==========

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

PARIS

Mémoire présenté en vue d'obtenir

UE **« Information et communication pour ingénieur »**

Spécialité : **INFORMATIQUE**

Par **Avisse, Steve**

(Sujet de l'examen probatoire)

Soutenu le

JURY

PRESIDENT :

MEMBRES :

==========

Table des matières

Table des illustrations :

Introduction

Le nom de carte à puces est couramment utilisé pour désigner des supports de sécurité en matière plastique aux mêmes dimensions qu'une carte de crédit et qui contiennent un circuit électronique intégré capable de mémoriser ou de traiter les informations

La carte à puces, dont la gestation a pu sembler très longue, est à la base de la sécurité des systèmes informatiques. Elle a désormais fait ses preuves dans de nombreux secteurs de l'activité humaine en tant que moyen de paiement, d'identification sur les réseaux fixes (de type Internet), mobiles (GSM ou UMTS) ou multimédia (télévision à péage), d'authentification pour les services gouvernementaux (cartes d'identité, passeports électroniques).

Grâce aux progrès continuels des semi-conducteurs, des technologies de fabrication et de l'évolution des techniques de programmation utilisables, des développements considérables de la carte à puces ont pu avoir lieu et se poursuivent. La carte à puces et ses variantes constituent, pour beaucoup d'applications, une solution particulièrement bien adaptée aux enjeux socio-économiques de notre société.

La sécurité constitue une composante cruciale des technologies de l'information et de la communication et représente un des leviers de leur essor car elle est à la base de l'instauration de la confiance nécessaire pour les utilisateurs finaux.

Ceci explique certainement pourquoi le marché de la carte à puce, laquelle implémente des fonctions cryptographiques assurant la confidentialité, l'authentification et l'intégrité des données, continue à afficher une dynamique à deux chiffres depuis sa création, il y a plus de 20 ans.

Parmi les manipulations frauduleuses qui peuvent être mises en œuvre sur les composants de sécurité, trois types d'attaques font l'objet d'une attention particulière depuis la fin des années 1990, à la fois de la part du marché mais également du monde universitaire. Elles sont qualifiées de « physique » car elles nécessitent pour l'attaquant d'avoir le composant « entre les mains » ce qui est généralement le cas pour les cartes à puce. Certaines de ces attaques sont dites invasives (ou « intrusives ») au sens où elles endommagent (parfois irrémédiablement) le composant

D'autres méthodes, qui sont également très efficaces mais qui ne mettent pas à mal l'intégrité du composant (on parle d'attaques « non intrusives »), sont basées soit sur l'analyse du comportement du circuit en présence de perturbations (on parle dans ce cas d'attaques « en faute ») ou sur l'observation des modifications de l'environnement créées par le circuit lorsqu'il réalise des calculs cryptographiques (on parle alors d'attaques par « effet de bord », par « canaux cachés » ou en « side-channel »). A noter que toutes ces attaques, bien que distinctes dans leur principe, sont généralement combinées en pratique.

Contre ces manipulations frauduleuses, les concepteurs de composants sécurisés ont proposé de nombreux dispositifs (ou contre-mesures) qui, soit donnent une information sur l'état du circuit soit agissent pour protéger les données. Dans le premier cas, on parlera de « capteurs » et dans le second d' « actionneurs »

Comme la course poursuite engagée entre les concepteurs de circuits de sécurité et les attaquants s'accélère avec la diversité des systèmes, leur ouverture et leur multiplicité, il apparaît aujourd'hui comme un enjeu majeur de devoir améliorer drastiquement la résistance de ces composants à toutes ces attaques. Ces composants sont conçus grâce aux techniques et méthodes développées depuis plus d'un demi-siècle pour les circuits intégrés non sécurisés

L'objet de ce mémoire est d'apporter une vue d'ensemble sur la problématique suivante « comment sécurise-t-on une carte à puce de par son architecture et son fonctionnement et quelles sont les attaques possibles et leurs contre mesure ? »

Pour y répondre nous allons procéder en trois parties. Dans un premier temps nous évoquerons l'architecture de la carte à puce ainsi que de son fonctionnement. Dans un second temps nous expliquerons l'importance de la fiabilité et la sécurité physique ce produit. Enfin pour finir nous parlons des attaques qu'elle peut encourir d'un point de vue physique et comment y remédier.

1.L’histoire de la carte à puce

En 1950, la société américaine Diners ’Club a émis la première carte de voyage et de loisirs.

Elle se présente sous la forme d'un petit carnet (carton), qui contient une liste d'adresses (du restaurant de l'hôtel qui accepte cette carte), la signature de son titulaire et diverses informations.

Elle est la première société de cartes de crédit au monde et a fondé le concept de sociétés indépendantes pour produire des cartes de crédit de voyage et de loisirs.

En 1958, la carte American Express (carte plastique) qui a été émise par l'héritier de la célèbre compagnie de diligences Wells & Fargo, à 5 dollars par mois. À l'époque, c'était la première entreprise à industrialiser toutes les cartes plastifiées

En 1967, tout commence en France avec le groupe carte Bleue qui apparaît en réunissant six banques la BNP, le CCF, le Crédit du Nord, le CIC, le Crédit lyonnais et la Société générale, afin de fournir un mode de paiement compétitif pour les cartes américaines.

L'objectif est de réduire le nombre de chèques en circulation qui représentent déjà 40% des transactions de paiement et atteindront 90%

En 1980, ils ont fourni une carte bleue française qui pouvait être utilisée sur les terminaux de paiement électronique.

En 1971, les premiers distributeurs automatiques de billets (DAB) voient le jour et utilisent des cartes bleues avec une bande magnétique (la bande magnétique se compose de deux zones de lecture d'une capacité de 200 octets).

En 1974, Roland Moreno a déposé un premier brevet pour des articles portables à mémoire. Il décrit un composant (l'ancêtre d'une carte mémoire), qui consiste en une mémoire électronique (E2 PROM) fixée sur un support (comme un anneau) et un lecteur (via un couplage électromagnétique) pour l'alimentation et l'échange de données (par liaison optique), Il a développé une carte à puce à circuit intégré. Il a démontré son système à plusieurs banques convaincues. Il fonde donc alors la société **Innovatron.**

En 1977 Michel Ugon (Bull) enrichit l’idée de **Roland Moreno** et la concrétise : la carte doit être intelligente : c'est-à-dire fonctionner comme un micro-ordinateur. Il dépose ensuite un premier brevet qui décrit un système à deux puces, un microprocesseur et une mémoire programmable.

