RSA Implementation and Timing Attack on the UDOO Board

Sondre Basma, Emil Grønnbeck, Magnus Ohm

April 24, 2015

Abstract

We would like to implement the RSA algorithm on the UDOO board using the Montgomery Exponentiation Method. Our intention is to exploit the timing difference exposed by the extra reduction step in order to get access to the private key. The first phase will be to install Linux on the UDOO board, and use Python to implement the RSA algorithm with the Montgomery Exponentiation method.

The second phase is what we believe to be the most time consuming. It involves implementing a timing attack on our RSA implementation, it also involves gathering the timing data and analyzing it in order to deduce the bits used in the private key. Our intention is to use Python for this as well, though we also see the possibility that the language might be too contained, obscuring the data we want to collect. In that case we will use C for the data gathering.