M2 Cyber security - Smart Card Security
Attaques sur un badge sécurisé
Attacks on security badge

L. Maingault, M.- A. Cornélie

21/01/2018

1. Introduction / Protocol [2/20]

Dans une entreprise, chaque employé possède un badge avec une carte à puce - SC - contenant des documents confidentiels et une clé privée d_{SC} identique sur tous les badges, stockée dans la ROM (Read Only Memory). Un lecteur dédié communique avec le badge via le protocole décrit ci-dessous:

In a company, each worker has got a security badge hosting a SmartCard (SC). This badge contains confidential data and a secret key d_{SC} identical for all the cards, stored in the ROM (Random Access Memory) area. A dedicated reader communicates with the badge by the following protocol:

1. La carte et le lecteur partagent une clé secrète par le protocole ECDH. *Badge and reader share a secret key via ECDH protocol.*
2. La carte et le lecteur possèdent le même secret partagé qu'ils utilisent comme clé privée d'un algorithme de chiffrement symétrique pour communiquer entre eux. *The same secret key is shared between the badge and the reader. They use this secret as the key of a symetric algorithm to communicate on a non secure channel.*

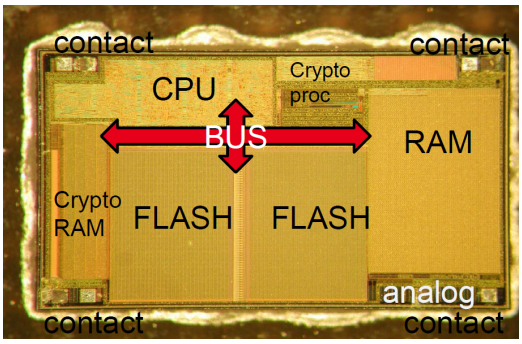
1.1. Dans quelle partie de la puce sont stockées les informations confidentielles ? *On which part of the chip can be stored confidential data ?*

1.2. Citer un algorithme possible pour l'étape 2, présent classiquement dans une carte à puce. *Cite an algorithm usually present onto SCs that could be used for step 2.*

2. Attaque sur ECDH / Attacks on ECDH [9/20]

Un attaquant veut retrouver les informations contenues dans la carte. Il a réussi à voler un badge et est capable d'émuler les commandes du lecteur pour percer les secrets de la carte. Il a ouvert la puce pour voir ce qu'elle contenait et a pris la photo ci-dessous. Le but de cette partie est d'attaquer la puce pendant l'étape 1, pour retrouver la clé privée d_{SC}. Durant cette étape, la puce exécute une multiplication sur une courbe elliptique C à partir d'un point P publics. Cette multiplication par un entier k est définie : $Q = k \times P = P + \ldots + P$ (k fois). La protection est basée sur le fait qu'il est très difficile de retrouver k en connaissant P et Q.

An attacker wants to retrieve secret data stored on the chip. He was able to steal a badge and can emulate reader commands to talk with the SC. He opened the chip and took the picture that follows. The goal of this part is to retrieve the secret private key d_{SC}. During this step the chip performs a scalar multiplication on an elliptic curve C given 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.



L'algorithme ci-dessous permet d'effectuer la multiplication scalaire. Il utilise 2 fonctions **différentes** $ADD\_POINT(Q,P)$ pour additionner les points P et Q et $DOUBLE\_POINT(P)$ qui calcule $2 \times P$.

The algorithm presented below calculates the scalar multiplication. It uses 2 specific and **different** *functions:* $ADD\_POINT(Q,P)$ *to add 2 points* P *and* Q *and* $DOUBLE\_POINT(P)$ *which calculates* $2 \times P$.