Décidé, il approfondit son idée et dépose cette fois le **brevet SPOM** (Self Programmable One Chip Micro-Computer) qui va permettre de détermine l'architecture nécessaire au fonctionnement auto-programmable de la puce.

Cette démarche de l'auto-programmation permet à un microprocesseur lorsqu'il y a une alerte de modifier son comportement pour contrer cette alerte. Au pire, le microprocesseur peut engendrer son autodestruction.

En 1979, La compagnie **BULL CP8** (Cartes des Années 80) est créée et a première carte à deux composants vois le jours, elle est surnommée aussi (carte intelligente) est assemblée.Il est équipé d'une mémoire et d'un microprocesseur (Motorola)T

En 1979, Schlumberger entre au capital d'Innovatron puis entame ses recherches sur **la carte mémoire :** la "Cartes à Mémoires & Systèmes" est créée au sein de la société Schlumberger.

En 1980, Le Gie (l'écosystème de la monétique, interbancarité et interopérabilité) carte à mémoire est créé, il comprend des industriels (CP8, Schlumberger, Philips), le secrétariat d'Etat des P&T, et plusieurs banques.

En 1981, Le Microprocesseur Auto-programmable Monolithique (MAM, en anglais Self Programmable One chip Microprocessor – SPOM) est né, c'est alors le composant qui équipera toutes les cartes à puce.

Marc Lassus (futur fondateur de Gemplus) supervise la production des premières puces (microprocesseur et mémoire puis MAM) insérées par CP8 (un nouveau procédé de fabrication est développé pour obtenir des épaisseurs inférieures à un mm).

En 1982, plusieurs prototypes de publiphones utilisant des cartes mémoire (cartes téléphoniques) ont été commandés par la DGT (Délégation Générale des Télécommunications) à plusieurs industriels à ce jour personne pouvait imaginer que les télécartes constitueraient plus tard un marché très important pour les cartes à puce.

En 1983, une idée est apparue que la carte à puce pouvait aider le secteur sanitaire et social, dans ce qui touche à la santé : l'objectif est de fournir aux patients une carte de santé qui fournirait au médecin des informations plus précises sur le patient.

La même année, la Direction générale des Télécommunications (futur France Télécom) présente la "carte télécommunications" : une carte d'abonnement qui vise à collecter chaque communication sur la facture téléphonique de l'abonné.

En 1982, apparition des premières puces sécurisées (logique câblée) et 1983 (microcontrôleur).

En 1984, la technologie CP8 (MAM) a été adoptée par les banques françaises, le système d'exploitation B0 est devenu la norme pour les cartes bancaires françaises.

En 1988, Le groupement des cartes bancaires (CB) passe une première commande de 12,4 millions de cartes et introduction des normes de base des cartes à puce (ISO 7816)

En 1988, Marc Lassus crée **Gemplus** en France. Cette société était jusqu'à sa fusion avec Axalto (ex-Schlumberger) en juin 2006, numéro 1 mondial de la carte à puce, ayant mis en circulation de 1980 à 2006 plus de 6,8 milliards de cartes

En 1987, la norme des réseaux mobiles de 2°génération (GSM) intègre la notion de module de sécurité (une carte à puce SIM –Subscriber Identity Module). Les télécommunications deviennent le premier marché de la carte à puce.

En 1996, l'apparition des cartes java marque l'entrée des systèmes cartes à puce dans le monde des systèmes ouverts. Il devient possible de développer des applications dans un langage largement diffusé.

En 2002, la technologie de communication near field communication NFC a eté lancée par Sony et Philips. C'est une technologie de communication sans-fil à courte portée et haute fréquence, permettant l'échange de données entre un lecteur et un terminal mobile ou entre les terminaux eux-mêmes

2.Généralités sur les cartes

A partir des **années 1980**, la carte à puce a **révolutionné** notre quotidien, qu'il s'agisse de cartes bancaires, dans le passé de Télécartes, des cartes SIM de nos téléphones portables, etc.

Elle a donné naissance à une importante activité économique qui affecte la fabrication de composants électroniques, le développement de logiciels et de distribution, les machines-outils, les périphériques, le développement d'applications, les tests de conformité, les tests de sécurité, etc.

Mais surtout, cette innovation a créé de toute pièce un objet sécurisé dans le domaine des technologies de l'information dont la sécurité intrinsèque est hors de proportion avec tout ce que vous pouvez faire. De nombreux experts en sécurité ne connaissent pas les spécificités de ces objets qu'ils assimilent à un système informatique comme les autres.

3.La carte à puce

La **définition ISO** nous pouvons donc dire qu'une carte à puce est :

« Une carte plastique de la taille d'une carte de crédit comportant un circuit électronique et conforme à la norme ISO 7816. »

Selon un ensemble de normes établies par l'organisme international de normalisation (ISO), portant le nom de **ISO 7816** une carte porte un circuit intégré capable de mémoriser de façon sécurisée une série d'informations. Ce circuit intégré s'appelle une puce c'est donc un composant électronique Qui permet d'effectuer des opérations (stocker, calculer, etc.), de façon sécurisée.

Mais attention tout de même car sa puissance de calcul et sa capacité de stockage d'informations sont restreintes et peuvent être différentes d'une carte à l'autre.

« This application will put a sophisticated information-security device in the wallet or purse of practically every person in the industrialized world, and will therefore be the most extensive application ever made of cryptographic schemes. »

Gustavus Simmons (1992)

A noter tout de même que les cartes à logique câblée sont des cartes dit « **actives** » parce qu'elles procèdent à des opérations logiques et les cartes à puce intelligentes sont nommer ainsi parce qu'elles peuvent traiter l'information.

Il faut retenir que le terme carte à puce est un générique. Sous cette appellation sont regroupées la **carte à mémoire simple**, la **carte à logique câblée** et la **carte à puce intelligente.**

La plupart des cartes en plastique dont nous disposons aujourd'hui comportent des bandes magnétiques qui ne sont pas sécurisées.

