COE 485 Senior Design Project (022)
Automation and VLSI #2
Design and Analysis of Encryption/Decryption Hardware

Mostafa Abd-El-Barr and Alaaeldin Amin

October 1, 2002

1. Objective

To design and analyze high performance circuits for encryption/decryption applications. The main circuits to design are modulo multipliers and dividers. The performance measures are speed, power, area, and testability.

2. Lecture Material

Introductory lectures will be given by course instructors covering the following topics.

(1) Sign Digit Arithmetic
(2) Multiplies Design
(3) Dividers Design
(4) Modulo Multiplication & Exponentiation
(5) Encryption/Decryption Schemes.

3. Project Nature

(a) **Multipliers**: design multiplication algorithms and high performance circuits for
   1. Montgomery
   2. High Radix Multiplication
   3. Others

(b) **Dividers**: design multiplication algorithms and high performance circuits for
   1. Binary Division
   2. High-Radix Division
   3. Others

(c) **Combined Division and Multiplication Circuits**: design multiplication algorithms and high performance circuits for
   1. The (4,2)
   2. Others

4. Required Simulation Language

Possibilities are: VHDL, Verilog, Java and C++. The use of Applet in Java is considered an added property, which allows step-by-step execution of various algorithms.

5. Required Number of students

Multipliers	**2-3**
Dividers	**2-3**
Combined Multipliers &Dividers	**3-4**
Modulo Multiplier & Exponentiation	**2-3**
Total	**9-13**

6. Expected Outcome

1. Algorithms (conventional and Parallel)
2. Simulation Programs
3. Circuit design
4. Circuit Simulation for performance analysis
5. Prototypes (may be using FPGAs)
6. Documentation