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]

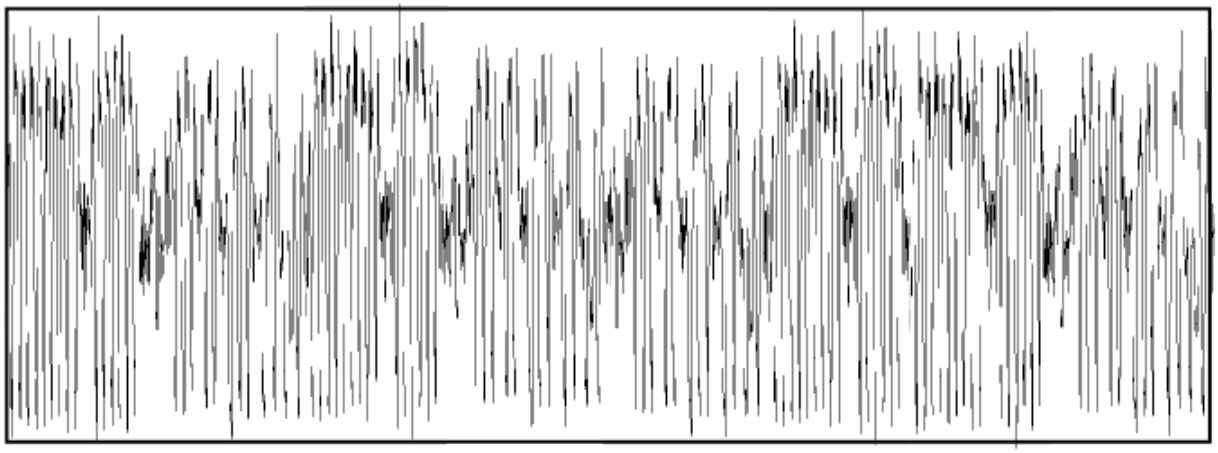
1: $Q \leftarrow 0$, $R \leftarrow 0$
2: **for** $i = 0$ to $n - 1$ **do**
3: **if** $k_i = 1$ **then**
4: $Q \leftarrow ADD\_POINT(Q, P)$
5: $P \leftarrow DOUBLE\_POINT(P)$
6: **end if**
7: **if** $k_i = 0$ **then**
8: $P \leftarrow DOUBLE\_POINT(P)$
9: $R \leftarrow ADD\_POINT(R, P)$
10: **end if**
11: **end for**
12: **return** Q

2.1. Dérouler l'algorithme dans le cas où $k = 11$ pour vérifier que l'algorithme calcule bien $11 \times P$, et donc que l'algorithme effectue bien la multiplication scalaire du point *Describe every step of this algorithm in case* $k = 11$. *Check that it indeed calculates the point scalar multiplication.*

2.2. A quoi sert la variable R ? Trouver une vulnérabilité exploitable en side-channel à cet algorithme. *What is the purpose of* R *variable ? Find a vulnerability that could be exploited in a side-channel attack.*

Une acquisition de la consommation de la puce durant la multiplication scalaire sur les 4 premiers bits de la clé est présentée ci-dessous. *A chip power consumption trace for the first 4 bits of the key is shown below.*

2.3. Retrouver les valeurs possibles des 4 premiers bits de la clé à l'aide de cette figure. *Retrieve the first 4 bits of the secret key, with the help of the power consumption trace.*



2.4. Proposer une correction rapide (<= 2 lignes à modifier) de l'algorithme pour parer cette attaque. *Propose a quick fixin (<= 2 modified lines) to this algorithm to prevent this attack.*

Après cette correction, l'attaquant est dorénavant condamné à effectuer des attaques en perturbation. On prend comme modèle de fautes (i.e. les fautes que l'attaquant est capable de faire avec son équipement), le saut d'une ligne de l'algorithme. *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),*

2.5. Décrire au moins 3 moyens physiques différents pour attaquer un composant en perturbation. *Describe at least 3 differents physical means of injecting faults on a chip.*