Il est aisé d'accéder aux données qui y sont stockées et de les modifier, d'où un risque pour les informations confidentielles. Les cartes magnétiques offrent également peu de protection lors d'une transaction avec des ordinateurs hôtes distants car de fausses cartes sont faciles à reproduire, par exemple pour une vérification du PIN.
Une carte à puce est une carte format de poche incorporant des circuits intégrés (IC) qui lui permettent de **traiter** et de **stocker des données** en conformité avec la **norme ISO 7816.**
Cette technologie est une alliance entre la technologie des **puces à semi-conducteur**, le **matériel** et le **logiciel**, permettant à la carte de fonctionner tel **un micro-ordinateur**. Elément non négligeable, elle est personnalisée et de plus en plus contrôlée par l'utilisateur, ce qui en renforce la sécurité.

4.Composantes essentielles d'une carte à puce

Une carte à microprocesseur est constituée d'un **micromodule** (appelé aussi puce) inséré dans rectangle de plastique au format « carte de visite » sur lequel sont en général inscrites des informations liées à l'identité du possesseur de la carte. Par ailleurs, la carte peut aussi comporter une **piste magnétique** (c'est le cas notamment des cartes bancaires actuelles).

Conformément au standard **ISO/IEC 7816-1 [52]**, les dimensions de la carte à microprocesseur doivent vérifier :

- 85.47 mm ≤ Largeur ≤ 85.72 mm ;
- 53.92 mm ≤ Hauteur ≤ 54.03 mm ;
- Epaisseur = 0 ´ .76 ± 0.08 mm
-

La carte à puce est composée de plusieurs éléments :

- Une carte plastique
- Une puce électronique
- Une mémoire

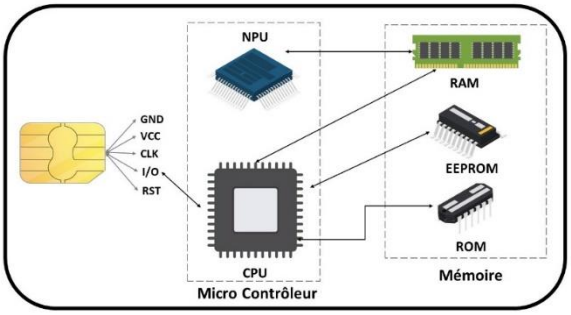

Figure 1 Composition Carte à puce

4.1 La carte plastique

Aux bords arrondis est au format d'une carte de crédit traditionnelle. Cette carte possède en incrustation un circuit électronique miniaturisé. Ce circuit intégré est réalisé en silicium pour les technologies actuelles. Il se trouve logé sous les contacts d'un (micro)module qui est parfaitement visible.

Deux principaux types de plastique sont utilisés :

• le PVC non recyclable mais embossable,
• l'ABS recyclable mais non embossable.

La figure x montre un schéma simplifié de la carte en faisant apparaitre les différents composants entrant en jeu

4.2 Le microprocesseur :

Plus souvent en 8 bits et fonctionnant à une vitesse de 4 MHz, il comprend deux unités :

- Le **CPU** (central processing unit, unité centrale de traitement) est le cœur de la puce.
  Ce sont les circuits logiques du CPU qui permettent la sécurisation des données contenues dans la mémoire de la puce.

- Le **NPU** (network processing unit, unité de traitement du réseau) est une unité spécifiquement dédiée à la gestion des flux de données.
  Son rôle est d'optimiser ces échanges (notamment leur vitesse).

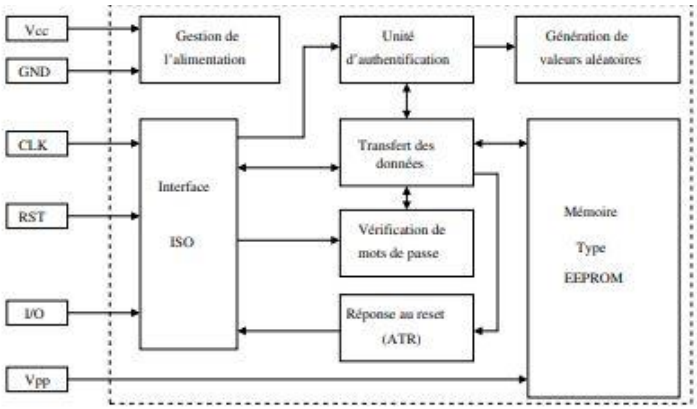

Figure2 Architecture de la première version d'une carte mémoire

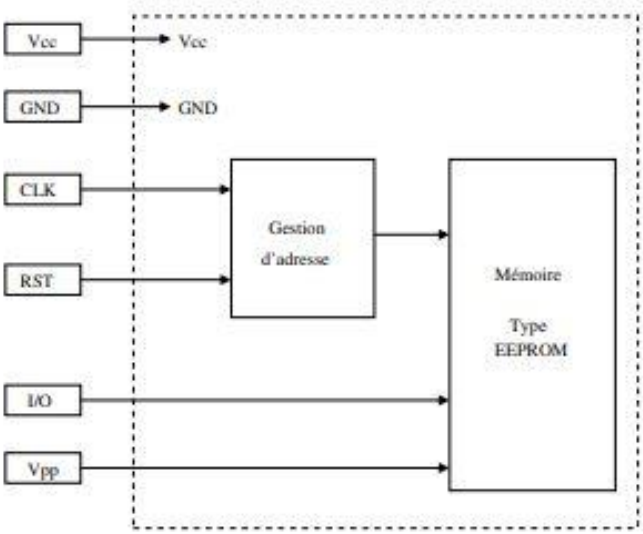

Figure 3 Exemple de carte à mémoire à sécurité câblée

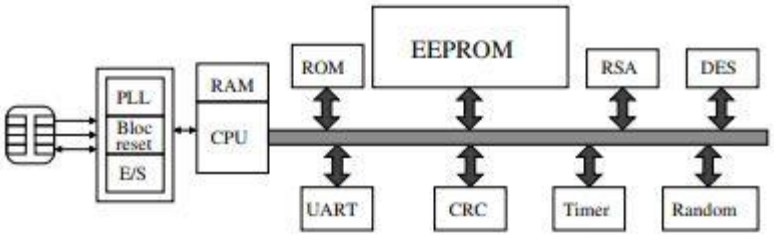

Figure 4 Architecture de la carte à puce à microprocesseur

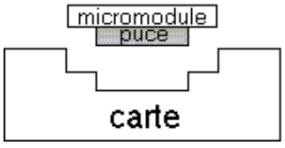

Figure 5 vue d'un micromodule

4.4 Le micromodule :

Le micromodule est le très mince circuit imprimé logé dans l'épaisseur de la carte Qui accueille les contacts (visibles) du connecteur sur une face et La puce (non visible) sur l'autre.

