M2 Cyber security - SmartCards Security - 2022

1. Security evaluations for a SmartCard [3/20]

1.1. How many security levels (Evaluation Assurance Levels) are defined in the Common Criteria?

1.2. Which is the level that should obtain a SmartCard used for banking transaction?

1.3. Describe the tools used during an invasive probing attack on embedded devices.

1.4. Describe at least 2 specific tools you can use to perform a perturbation attack.

2. RSA attack [7/20]

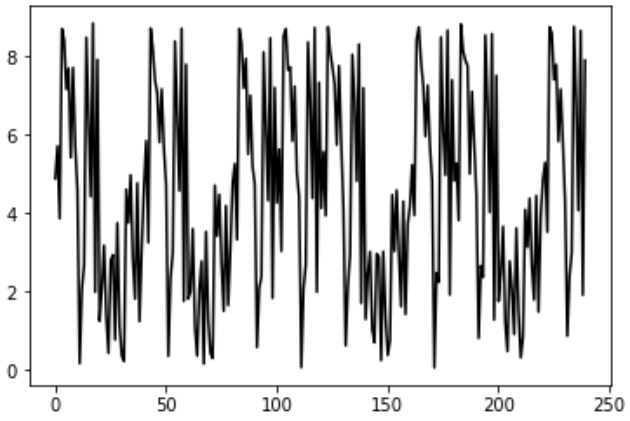
A chip performs a modular exponentiation $C = M^d$ where d is the private key you want to retrieve. The algorithm used is described below.

Algorithm 1 Calculate $C = M \times d \mod n$ with $d = [d_{n-1}..d_0]$ d_0 being the Least Significant Bit. ex: d=0d13=0b1101 = [1101]

1: $C \leftarrow 1$, $R \leftarrow M$
2: **for** $i = 0$ to $n - 1$ **do**
3: **if** $d_i = 1$ **then**
4: $C \leftarrow C \times R \mod n$
5: **end if**
6: $R \leftarrow R^2 \mod n$
7: **end for**
8: **return** Q

2.1. A consumption curve is recorded during the processing of this algorithm. Describe the experimental set-up to acquire such a curve.

2.2. Retrieve one byte of the private key with the help of the curve.



2.3. Propose an improvement to this algorithm such that the previous attack is not possible anymore.

2.4. Is this new algorithm is safe against perturbation attacks? Explain why.

3. Verify PIN [7/20]

A developer implemented a user authentication with a 4-digit PIN code. The goal of the attack is to authenticate yourself without knowing the real PIN code (i.e. function `Verify_PIN` shall return `true`). Number of tries is limited to 100 and controlled by variable `tries` stored in a Non Volatile Memory. When this variable is below 0, the function `kill_card()` destroys the SmartCard. For this evaluation, the developer gave you the C code used in this function. It is reproduced below:

```
1  const int true = 0x1234;
2  const int false = 0x9876;
3  extern void kill_card(void);
4  int tries = 100; // permanently stored & updated in a Non Volatile Memory
5  int correct_PIN[4] = {9,8,7,6};
6
7  int verifyPIN_1(int user_PIN[]){
8    int correct_digits = 0;
9    if (tries < 0) kill_card();
10   tries--;
11   for (int i=0; i < 4; i++) {
12     if(user_PIN[i] != correct_PIN[i])
13       correct_digits --;
14     else
15       correct_digits ++;}
16   if (correct_digits == 4){
17     tries ++;
18     return true;}
19   else
20     return false;}
```

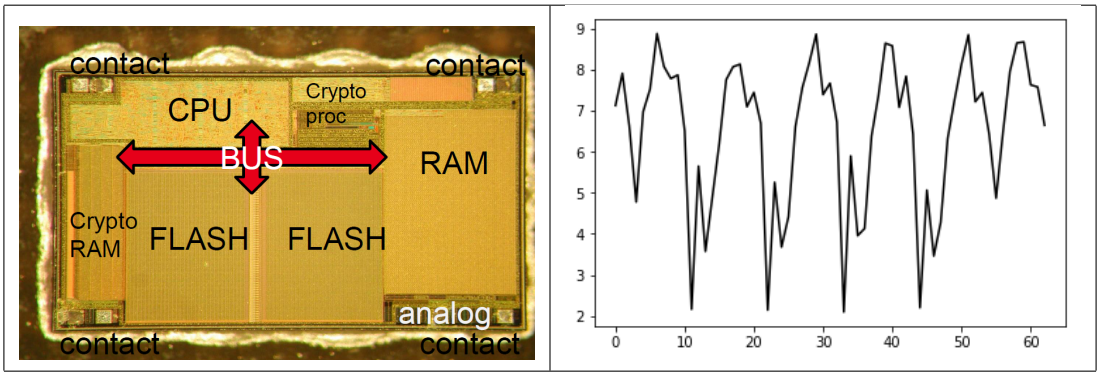
Explain the countermeasures at the following lines. Why and against which kind of attacks have they been inserted ?

3.1. lines 1-2

3.2. lines 12 to 15

3.3. lines 9 and 16

3.4. The figure below shows a chip picture as well as electromagnetic leakages recorded when the preceding code is run on the chip. Propose a single fault attack that allows to be authenticated without knowning the PIN code. Indicate where and when to attack the chip.



4. Symmetric cipher [3/20]

4.1. Explain shortly how to perform a Side Channel attack on an AES.

4.2. What is a Differential Fault Attack (DFA) on a symmetric cipher?

4.3. How many faults and what kind of faults do you need to succeed a Piret and Quisquater DFA on AES?