any overflow)

All these operations operate on 16-bit subblocks. Following are the basic steps that are taken in the algorithm [2]

- 64 bit input block is divided into four 16 bit blocks: X1, X2, X3 and X4 which become the input blocks to the first round of the algorithm.
- In each of the eight total rounds, the four sub-blocks are XORed, added, and multiplied with one another and with six 16 bit sub-blocks of key material.
- Between each round the second and the third blocks are swapped.

5. Procedures for testing

- a. Simulator: DAI SignalScan
- b. Source of test vectors: A publicly available C based source code will be compiled to generate plaintext/cipher pairs for verification.
- c. Format of input stimuli: All the testbench will be coded in Verilog as well. However, there will/might be communication between the C files that generate the test vectors. (i.e. a behavioral memory will be generated to save the test vectors and this will be introduced as the stimulus of the design)
- d. Performance parameters: Major parameters that the design will be developed around will be throughput, key setup time, time to encrypt one block, time to decrypt one block.
- e. Parameters to be determined using the implementation tools: The area and the speed will be the major parameters in the implementation. If time permits several advanced optimization techniques will be applied to improve the figures obtained from these parameters.

6. Plan of simulation experiments

- Develop a fully functional RTL hardware definition of the IDEA algorithm
- Develop testbenches to verify the functionality of submodules.
- Develop a top level stimulus testbench to verify overall functionality.
- Develop synthesis scripts that will optimize the design for different parameters.
- Run these scripts and obtain an optimized synthesized hardware.
- Examine the timing reports and reiterate the last steps in order to meet the specs.

7. Time schedule

Week	Oct 1	Oct 8	Oct 15	Oct 22	Oct 29	Nov 5	Nov 12	Nov 19	Nov 26	Dec 3	Dec 10
Define Project -Finalize Specs.											
Specification - Report Submit											
Implementation Subblocks											
Verification of Subblocks Testbench+Simulation											
Implementation of Top module											
Verification of Top Module Testbench+Simulation											
Synthesis script Development+ Logical Synthesis											
Optimization by applying different methods											
Project Report											
Project Presentation											

8. Possible Areas of Specification Changes

Specifications of the implementation described in this paper are based on the standard that has been listed in literatures. Therefore, no major changes expected in these specifications. However, some steps to be taken can be altered or modified in order to meet the timing requirements for the project work. For instance, the optimization techniques that will be applied is going to be limited to the amount of time that is available in the end of the timeline.

A probable follow-up to this work –in another context, e.g. second semester work - can be an FPGA implementation of the synthesized logic into a known board from Altera and/or Xilinx. And then performance analysis can be run on these boards and the results can be compared with the ASIC implementation proposed in the context of this project.

9. References

- [1]: http://www.cs.nps.navy.mil/curricula/tracks/security/notes/chap04_43.html
- [2]: <http://strato.visgraf.impa.br/tron/Livros/books/book10/9312e/9312e.htm>
- [3]: A. Curiger, H.Bonnenberg, R.Zimmerman, N.Felber, H.Kaeslin, and W.Fichtner. “VINCI:VLSI implementation of the new secret-key block cipher IDEA”. IEEE Custom Integrated Circuits Conference, 1993.
- [4]: W.Stallings, “Cryptography and Network Security: Principles and Practice, 3rd edition, Prentice Hall, Upper Saddle River, 2003.