ECE6960Final Project Proposal

Todd Renner & <TBD>

Introduction

The world of IoT has been rapidly expanding and created the need for a changing face of security measures given the limited size and power of some of these new devices. For example, implanted medical devices have been developed that rely on communication with external devices to support such processes as gathering metrics, data analysis, and functional equipment support. While all of these processes are important to safeguard, it is easy to see how insidious the reality of an untrusted third-party taking control of someone's insulin pump or pacemaker could be.

In order to ensure protected communication in these instances, powerful encryption schemes have been adjusted for lightweight applications wherein size and power have been optimized without sacrificing throughput and security. One such hardware implementation is the SIMON block cipher developed by the NSA in 2013 [1]. This cipher boasts minimal hardware footprints without sacrificing throughput when compared to the top ciphers at the time of publication [1]. The focus of this project will be implementing a 64-bit SIMON block cipher with a 128-bit key in VHDL for the purpose of encryption/decryption.

SIMON64/128 consists of 44 rounds. Each round is identical and consists of bitwise XORs, addition modulo 2^n, and circular shifts S^j. The encryption round function is as follows:

$$R_k(x, y) = (y \oplus f(x) \oplus k, x)$$

For decryption, the round functions are as follows:

$$R_k^{-1}(x, y) = (y, x \oplus f(x) \oplus k)$$

Where $f(x)$ is defined as:

$$f(x) = (S^1 x \; AND \; S^8 x) \oplus S^2 x$$

From a given key, 44 round keys are generated which depend on a 62-bit period sequence of round constants in addition to a cipher constant defined as

$$c = 2^{n=44} - 4$$

Proposed Milestones

To achieve the implementation of SIMON64/128, the following milestones will be reached by the project deadline of May 7.

- Full implementation of SIM64/128 in VHDL with associated testbenches
- Demonstration of successful encryption/decryption of an image file
- *Optional*: Demonstration of encrypted transmission OTA using the U's POWDER network
    - This is time and POWDER resource dependent. Requires authorization.