2.6. Présenter une attaque en perturbation possible sur l'algorithme corrigé: quelle(s) ligne(s) de code faut-il attaquer ? Pour quel résultat ? Où attaquer sur le composant ? Combien de fautes faudra-t-il réaliser pour retrouver la totalité de la clé ? *Give 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 ?*

2.7. Proposer une contremesure possible pour cette attaque. *Give a proper countermeasure against this attack.*

3. Symetric cryptography [Barème: 9/20]

Un autre chemin d'attaque serait de retrouver la clé partagée pendant le déroulement de l'étape 2 de l'algorithme grâce à une attaque par canaux auxiliaires. *Another path would be to attack the secret shared key during step 2 with a side-channel attack*

3.1. Rappelez le principe général d'une attaque par canaux auxilliaires. *Recall the general principal of a side channel attack.*

3.2. Rappelez le principe de la DPA, et décrire les differentes étapes de l'attaque. *Recall the general principle of a DPA and describe the differents stages for the attack.*

L'algorithme utilisé par le badge est un algorithme propriétaire dont le principe est décrit ci-après. *The symetric algorithm used by the badge is proprietary and described below:*

3.3. Décrivez les avantages et les inconvénients d'utiliser un algorithme propriétaire. *Describe the advantages and drawbacks to use a proprietary algorithm rather than a public one.*

On considère l'algorithme de chiffrement suivant: *We consider the following encrytion algorithm:*

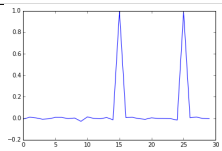
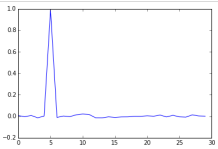
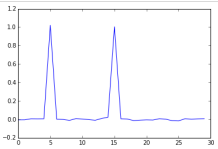
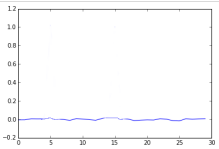
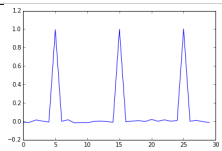
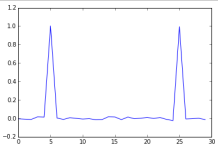
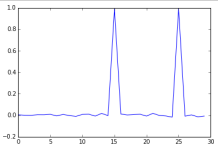
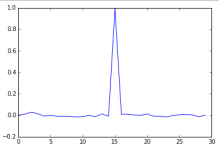
- m: 3 bits, k: 3 bits
- $C(m,k) =$ SBox(m xor (not k))

– SBox[] = [0x3, 0x7, 0x2, 0x0, 0x6, 0x1, 0x5, 0x4]

3.4. Compléter le tableau suivant avec les valeurs manquantes pour C(m,k). *Complete the following table with the missing values for C(m,k).*

k/m	000	001	010	011	100	101	110	111
000	?	101	001	110	000	010	111	?
001	101	100	110	001	010	000	011	111
010	001	110	100	?	111	011	000	010
011	110	001	101	100	011	111	010	000
100	000	010	111	011	100	?	001	110
101	010	000	011	111	101	100	110	001
110	111	?	000	010	001	110	100	101
111	011	111	010	000	110	001	?	100

En utilisant l'ensemble des courbes acquises, les moyennes suivantes ont été calculées: *Using the set of acquired curves, the following means have been computed:*

m	000	001	010	011
Moyennes (Means)				
m	100	101	110	111
Moyennes (Means)				

3.5. Une première DPA a été menée en ciblant le bit le plus significatif (MSB) et aucune fuite n'a été observée. Que faut-il envisager de faire ?*A first DPA vas bien conducted targeting the most significant bit of the result but no leak has been observed. Which are the possible solution to apply ?*

3.6. Appliquer votre solution pour retrouver la clé. *Apply your solution in order to retrieve the key.*

3.7. Si aucune fuite n'est observée lors d'une DPA, quelles sont les solutions possibles à mettre en oeuvre? *If no leak is observed in a DPA, which are the possible solutions to apply?*