George Mason University  
Department of Electrical and Computer Engineering

Software/Hardware Co-design: A case study on implementation of RSA using Montgomery multiplication

MS Scholarly Paper Presentation

Navaneeth Garakahalli

Advisor: Dr. Kris Gaj

Day: Thursday, May 8, 2014  
Time: 5:30–6:15 PM  
Location: ENGR 2901

Abstract

Hardware design in general aims to deliver a product that is highly optimized for a specific application and ideal for performing operations in parallel. As an inherent drawback, once manufactured, a hardware chip cannot be modified. Software design on the other hand, offers flexibility. Once coded onto a general-purpose processor, it can be modified to suit the designer’s needs. As a drawback, it is executed sequentially. Software/hardware co-design is a design philosophy that is aimed at taking advantage of the best of both worlds. It aims at designing a system that is good at implementing both parallel and sequential operations.

Modular multiplication is one of the fundamental operations in many cryptographic algorithms. Modular exponentiation is at the heart of RSA, the most popular Public Key Cryptographic algorithm. Montgomery multiplication offers a method to perform modular multiplication that speeds up modular exponentiation. This method can take advantage of parallel execution, and hence hardware implementation may be close to optimal. Flexibility can be achieved by using a Nios II processor with a coprocessor used for Montgomery multiplication. This approach enables the sequential parts of this application to run on the Nios processor, while the computationally intensive modular exponentiation is moved to the coprocessor. This presentation discusses the merits and demerits of such an implementation approach.