Pour le micromodule, l'affectation des contacts (1 à C) varie selon le type de puces :

- 1 : tension d'alimentation de la carte (Vcc = 5v),
- 2 : signal de remise à zéro (Raz ou A ou Reset),
- 3 : signal d'horloge H (Clock ou Clk),
- 4 : non utilisé ou code fonction (télécarte),
- 5 : masse électrique (Vss = 0v),
- 6 : tension de programmation Vpp (écriture),
- 7 : entrées-sorties (In/Out) série des données,
- 8 : non utilisé ou contrôle fusible (télécarte)

Figure 6 micromodule à la norme ISO

Figure 7 micromodule à la norme AFNOR

La norme ISO internationale a été précédée au niveau français par la norme AFNOR.
L'interface correspond à la fois à une prise électrique (alimentation en énergie) et à une prise d'échange de données. L'interface gère également quelques fonctions de maintenance.

4.5 L'interface

Correspond à la fois à une prise électrique (alimentation en énergie) et à une prise d'échange de données, affectation (1,2,3 des contacts du micromodule). L'interface gère également quelques fonctions de maintenance.

4.6 Le système de fichier

Responsable de l'organisation des informations dans la mémoire eeprom, le système de fichiers est construit autour de dossiers contenant des informations de la même applications et fichiers, conteneurs unitaires pour ces informations ;

4.7 mécanismes de journalisation

Mécanismes d'enregistrement responsables de l'intégrité des processus d'enregistrement eeprom utilisant l'enregistrement paresseux dans la zone tampon.

4.8 mécanismes d'erreurs

Responsable du traitement des erreurs logicielles ou matérielles qui peuvent apparaître dans un contexte fonctionnel normal et mettre à la disposition du terminal informations de base et peut-être la source de l'erreur.

5.Famille de carte à puce et types de cartes

Toutes les cartes (à contact et sans contact) possèdent des caractéristiques communes :

- Dimension permettant de les reconnaitre facilement
- Mémoire qui permet de stocker des données
- Une intégration de la mémoire et potentiellement un processeur
- Un numéro de série unique et permanent, inscrit dans la mémoire permanent

On peut distinguer différentes familles de cartes à puce dû à la présence ou non d'un microprocesseur et le type d'interface, avec ou sans contact :

5.1 Carte à mémoire

Historiquement les plus anciennes, les cartes à mémoire possèdent un circuit intégré qui ne contient qu'une zone mémoire avec le minimum de logique nécessaire pour la mettre en œuvre intégrant éventuellement un mécanisme de protection. Elles permettent le stockage des informations en quantité plus importante.

Les cartes à mémoire se répartissent en deux sous-catégories :

5.1.1 Cartes à mémoire simples (memory only cards) :

Ces cartes sont employées comme systèmes permettant d'intégrer des unités stockées
Servent de simple support de stockage et sans réel mécanisme de protection, le niveau de sécurité de ces cartes est très faible ;

5.1.2 Les cartes à mémoire avec logique câblée : memory card with logic

Ce type de carte comporte un dispositif câblé de protection des données ce qui lui permet d'avoir un niveau de sécurité.

Elles possèdent aussi un support de stockage permettent d'effectuer des opérations de logique simple, un premier mécanisme de protection est introduit par la limitation de l'accès de certaines zones mémoire à leur seule lecture ou à lors de la phase de personnalisation, et par la mise en œuvre d'automates simples.

Les cartes à microprocesseur sont des cartes possédant une mémoire programmable ainsi que plusieurs fonctionnalités permettant des opérations logiques avancées.

5.2 Carte à microprocesseur

Les cartes à microprocesseur (ou microcontrôleur) **intègrent de l'intelligence**, en effet L'accès à la mémoire contenant les données est sécurisé par la présence d'un circuit. Elles incorporent ainsi une capacité de traitement de l'information administrer par un véritable microprocesseur.

Ce un microprocesseur 8 bits doté de capacités de traitement de données et de calculs complexes (**cryptographie**) la carte est donc programmée par un logiciel qui intègre dans la mémoire un programme (**qui contient le système d'exploitation et les applications**)

Le cœur du système est constitué par **une mémoire EEPROM** permettant de gérer des données stockées à l'aide de protocoles sophistiqués rendus possibles par la présence du microprocesseur.

Selon l'approche utilisée pour leur programmation, on peut distinguer trois sous-catégories des cartes à microprocesseur :

- **Cartes spécifiques :** le programme de la carte est inscrit dans le masque du composant, avec un OS (operating system) propriétaire
- **Cartes personnalisables :** la Configuration de la carte en fonction de l'application est admise par un OS supportant une action d'instructions spécifique
- **Cartes à OS ouvert :** une carte à puces à os ouvert est en quelque sorte une carte « programmable « c'est-à-dire une carte dans laquelle il est possible, en plus d'exécuter du code natif suivent le même principe que celui des systèmes fermés
    - Soit de télécharger du code natif après délivrance de la carte.
    - Soit de programmer un interpréteur de commande particulier et donc en jeu d'instruction et de mécanisme de gestion de fichiers et / ou programmes additionnels.

5.3 Type de carte

Nous pouvons donc distinguer **deux grandes familles** de carte :

5.3.1Cartes avec contacts

Il était nécessaire de fournir plus d'énergie et donner la possibilité de communiquer avec l'extérieur donc la carte contact nécessite un **contact physique direct** avec le lecteur au niveau du micromodule pour que l'alimentation et les commandes soient adresser.

Normalisation internationale, A défini une position à donner aux contacts de la carte et la signification de chacun d'eux. *(Voir figure 01 et 02)*

5.3.2 Cartes sans contacts

Cette carte contient des circuits spécialisés qui est utilisés également dans le domaine des transpondeurs qui leur permettent de travailler sans contact mécanique ainsi que sans application directe qui demande une alimentation.

Elles font partie de la famille de produits **appelés RFID (Radio Frequency Identification Device)** qui est plus vaste. Le principe consiste à assurer l'alimentation de la carte et l'échange de données avec le lecteur par l'intermédiaire d'un champ électromagnétique plutôt que par des connexions électriques physiques avec une antenne bobinée dans la carte reçoit l'énergie **radio-fréquence transmise par un lecteur de carte via la porteuse.**

On parle aussi de cartes NFC (pour Near Field Contactless). Cet acronyme signifie que la carte est alimentée et communique en champ proche (quelques centimètres) avec un lecteur.

