Low Power Hardware Accelerated Internet of Things Cryptography

Author: Lewis Smith
Supervisor: Mark Zwolinski

October 12, 2017

The last few years has seen the rapid emergence of internet connected domestic devices dubbed "Internet of Things" or "IoT". These devices range from the trivial light switch or thermostat controlled through the internet to a more complex networked self driving car or possibly door and safe locks. These IoT devices work by transferring data, which can be commands or possibly sensitive and private information, through the internet between the device and the user. Thus to keep potential adversaries from accessing the private information or controlling the numerous internet connected appliances, maliciously or not, a layer of encryption is usually used, with the decryption key only known by the specified users. This encryption can be achieved through software on a processor or on dedicated hardware like Application Specific Integrated Circuits (ASIC) or Field Programmable Gate Arrays (FPGA). As many IoT devices are small embedded processors there isn't much available program space available to store the encryption algorithms so hardware accelerated encryption is probably a better solution. Dedicated hardware can also, theoretically, perform the algorithms faster and more accurately. However, due to the fact that most IoT devices are always on, power consumption is a very important factor when considering options for adding hardware accelerated encryption and for battery powered devices is often more critical than the actual encryption.

The goals of this project are to explore various encryption algorithms and compare their performance based on data throughput, accuracy, security and power consumption when implemented in software and hardware. To evaluate these parameters the same algorithms can be coded in C or C++ for the software versions and a Hardware Development Language (HDL) such as System Verilog can be first simulated in ModelSim before programming a FPGA for the hardware version. These comparisons can then be used to match the algorithms to the appropriate IoT device as they all have different requirements for relative security level and power consumption, as for example a light switch does not necessarily need to be protected from the same level of attack as a set of digital locks or private data storage. In order for the hardware to work with IoT devices it will also need a communication protocol like I^2C or SPI to work with embedded processors, and possibly Ethernet or WiFi to act as the gateway to internet for the device. Some of these protocols are available on FPGA development boards but can be implemented in System Verilog code.

The scope of this project is therefore to develop encryption algorithms in System Verilog for a FPGA and compare their performance to the equivalent software before applying the hardware to actual IoT devices. Also if more time is available then a layout, based on the System Verilog synthesis, could be developed for ASIC fabrication in the future which could increase efficiency of the hardware due to the fact that only the required circuitry would be present on the chip.

By the progress report deadline in December the various algorithms need to identified and matched to an IoT device and developed and tested in software. Ideally the System Verilog development will have also been started by christmas which will be tested using Modelsim testbenches before programmed and tested on a FPGA before Easter.