**Lab 1 - SIMON encryption/decryption**

Group 4:

Joseph Burke  
Idan G. Kanter  
Seth Rausch

ECE 459 - Secure & Trustworthy Computer Hardware Design

Spring 2017

Dr. Garrett S. Rose

January 28 2017

Instructor Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Abstract/Introduction**

The field of security in software and hardware was always an important subject. A few encryption algorithms were introduced including the older Data Encryption Standard (DES), and the newer Advanced Encryption Standard (AES). AES is considered to be a very strong non-Feistel encryption algorithm; however, it is also considered heavyweight; AES requires heavy usage of the system resources as memory, area, and power. Due to the rising need of a more lightweight encryption algorithm for FPGAs, ASICs, Internet of Things (IOT), embedded systems, and more, a team at the National Security Agency (NSA) introduced the SIMON block cipher algorithm which is optimized for hardware. SIMON is a Feistel encryption algorithm that uses less system resources than the AES, which makes it suitable for small systems that were introduced above.

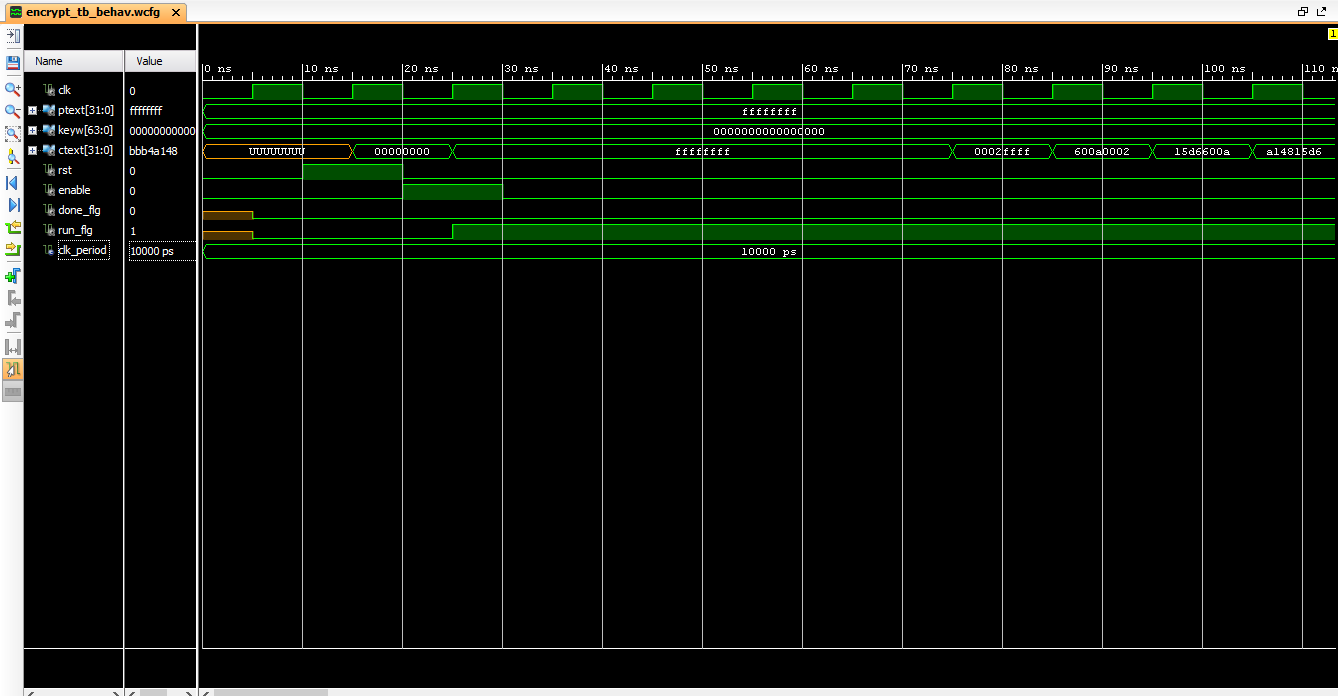
The purpose of the lab is to learn how SIMON works and to implement some of its functions. After reading two papers about the implementation of SIMON, the round and the key expansion function are implemented. After the algorithm is completed, some test benches are run to simulate the encryption. Next, the program is synthesized, implemented, and is generated to a bit file for testing on a Nexys-4 FPGA board. Finally, the implementation is programmed to the board and the program encrypts two image files. In addition, the FPGA is used to test the decryption of the images since SIMON is a Feistel algorithm. During the whole process, interesting features, observations, and shortcomings of SIMON are recorded.

