M2 Cyber security - SmartCards Security - 2020

The goal is to evaluate the security of a device. The purpose of the whole test is to retrieve a secret key - denoted k - stored inside the chip.

1. Attacking a physical device [4/20]

1.1. Cite the 3 different types of physical attacks that you could perform on a device, with a short rationale explaining some their advantages and drawbacks.

1.2. This device is certified by the Common Criteria at the level EAL5. Against what kinds of attacks this device is supposed to be secured ?

Actually it seems that the certification lab has not done a great job and that attacks are still possible. This will be the following of the test.

2. Symetric cipher [5/20]

The device uses a symetric cipher, with the secret key k. The developer gave you the secret and proprietary code to cipher a message.

A part of the algorithm has eventually been retrieved and is explained below. The idea is to find the secret key with a side-channel attack targetting chip consumption, knowing the message can be chosen by the attacker.

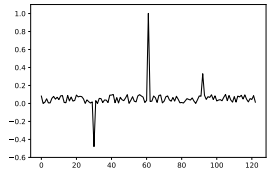
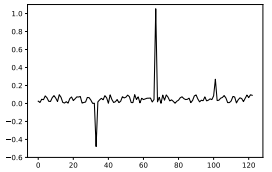
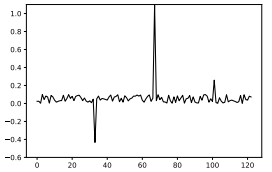
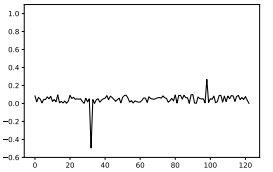
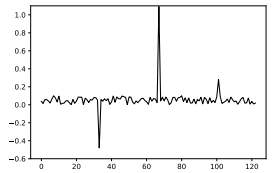
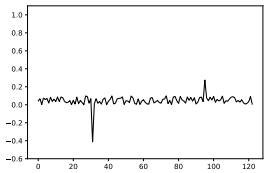
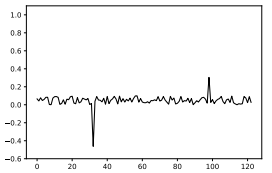
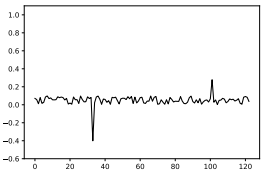
The algorithm uses a messsage m (3 bits) and a key k (2 bits), and calculates:

- $C(m,k) = \text{SBox}[m \oplus k]$
- SBox[] = [0x5, 0x3, 0x2, 0x7, 0x4, 0x1, 0x2, 0x0]

2.1. Complete the following table with the missing value for $C(m,k)$.

k/m	000	001	010	011	100	101	110	111
00	101	011	010	111	100	001	010	000
01	011	101	111	010	001	100	000	?
10	010	111	101	011	010	000	100	001
11	111	010	011	101	000	010	001	100

Using the set of acquired curves for different messages (0b000, 0b001 ..., 0b111) , the following means have been computed:

Message	000	001	010	011
Curve				
Message	100	101	110	111
Curve				

2.2. Find the time position(s) on the curve where the chip may leak ?

2.3. Retrieve the correct key with a DPA targeting the third bit (the last one in bold: 0bxx**X**?)

2.4. What would you advice to the developer to enhance its chip security ?

3. Asymetric cryptography [11/20]

The chip has also an asymmetric cipher scheme to initiate a secure communication protocol. It is used to store the secret key k. The developer was scared of the Bellcore attack on RSA symetric cryptography so she decided to use an Elliptic Curve Cryptography (ECC) scheme.

3.1. Desribe briefly the Bellcore attack with emphasis on the reasons why this attack is powerful.

Elliptic curve reminder The Communication between card and reader is ciphered with a common shared key given by ECDH (Elliptic Curve Diffie Hellman) protocol. From an elliptic curve C and an initial point P (both public), the scalar multiplication by k is defined as follows: $Q = k \times P = P + \ldots + P$ (k times).

Protection is based on the very difficult problem to retrieve k knowing P and Q.

