INDIAN STATISTICAL INSTITUTE
Semester Examination
M. Tech. (CrS) II year, 1st Sem, AY 2021–2022
Cryptographic and Security Implementations

Date: 09-02-2022 Submission Time: Midnight of 11-02-2022

Total Marks: 80

1. Consider the following C-code of the function `Swap` which takes three integers `x1`, `x2` and `n` as input. Assume that `n` $\in \{0, 1\}$. Write a modified version of `Swap` which does not use conditional instructions like `if-else` condition, and any form of integer multiplication and division.

```
void Swap(int x1, int x2, int n){
    int t;
    if(n=1){
      t=x2; x2=x1; x1=t;
    }
}
```

[15]

2. Let $\mathbb{F}_p$ be a prime field where $p = 2^{61} - 1$ is a prime. Let us define a Montgomery elliptic curve over $\mathbb{F}_p$ as

$$E_M : By^2 = x^3 + Ax^2 + x,$$

where $A, B \in \mathbb{F}_p$ and $B(A^2 - 4) \neq 0$. E_M is defined by the following values

$$\begin{aligned} A &= 798026816538591017 \pmod p, \text{ and} \\ B &= 1 \pmod p. \end{aligned}$$

Let $P = (576568326687948115, 2075987454224306306)$ be a generator of the largest prime subgroup of E_M and order of P is $\text{ord}(P) = 576460752315733303$.

   (a) Write a C program to compute scalar multiplication nP where $n < \text{ord}(P)$. Your code must satisfy the following conditions.
      i. Each field element must be represented using base 2^{31}.
      ii. Field multiplication must use the Karatsuba multiplication algorithm.
      iii. Use x-coordinate only Montgomery ladder scalar multiplication algorithm.
      iv. Use the projective coordinate system for scalar multiplication.
      v. Each ladder step must not use any conditional instruction like `if-else` condition. Use of unnecessary conditional instructions will be subject to marks reduction.

   (b) Let the output of the scalar multiplication be $nP = (x_n, \cdot, z_n)$ in projective coordinate system. Convert the output from the projective coordinate system to the affine coordinate as $nP = (x_n/z_n, \cdot)$. Inversion must be computed using Eular's theorem. Otherwise **zero** will be awarded.

[(10+40)+15 = 65]