Thesis Plan

Marcel van der Made

July 2, 2017

Basic info

Following the TRU/e Digital Security Master, my thesis subject will be about security as well. To be more precise, my thesis will be about optimizing a new algorithm for a specific micro controller. My project started in the second semester of the college-year 2016-2017. I plan to finish my thesis as soon as possible.Currently, this is estimated to be in the start of the first semester of 2017-2018. The thesis will be supervised by Peter Schwabe.

The problem

Last year, a new cipher was proposed, named McBits: https://binary.cr.yp.to/mcbits.html. This cipher is resistant to side-channel attacks, and is future-proof. That is to say, the cipher will still be secure when quantum computers arrive.

For my thesis I will take this cipher, written in C, and run it on a Cortex M4 microprocessor. Then, I will make the decrypting function as fast as possible. So, as few clock-cycles as possible. The M4 device has limited memory: only 128kb. This means that the public key will not fit on the device. The secret key however does fit, making it possible to perform decryption, once the key is stored on the device. Because of this limitation, I will only consider the decrypting functionality in the speed-up process.

The plan

First things first: get the program running on the M4 micro controller. Using dependancies from SuperCop http://bench.cr.yp.to/call-encrypt.html I will compile the program and generate a key pair on a normal computer. Besides this, we will also need a cipher text to decrypt. Once these are generated, I will have to send these to the device to store them in memory. This will be done by writing a custom main-function which will communicate with the computer. Both the secret key and the cipher text will be send to the M4 device.

Once I got the data I need, I will run the program as-is, to get base measurement of how many clock-cycles the program uses. From there onwards, I will research about optimizing C code, and applying this in the McBits algorithm. During this process, I will measure the speeds which are achieved so far. Finally, I will be able to compare these speeds to other algorithms, some of which are also mentioned in the McBits paper. All that remains then is to write the paper accompanying the project.