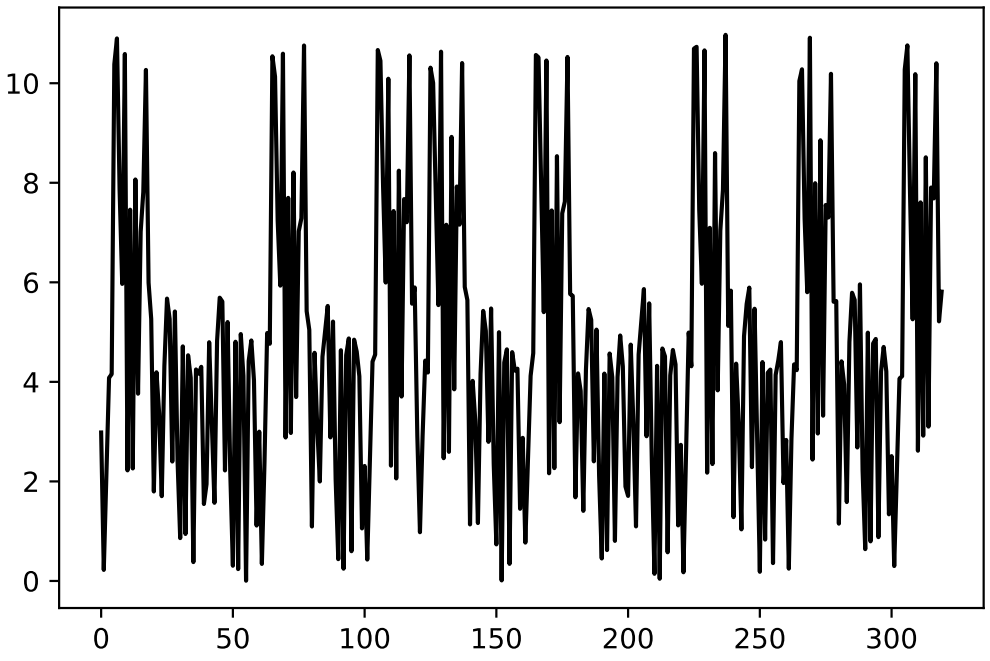
Algorithm 1 Calculate $Q = k \times P$ with $k = [k_{n-1}..k_0]$ k_0 being the Least Significant Bit. ex: k=0d13=[1101]

```
1: Q ← 0, R ← 0
2: for i = 0 to n − 1 do
3:    if k_i = 1 then
4:       Q ← ADD_POINT(Q, P)
5:       P ← DOUBLE_POINT(P)
6:    end if
7:    if k_i = 0 then
8:       P ← DOUBLE_POINT(P)
9:       R ← ADD_POINT(R, P)
10:   end if
11: end for
12: return Q
```

3.2. Describe every step of this algorithm in case k=0d9. Check that it indeed calculates the point scalar multiplication.

3.3. Find a vulnerability that could be exploited in a side-channel attack.

A chip power consumption trace for the first byte of the key is shown below.

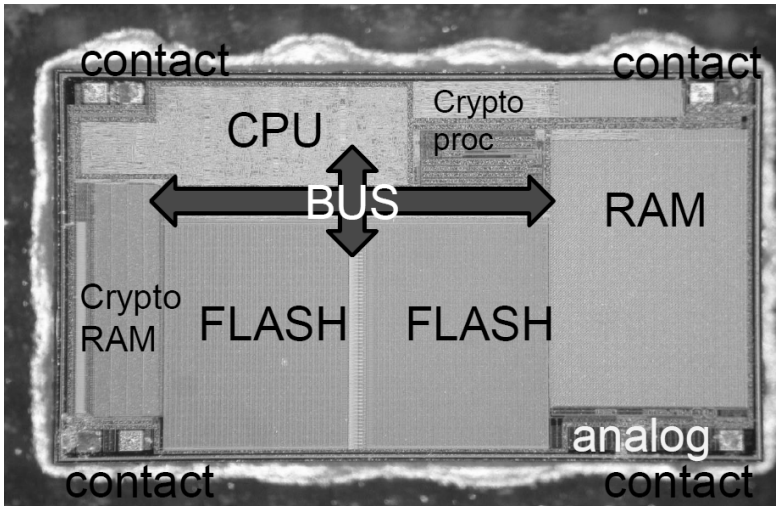


3.4. Retrieve the first byte of the secret key, with the help of the power consumption trace above.

3.5. Propose a quick fixin ($<=$ 2 modified lines) to this algorithm to get rid of this attack.

This correction begin made, the attacker must now perform a perturbation attack. Jumping over one line of the algorithm is taken as the fault model (i.e. type of faults that the attacker can do).

3.6. What is the purpose of R variable ? Find a pertubation attack that can be done on the corrected algorithm: which line(s) would you attack ? What for ? Where on the chip ? How many faults should be performed to retrieve the whole key ?



3.7. State a proper countermeasure against this attack.

Another possibility to protect this code is to blind/mask the key with a random value r.

3.8. How would you modify the above algorithm in order to mask k ?

3.9. Against which types of attack will it protect ECC protocol ?