Indian Institute of Technology Kharagpur

SPRING Semester, 2023
COMPUTER SCIENCE AND ENGINEERING

CS60004: Hardware Security

Coding Assignment 1

Full Marks: 20

1. Write a Verilog code for computing $C(x) = A(x) * B(x)$ where $A(x)$ and $B(x)$ belong to $GF(2^{163})$. Consider the irreducible polynomial for the field as $x^{163} + x^{80} + x^{47} + x^{9} + 1$. Use the Karatsuba multiplication technique as discussed in class. Submit the source files with a proper test bench.

Sample Test vectors are as follows:

(a) $A = 163'h8000000000000000000000000000000000000000000000001$
$B = 163'h8000000000000000000000000000000000000000000000001$
$C = 163'h4000000000000000000000000000000000000000000000002000000000000000001$

(b) $A = 163'h8100000000000000000000000000000000000000000000001$
$B = 163'h8200000000000000000000000000000000000000000000001$
$C = 163'h4800000000000000000000000000000000000000000000000201000000000000000001$

(c) $A = 163'h7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
$FFFFFFFFFFFFFF$
$B = 163'h7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
$FFFFFFFFFFFFFF$
$C = 163'h3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
$FFFFFFFFFFFFE00000000000000000000000000000000000000000000000001$

(20 marks)