Indian Institute of Technology (IIT-Kharagpur)

SPRING Semester, 2022
COMPUTER SCIENCE AND ENGINEERING

CS60004: Hardware Security

Graded Tutorial

Full Marks: 20

Time allowed: 1 hour

1. Consider the following algorithm for computing modular exponentiation used in the RSA cipher. Our objective is to ascertain the scalar k using side-channel analysis.

Algorithm 1: RSA Modular Exponentiation

```
Data: Base: X, Secret Exponent k = k_{n-1}, k_{n-2}, ..., k_0 and modulus N
Result: Q = X^k
R_0 → 1 ; R_1 → X ;
for i = n − 1 downto 0 do
    R_[1−k_i] → (R_0 × R_1) mod N;
    R_{k_i} = (R_{k_i}^2) mod N ;
return Q = R_0 ;
```

You are also given the power trace values of the 10 exponentiations with different values of the base X, for 8 leakage points, as shown in Table 1. The value of N is 4763.

You are given that the value of $(n-1)^{th}$ bit of k is 1. Find out the value of $(n-2)^{th}$ bit of the k using Correlation Power Analysis (CPA). Assume that the leakage model is Hamming weight.

Table 1: Power Trace Value of RSA execution

Execution No	X	Leakage of $(n-1)^{th}$ bit	Leakage of $(n-2)^{th}$ bit	Leakage of $(n-3)^{th}$ bit	Leakage of $(n-4)^{th}$ bit	Leakage of $(n-5)^{th}$ bit	Leakage of $(n-6)^{th}$ bit	Leakage of $(n-7)^{th}$ bit	Leakage of $(n-8)^{th}$ bit
1	810	13	12	9	12	11	12	10	7
2	891	15	13	7	14	9	17	11	11
3	789	10	11	13	9	12	14	16	8
4	431	8	8	6	6	12	13	10	13
5	918	11	10	9	9	13	11	13	13
6	862	8	6	6	12	10	10	13	9
7	706	8	9	13	16	15	7	12	13
8	742	11	11	13	14	19	7	14	12
9	53	12	12	15	8	14	12	12	12
10	408	10	14	10	12	10	19	11	10

(20 marks)