Indian Institute of Technology Kharagpur

SPRING Semester, 2023
COMPUTER SCIENCE AND ENGINEERING

CS60004: Hardware Security

Class Test – 1

Full Marks: 30

Time allowed: 1 hour

1. The addition chains in the *Itoh-Tsujii* inversion algorithm are used to reduce the number of multiplications required. Let $a \in GF(2^{193})$ and you are asked to find a^{-1} using following addition chain

$$[1, 2, 4, 8, 16, 32, 64, 128, 192]$$

Based on the given information, answer the following three questions.

(a) What is the number of squaring and multiplications required in a naïve implementation without an addition chain? (4 marks)

(b) What is the number of squaring and multiplications required in an implementation with an addition chain? (4 marks)

(c) While implementing the *Itoh-Tsujii* Algorithm on FPGA, the delay of a squarer circuit and a quad circuit are the same. Give reasons. (2 marks)

2. Implement the squarer circuit in $GF(2^4)$ with modulus polynomial $x^4 + x^3 + 1$. Derive the expression for the square of an element $a \in GF(2^4)$ and implement the circuit using 4-input LUTs. (10 marks)

3. Implement the circuit to compute the modulo of multiplication of two polynomials $a(x), b(x) \in GF(2^{233})$ using modulo polynomial $m(x) = x^{233} + x^{159} + 1$, i.e. compute the product as $a(x).b(x) \bmod(m(x))$. Find the critical path of the circuit. (10 marks)
