Montgomery Ladder Exponentiation as a countermeasure against RSA timing attacks
CS290G Project Proposal

Hessen, Hans-Olav
hansolavhessen@gmail.com

Nygård, Arve
mail@arve.in

April 21, 2015

Abstract

For our project we want to implement the RSA algorithm on the UDOO board.

RSA relies on modular exponentiation. There are several ways to do this. A commonly used technique for doing the exponentiation is called Montgomery exponentiation. However, this technique is vulnerable to timing attacks. We will implement RSA using both the standard Montgomery exponentiation and an alternative technique called Montgomery powering ladder, and show that the latter is resistant to timing attacks. Finally we will compare the execution time of each implementation, and assess how suitable the Montgomery ladder implementation is for practical use on a low-end device such as the UDOO.

We will analyze the trade-off between added security and performance, and conclude what implementation is applicable for this device.

The biggest challenge for this project will be the short time frame and our limited experience using the UDOO.

1 Introduction (placeholder)

Short introduction about RSA, and the two exponentiation methods, as well as the UDOO board.

2 Algorithm walkthrough (placeholder)

RSA, Montgomery ladder, Montgomery exponentiation pseudo code