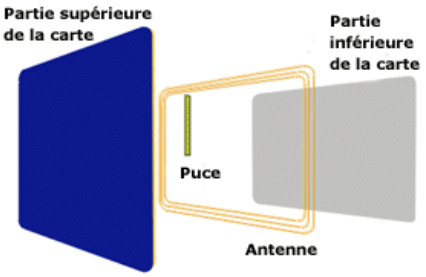

Figure 6 cartes NFC

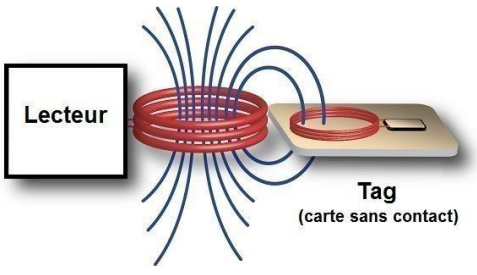

Figure 7 Principes physique du NFC

5.3.2.1 L'architecture de la carte sans contact :

Une carte à puce sans contact contient :

• une partie classique mémoires et une unité centrale de traitement (microprocesseur)
• une interface radiofréquence qui va lui permettre la récupération des données dans la porteuse et différents dispositifs

6.Systéme d’exploitation :

Le terme « système d’exploitation » cache certaines contradictions en termes de postes de travail et de cartes à puce. L'utilisateur voit le système d'exploitation comme un ensemble de logiciels pour pouvoir faire fonctionner le matériel. **Richard Stallman** définit le système d'exploitation comme un **ensemble de logiciels**, tels que les logiciels requis pour utiliser la machine.

Il comprend le programme qui est exécuté au démarrage de l'ordinateur, mais aussi l'ensemble des programmes de base qui permettent l'utilisation. Avec cette définition, le système d'exploitation est une boîte à outils logicielle qui comprend divers programmes, tels que des interpréteurs de commandes, des outils de traitement de fichiers et même des compilateurs de programmes. Lorsqu'on parle de logiciel embarqué dans une carte à puce, les gens utilise souvent une définition très large de ce type.

Par conséquent, le "système de carte" se réfère généralement à tous les logiciels de la ROM de carte, qui existent immédiatement lors de l'acquisition et sont donc immédiatement disponibles, donc ils sont considérés comme des "logiciels de base".

Situé dans la partie mémoire persistante du microcalculateur (ROM, EEPROM ou FLASH), il est implanté pour la ROM dans l’un des masques qui sert à la fabrication du circuit intégré. Ainsi, par abus de langage, les notions d’OS et de masque sont couramment confondues.
Le système d'exploitation COS (Chip or Card Operating System) ou aussi dénommer masque est doté de fonctions permettant les opérations suivantes :

- gestion des Entrées / Sorties,
- organisation de la réponse au Reset,
- organisation de la mémoire en zones de travail avec gestion des codes confidentiels,
- gestion des autorisations d’accès (codes confidentiels) en lecture et en écriture au niveau de chaque zone,
- chargements éventuels de sous-programmes spécifiques lors de la personnalisation ou pendant la durée d’utilisation de la carte.

Le système d'exploitation de la carte micro-ordinateur est similaire au système utilisé dans les micro-ordinateurs. C'est l'une des parties les plus importantes des cartes micro-ordinateur car c'est ce qui leur donne toutes les fonctions, notamment dans la supervision des fonctions de sécurité.

Un bon système d'exploitation est très complexe à produire et sa mise en œuvre doit tenir compte du faible coût, de la sécurité, de l'architecture de la machine, des performances, de la compacité, de la normalisation et de la fiabilité

7.Fonctionement de la carte à puce :

Fonctions fournies par le système de cartes en interaction avec un lecteur qui peuvent être connectés à un serveur, sont axés sur la sécurité, celle- comprennent :

Des fonctions techniques :

- Traiter, échanger des données et les stocker
- De faire face aux attaques malveillantes et ainsi leurs résister
- S’Interfacer avec le lecteur (physique, électrique, magnétique, interface logicielle) et ainsi de pouvoir alimenter la puce de la carte afin de pouvoir interagir avec le lecteur en dialoguant
- Résister à l’environnement et à l’utilisation (contraintes mécaniques, frottement, champ électrique, décharge électrostatique, champ magnétique…)

Des fonctions de service :

- Identifier la carte et éventuellement son titulaire
- Authentifier : le lecteur par la carte, la carte par le lecteur, le porteur par le système
- Portable
- Stocker, modifier et restaurer des données
- Signer les données pour un examen ultérieur

7.1 Communication de la carte

Dans sa phase d'utilisation, la carte à microprocesseur subit un cycle triphasé :

- Insérez la carte,
- Exécution des ordres,
- Déconnectez.

Ces trois étapes constituent la connexion.
Après avoir inséré la carte, elle sera alimentée et réinitialisée à nouveau
Deuxième étape cela comprend la réception et l'exécution des ordres sur les ports d'entrée / sortie.
Cette étape peut être répétée plusieurs fois pour terminer avec succès la demande
La troisième étape correspond à couper franchement l'alimentation de la carte.
Les deux premières étapes de la connexion permettent d'intervenir sur le contenu de la carte.

7.2 La connexion

La connexion de la carte dans le terminal représente toutes les activités effectuées entre le moment où la carte est inséré dans le terminal et après son retrait.
Une fois la carte est connectée au terminal, celle-ci va effectuer une série d'actions pour tester son état, puis émet une série d'octets appelée « Réponse à la remise à zéro » (aussi appelée **ATR** pour Answer To Reset). Cette réponse est normalisée.
L'ATR est composée de plusieurs champs :

- Les **conventions de codage** des octets de données
- **Protocole de communication** utilisé par la carte et la taille de l'ATR.

