Jérémy Barthélemy & Matt Drummond
Final Project
ECE 645

Montgomery Multiplication
Description

This project is based upon the Multiple-Word Radix-2 Montgomery Multiplication (MWR2MM) of Tenca and Koç. Specifically, two optimized versions of this architecture are present, described throughout this project as Architecture 1 (Arch1) and Architecture 2 (Arch2). Arch1 is a scalable optimization of the Tenca and Koç architecture while the alternative Arch2 was designed to greatly improve performance.

Architecture 1 and Architecture 2 are described in this paper:

M. Huang, K. Gaj, and T. El-Ghazawi, "New Hardware Architectures for Montgomery Modular Multiplication Algorithm," IEEE Transactions on Computers, vol. 60, no. 7, July 2011, pp. 923-936.

Below is a listing of other reference documents used for this project.

- MontgomeryMultiplication
- Gaj_Montgomery_Slides
- montgomeryBuell