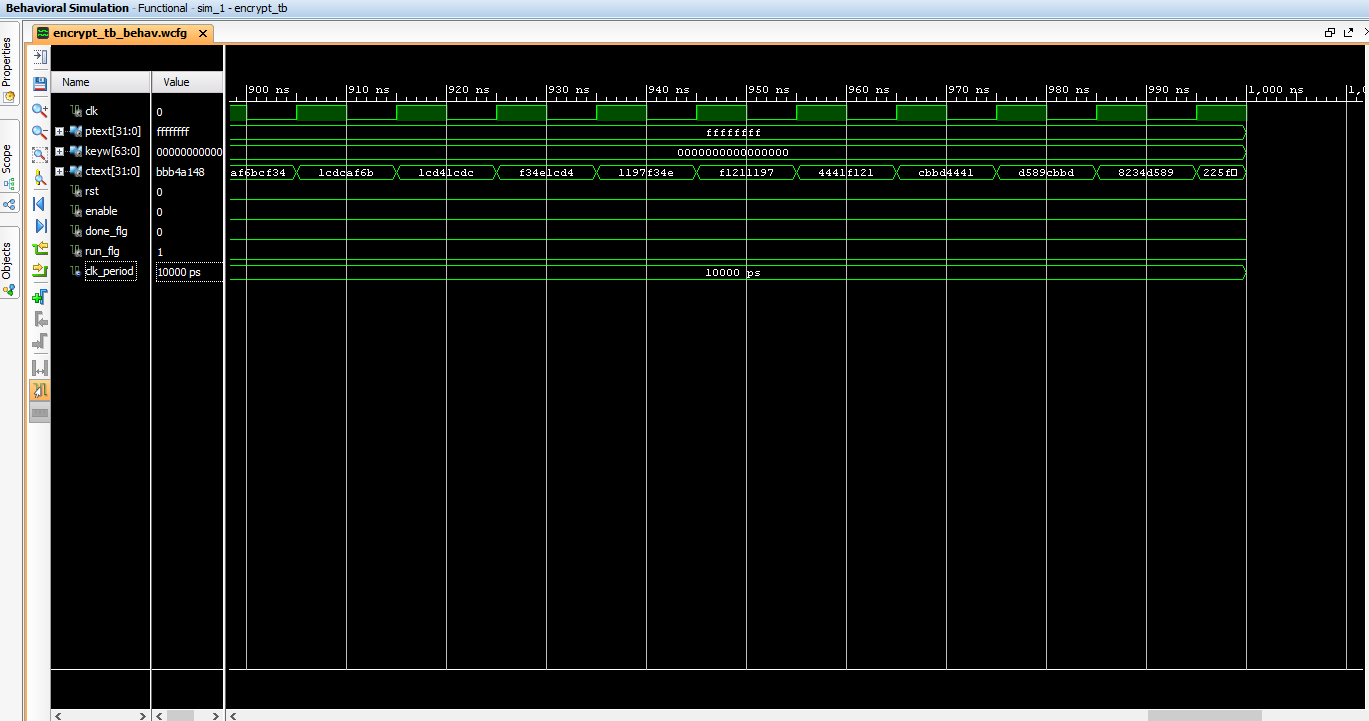
**Results**

**Observations**

**Appendix**

**encrypt\_tb.vhd – Simulation Output Snapshot**

** 10 ns – 110 ns**

**900 ns – 1000 ns**