La fin de la connexion Carte / Terminal est marquée par le retrait de la carte du lecteur (appelé arrachement).
Le porteur est informé par l'interface du lecteur que la connexion est terminée et qu'il peut enfin retirer sa carte. Il arrive aussi que la carte soit complètement "avalée" par le lecteur et restituée par lui à la fin de la connexion. Dans les deux cas l'utilisateur doit pouvoir retirer sa carte

Une fois que la puce a envoyé son ATR, elle ne parle plus tant qu'elle n'y est pas invitée par le lecteur. C'est donc le lecteur qui a la main sur la patte input/output. Quand le lecteur veut interagir avec la puce, il lui envoie un **APDU (Application Protocol Data Unit)**, c'est à dire une séquence de généralement 5 octets.

- **Le premier** octet est la classe (CLA) de la commande.
- **Le deuxième** octet est l'instruction dans la classe (INS),
- **Les 3ème et 4ème** octet sont les paramètres P1 et P2 de l'instruction,
- **Le 5ème octet** est généralement la taille de la réponse attendue.

8. Le dialogue employer

La communication entre la carte et le terminal s'effectue selon des **protocoles de communication standardisés**. Le protocole se fait dans l'**ATR** et est donc déterminé par la carte
Les protocoles ne varient que très peut sur leurs utilités et leur fonctionnement, un **Protocol permet : De définir les commandes pouvant être envoyées à la carte (commandes entrantes), ainsi que les commandes demandant des données à la carte (commandes sortantes).**

Toute communication entre la carte et le lecteur se termine par l'envoi de deux mots d'état pour indiquer que la **commande est terminée** (commande entrante) ou pour dire que toutes les **données ont été envoyées** (commande sortante). Il faut savoir que la demande **vient toujours du lecteur** : en conséquence la carte ne peut pas émettre la demande, elle peut que simplement y répondre elle est donc considérée comme : **Passif**

Le **format de commande** est **standardisé et normalisé** ; les commandes sont appelées **commandes APDU.** Une **commande APDU** est une **requête envoyée par le terminal** vers **une applet chargée dans une carte à puce**. La figure xxx représente les différents champs qui la composent :

CLA	INS	P1	P2	LC	Donnée optionnelle	LE

Figure 8 commande APDU

La **réponse APDU** contient des **informations sur le résultat de la commande** et éventuellement des données si nécessaires. Elle est composée d'un champ de donnée et d'un mot d'état (figure : 1.3).

Donnée optionnelle	SW1	SW2

Figure 9 Réponse APDU

7.3 commandes entrantes et commandes

Le fonctionnement des **commandes entrantes** et **commandes sortantes** est le suivant :

- **Commandes entrantes :** la carte commence valide la réception de l'ordre reçu, par accuser réception de l'ordre reçu, puis attend les données.
  Après réception des données, la carte commencera à traiter la commande.
  A la fin, la carte envoie deux mots d'état au terminal (marqués SW1 et SW2 pour le mot d'état)

- **Commandes sortantes :** la carte confirme la réception de la commande reçue, puis commence immédiatement la mise en œuvre de la méthode appropriée (la mise en œuvre commence immédiatement après la fin de la procédure d'entrée et de sortie de communication). A l'issue de cette implémentation, la carte envoie le résultat de son travail au terminal.

Nous assistons donc à des protocoles relativement limités et montrent que la carte à microprocesseur a été conçue comme un **serveur de données.**

A titre d'exemple, si l'on se réfère à un réseau développé, les protocoles **de communication Carte / Terminal** sont au même niveau que le **protocole TCP / IP** pour les communications sur le réseau Internet

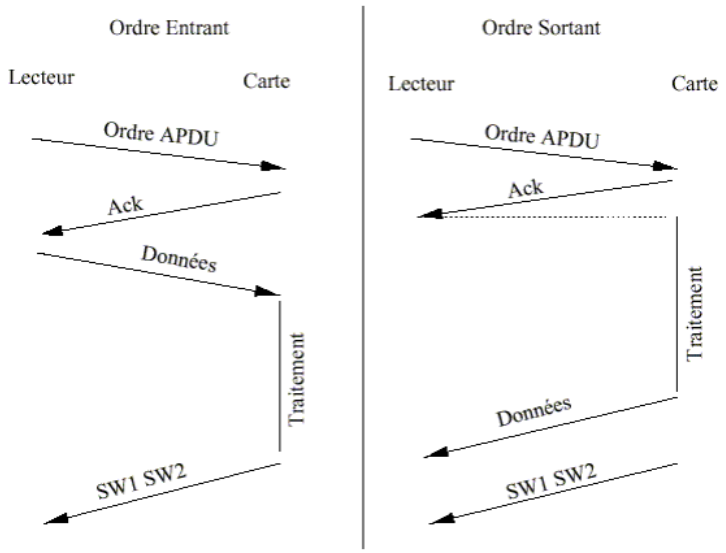

Figure 10 échange d'ordres APDU

Requête.	Réponse.
CLA INS P1 P2 Lc [Lc octets]	sw1 sw2
CLA INS P1 P2 Le	[Le octets] sw1 sw2
CLA INS P1 P2 Lc [Lc octets] CLA C0 00 00 Le	61 Le [Le octets] sw1 sw2

Figure 11 Commandes (APDUs) définis par la norme ISO 7816

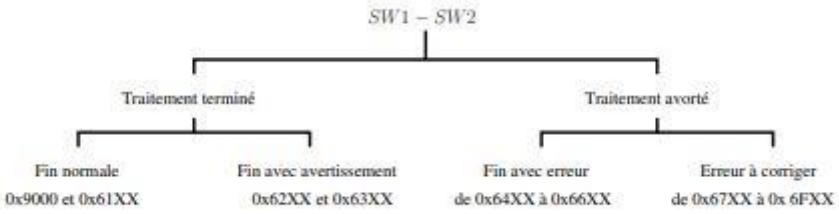

Figure 12 valeurs SW1 et SW2 du Status Word

8. La partie mémoire de la carte à puce :

Selon la définition d'A. Tanenbaum le système est intimement lié au matériel dont il permet l'exploitation.

