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:

- - C = 163'h01059b64800000000000438f160801068b040001
- - C = 163'h5000000000000000001555ffffffaaaaaabfeaa

(20 marks)