Indian Institute of Technology (IIT-Kharagpur)

SPRING Semester, 2022

COMPUTER SCIENCE AND ENGINEERING

CS60004: Hardware Security

Class Test I

Full Marks: 30

Time allowed: 1 hour

1. Consider a field $GF(2^m)$ where m is even. The field is constructed using an irreducible polynomial $P(x) = x^m + x^n + 1$, where n is odd, and $n < m/2$. Any element of the field can be expressed as $A(x) = \sum_{i=0}^{m} a_i x^i$, where the coefficients $a_i \in \{0, 1\}$

We would like to perform the operation $C(x) = (A(x))^2 \, mod \, P(x)$. Derive the equations to express the i$^{\text{th}}$ coefficient of $C(x)$, denoted as c_i where $0 \leq i \leq (m-1)$, in terms of the coefficients of $A(x)$. Split your derivation into the following four classes:

(a) i even, $i < n$ or $i \geq 2n$

(b) i even, $n < i < 2n$

(c) i odd, $i < n$

(d) i odd, $i \geq n$

(10 marks)

2. Let us consider a toy cipher as depicted in Figure 1. The SBOX in Figure 1 follows the map as depicted in Table 1. Now if we consider two sample ciphertexts 1 and 8, show that this cipher is susceptible to differential cryptanalysis.

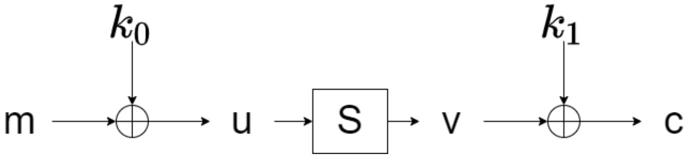

Figure 1: Structure of the toy cipher

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[X]$	6	4	C	5	0	7	2	E	1	F	3	D	8	A	9	B

Table 1: The S-Box

(8 marks)

3. Why does the last round of AES not have mix column operation? (2 marks)

4. Consider the following program which sorts an array of N numbers that are arranged according to a *secret file*. The output of the program is the sorted array. For instance, if

```
B = {3, 1, 2, 5, 4}
choose 5 random integers say 10, 54, 22, 64, 33
A = {33, 10, 22, 64, 54}
Note, that 33 is the 3rd smallest element in A,
           10 is the 1st smallest element in A,
           22 is the 2nd smallest element in A, etc.
```

Describe a way that you can determine B using timing channels. You have black box access to the function and are allowed to invoke it as many times as needed.

```
#define N  5
swapper(int *A){
   int i, j, tmp;
   int B[N];

   /* 1. Read a random permutation of {1,2,3,..., N} from file "Secret" into array B */
   /* 2. Fill N random integers into array A such that
         A[i] is the B[i]-th smallest element in the array */
   /*   (Assume that operations 1 and 2 execute in constant time) */

   /* 3. Sort A */
   for(i=0; i<N-1; ++i){
       for(j=i+1; j<N; ++j){
          if (A[i] > A[j]){
             tmp = A[i];
             A[i] = A[j];
             A[j] = tmp;
          }
       }
   }

}
```

HINT : **Connect this to Kocher's timing attack on RSA by noting that every swap results in a different timing from no swapping. Note that the attacker needs to obtain the array arrangement A which is input to Step 3 of the above code. In the example, if the attacker is able to obtain the value of $A = \{33, 10, 22, 64, 54\}$, B is revealed.**

(10 marks)