Ce matériel informatique peut servir trois intentions différentes :

- **Traiter l'information, stocker ou communiquer à l'environnement.**

Il existe différentes technologies de stockage de l'information sont utilisées au sein des cartes :

- **La mémoire vive**. Le stockage temporaire de l'information en cours de traitement est assuré par une faible quantité de mémoire RAM dit statique cette mémoire est utilisé pour stocker les informations temporaires et la pile d'exécution nécessaire au déroulement du programme.
  Sa gestion consiste essentiellement en son initialisation et à son allocation / libération, au besoin. Dans bien des cas, l'allocation est faite statiquement, lors de la conception du système d'application, mais dans les systèmes plus sophistiqués elle est faite dynamiquement, au besoin, lors de l'exécution des applications.
  Dans ce cas, la gestion de la RAM est assurée par le système encarté ; la mémoire morte.
  Parmi les autres mémoires encartées,

- **La ROM** contient le masque du système. Son contenu est fixé à la production du silicium et le matériel ne demande par la suite aucune gestion particulière de la partie du système d'exploitation ;

  - **les mémoires persistantes.** Les cartes à puce peuvent utiliser deux formes distinctes de mémoire persistantes :
    - **L'EEPROM** et plus généralement les mémoires persistantes dites **NOR,** sont des mémoires adressables. A ce titre, le programme exécuté par le microprocesseur peut directement lire le contenu, comme s'il était stocké en RAM ou en ROM.
      Ces mémoires dont le contenu n'est pas perdu lorsque la carte n'est plus alimentée ne peuvent cependant être écrites qu'en programmant un circuit dédié.
      Cette programmation implique deux opérations distinctes de plus, l'écriture sur ce type de support n'est pas fiable, et ce manque de fiabilité augmente avec le nombre d'écritures sur une même cellule (à la même adresse mémoire).

    - **Les mémoires Flash**, mémoires dites NAND, sont des mémoires non adressables. Les programmes exécutés par les microprocesseurs ne peuvent donc pas accéder directement à ces mémoires, en lisant une adresse particulière du bus. A l'instar d'un disque sur nos stations de travail, un circuit particulier des mémoires NAND doit être programmé pour qu'un fragment (appelé page) du contenu stocké sur ce support soit rendu lisible. Il en va de même pour les écritures qui, par ailleurs, se décomposent en deux étapes, à l'instar des mémoires NOR.

9. Cycle de vie d'une carte

L'Industrie de la carte à puce implique différents acteurs :

- **Le développement de l'applicatif**
- **Les fabricants de composants électroniques,**
- **Les concepteurs des « masques programme »,**
- **Les encarteurs/imprimeurs,**
- **Les personnalisateurs.**

Comme on le verra, certaines de ces fonctions sont souvent regroupées au sein d'une même société

La figure (le xxxx) décrit les **différentes phases de vie d'une carte à puce** et permet de mieux comprendre l'intervention des différents acteurs décrits ci-après

La première phase consiste au **développement de l'applicatif** de la carte à puce et à la **spécification des informations** nécessaires à la pré-personnalisation.

La puce est **conçue lors de cette Seconde phase,** ainsi que Le système d'exploitation est fabriqué par une entreprise spécialisée. Ce logiciel, adapté à un composant électronique spécifique, est **appelé masque.**

Le concepteur de masque le plus connu dans le domaine des **CAM « haute sécurité »** a longtemps été le créateur du concept lui-même à savoir **Bull CP8** créée en 1985 avec son **MAM** (Micro calculateur Auto-programmable Monolithique).

Le masque est stocké dans la ROM du composant pendant le processus de production. A l'issue de cette phase, le fabricant de silicium stocke dans la puce :

- La clé **dite clé de production** et stocke ces **dernières informations**, telles que le numéro de série du produit, la date de fabrication, etc.

Fabrication des tranches de silicium (« wafers ») comportant une puce dans lesquelles est gravé le logiciel développé. Ce process industriel, qui nécessite des moyens considérables, est assuré par des fondeurs de la microélectronique comme STMicroelectronics, Atmel, Infineon ou encore NXP.

Fabrication des modules : chaque tranche de silicium est découpée pour obtenir des composants qui sont **collés** sur des **contacts électriques,** puis **reliés électriquement** par **pontage** (« wire bonding ») et enfin **encapsulés** dans une résine qu'on polymérise puis usine.

Les encarteurs partent d'un composant déjà masqué (programmé), l'ensemble est ensuite protégé par une **substance isolante** puis collé sur un support en plastique (PVC), dans lequel la cavité (bouton) a été préalablement usinée.

Toutes les grandes sociétés d'introduction ont développé leurs machines jusqu'à ce que le marché soit suffisamment développé pour que l'offre industrielle soit enfin disponible.

L'encarteur, qui connaît les clés de production va lors **:**

- **Écrit de nouvelles informations dans le système** et **active le verrou de production,** qui **annule la clé de production**.

La nouvelle clé est alors enregistrée dans le système, ce qui permet de contrôler. Cette opération est également appelée **personnalisation** qui va consister à s'adapter au porteur final de la carte.

