Computer Engineering Design Project Proposal

May 3, 2010

Title: *Design of a High Speed Self-Synchronizing Encryption System*
Client: *Dr. Howard Heys,* hheys@mun.ca*, 737-2514*
Supervisor: *Dr. Howard Heys*

Description

The objective of this project will be to design an FPGA-based system targeted to providing a prototype system of high speed encryption for physical layer synchronous communication. The required design will use Pipelined Statistical Cipher Feedback (PSCFB) mode [1] to achieve high data speeds while ensuring robustness in relation to channel errors and synchronization losses. PSCFB is an extension of SCFB, analyzed in [2], and is intended to achieve high speeds similar to pipelined implementations of the Advanced Encryption Standard (AES) [3] configured for counter mode. The project will consist of the development of the following components:

(1) FPGA-based PSCFB system using AES

A board level design of an FPGA system must be completed and configured with the PSCFB system, which is to be coded using VHDL, simulated, and synthesized using appropriate tools.

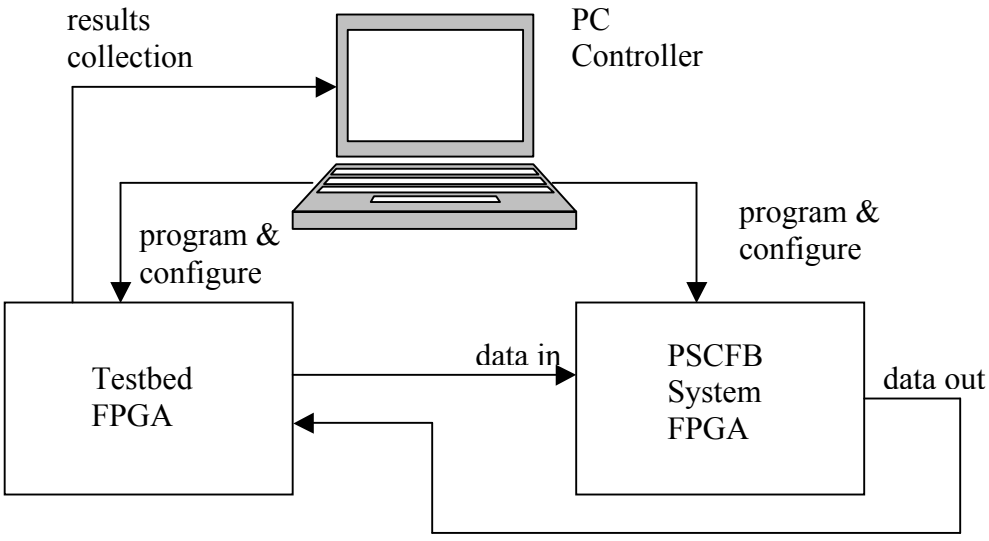
(2) FPGA-based testbed

The testbed is a system that will be used to test the functionality of the PSCFB board. A board level design of an FPGA system must be completed and configured with the testbed system, which is to be coded using VHDL, simulated, and synthesized using appropriate tools.

(3) PC Controller

The PC must interface to both the PSCFB FPGA board and the testbed FPGA board for the purposes of programming the hardware and configuring the corresponding system. As well, the PC will collect the results of the testing and present to the user.

A simple diagram of the overall system is shown below.



Roles

Team Member #1 (Computer Engineer)

Responsibilities:

(1) Design, test, and implementation of pipelined AES architecture
(2) Secondary on PSCFB board design
(3) PC interfacing to PSCFB system

Utilized Skills:

(1) VHDL design entry and FPGA design tools for functional simulation and synthesis
(2) FPGA board level design

Team Member #2 (Computer Engineer)

Responsibilities:

(1) Design, test, and implementation of PSCFB queuing architecture
(2) Secondary on PSCFB board design

Utilized Skills:

(1) VHDL design entry and FPGA design tools for functional simulation and synthesis
(2) FPGA board level design

Team Member #3 (Computer Engineer)

Responsibilities:

(1) FPGA board level design for both PSCFB and testbed systems
(2) Design, test, and implementation of testbed system
(3) PC interfacing to testbed system

Utilized Skills:

(1) FPGA board level design
(2) VHDL design entry and FPGA design tools for functional simulation and synthesis

References

[1] H.M. Heys and L. Zhang, "Pipelined Statistical Cipher Feedback Mode: A New Mode for Self-Synchronizing Stream Encryption", available from H. Heys.

[2] H.M. Heys, "Analysis of the Statistical Cipher Feedback Mode of Block Ciphers", *IEEE Tranactions on Computer Engineering,* vol. 52, no. 1, Jan. 2003.

[3] National Institute of Standards and Technology, *Advanced Encryption Standard*, Federal Information Processing Standards (FIPS) Publication 197, Nov. 2001.