Indian Institute of Technology Kharagpur

SPRING Semester, 2023

COMPUTER SCIENCE AND ENGINEERING

CS60004: Hardware Security

Tutorial – 1

Full Marks: 50

1. Consider a toy cipher as shown in Figure 1 implemented on a smart card. The cipher has a 4 bit plaintext which is not visible to the adversary. However, the adversary has access to the ciphertexts and also the corresponding power consumptions which are represented as integer values. The S-Box of the cipher is given in the following table.

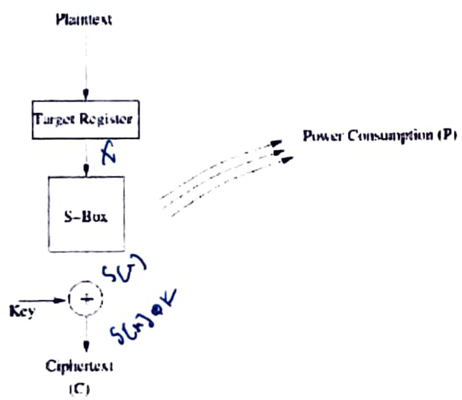

Figure 1: Power Attack

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

K 0101

C K

Table 1: The S-Box

The adversary runs the encryptions several times until it obtains all the unique 16 ciphertext values (denoted as C in Figure 1) at least once. It also notes the corresponding power values denoted as P as given in the following table.

C	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
P	10	15	20	5	10	5	5	15	15	5	10	10	0	15	10	10

Table 2: The Power Profile

(a) You are told that the key is either 0101 or 1010. Apply the Difference-of-Mean (DOM) technique to determine which is the correct key byte. **Target the MSB of the input of the S-Box.**

(10 marks)

2. 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 $k = k_{n-1}, k_{n-2}, \ldots, k_0$ and modulus N
Result: $Q = X^k$

$R_0 \rightarrow 1$; $R_1 \rightarrow X$;
for $i = n - 1$ *to* 0 **do**
  $R_{[1-k_i]} \rightarrow (R_0 \times R_1) \bmod N$;
  $R_{k_i} = (R_{k_i}^2) \bmod N$;
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 3. 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 3: 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)

3. 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.** (20 marks)