Design for Security: Assignment 1

February 3, 2023

Adders and Subtractors

- Design a 64 bit Adder using FPGA carry chains. Your design should not consume more than 32 carry chains for this implementation.
- Design a 64 bit combined adder and subtractor using FPGA carry chains.
- Design a 64-bit multilevel carry look-ahead adder using 4-bit look-ahead blocks. Your design should not have more than three levels of carry look-ahead block. Try to use carry chain for this design if possible. Compare the performance of this adder with the standard adder that you have implemented for question no: 1.

Finite field Adders

- Design a finite field adder for GF(p) where $p = 2^{255} - 19$. The basic building block will be the 64-bit adder and subtractor that you have designed in the previous section. The design should be implemented in a pipelined manner.

Finite field multiplication

- In this design, we would like to implement a finite field multiplier in $GF(2^m)$ where the underlying primitive polynomial is $x^{233} + x^{74} + 1$.

  Hint: Develop a combinatorial design of Karatsuba multipliers for binary polynomial multiplication with degree 233. Then apply fast trinomial reduction for reducing the multiplication result.

- In this design, we would like to implement a finite field multiplier in $GF(p)$ where the underlying prime is $2^{255} - 19$.

  Hint: Use DSP blocks to develop a multiplier for multiplying two integers of 255 bits. Then apply fast pseudo-Mersenne prime reduction methodology for reducing the result.

- Develop a Montgomery multiplication architecture for finite field multiplication in $GF(p)$ where p is a prime of length 255.