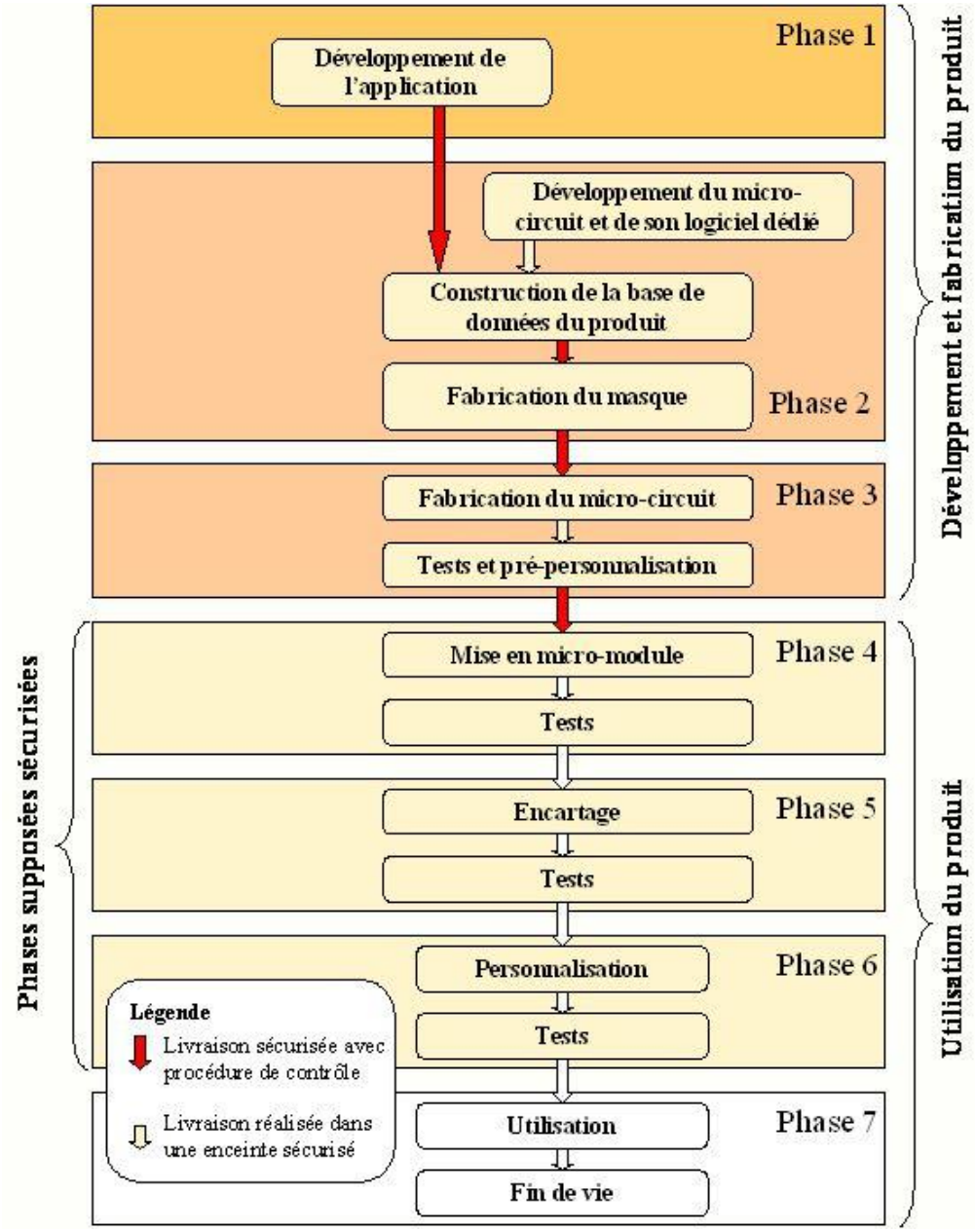

Figure 13 différentes phases de vie d'une carte à puce

La personnalisation peut être envisagée **sous deux aspects** :

- **Électronique :** Personnalisation électrique (par opposition à la personnalisation graphique) consiste à saisir les informations nécessaires dans l'application. Ces informations peuvent être l'identité du client, le code de l'opérateur, les clés secrètes, le numéro d'abonné, le numéro de compte, la photo scannée ou toutes autres informations

- **Graphique :** niveau de la gravure sur le recto et / ou le verso de la carte de tout logo enseigne (ou information) ou photo permettant une identification visuelle rapide, voire un hologramme.

Le personnalisateur est le dernier maillon de la chaîne avant d'arriver chez **l'émetteur** de la carte,

Fulfillment : cette dernière étape est composée de différents services proposés par les fabricants de cartes (collage sur support, insertion de courriers ou documents publicitaires, mise sous pli, expédition) qui permettent de mettre la carte à disposition de l'utilisateur final sans nécessairement passer par l'opérateur de service.

La durée de vie de la carte passe par l'utilisation d'un verrou de blocage ce qui empêche le système d'exploitation de fonctionner.

2. Sécurité des cartes à puces

2.1. Composants sécurisés : la carte à puce

Une carte à puce est un composant de sécurité composé d'un petit rectangle en plastique (carte) et d'un circuit intégré en silicium (puce) contenant un processeur et une mémoire.

La carte à puce est très facile à transporter et assure la sécurité de son support même en déplacement.

Il est bon marché à produire et de fournir une mémoire sécurisée, plus exactement que la mémoire n'est accessible que par la carte et que la partie physiquement est protégée contre une lecture inappropriée par l'environnement.

La carte à puce a commencé comme un composant très français, porté par des chercheurs et des entreprises françaises, comme Bull, Gemplus, Axalto, Schlumberger ou Carte Bleue.

Si les cartes à puce sont des exemples importants de composants de sécurité, les autres formes de sécurités ne doivent pas être ignorées, à commencer par divers lecteurs de cartes à puce, tels que les terminaux de paiement marchands, les distributeurs de billets ou les distributeurs automatiques de billets.

Actuellement, il existe également une partie sécurisée de l'environnement d'exécution Trusted Exécution Environment (TEE) dans les appareils mobiles ou du processeur de tablette mais aussi d'un module de plate-forme sécurisée Trusted Platform Module (TPM) qui fournit des fonctionnalités cryptographiques à une carte mère.

2.2. La carte à puce, besoins de sécurisation :

Les exigences de sécurité pour les cartes à puce sont renforcées car elles sont réelles et de par divers facteurs. Par conséquent, il n'est pas facile de mettre à jour la carte à puce une fois qu'elle est répertoriée. Cette possibilité est techniquement réalisable elle en n'est pas moins difficile à mettre en œuvre sur le terrain.

De plus, les cartes à puce sont soumises à des contraintes liées à leur nature de système embarqué Toujours plus petite et toujours moins couteux ce qui réduits et limitent considérablement sa taille mémoire et sa puissance de calcul, ce qui exclut les mesures de protection les plus exigeantes.
Il faut aussi prendre en considération que l'environnement de la carte à puce est hostile.

Elle peut être attaquée physiquement, soit après un vol, soit directement par le titulaire de la carte. Une carte à puce contient généralement des informations auxquelles même le titulaire ne peut pas accéder (par exemple, une clé de cryptage). Exemple la télévision à péage et des décodeurs piratés.

Les utilisateurs de carte vitale par exemple peux être intéresser à les pirater afin de bénéficier des remboursements à 100% ou des passeports biométriques afin de pouvoir les vendre.

La demande croissante de sécurité a incité les institutions à réagir en conséquence aux niveaux national et international. Il s'agit du processus de certification des composants de sécurité et de norme, qui sera abordé dans ce mémoire.

2.3. Certification d'un composant sécurisé

Ce processus de certification vise à évaluer les allégations de sécurité formulées par les fabricants de composants à des fin de sécurité de manière standardisée.

Leur certification permettra aux clients de produits de sécurité de les choisir en connaissant de leurs niveaux de sécurité, et ainsi garantir une équivalence au niveau de sécurité entre deux produits similaires. Tout ce processus permet de garantir que le guide de l'utilisateur du composant de sécurité

Précise l'ensemble des conditions à respecter par le client et l'utilisateur afin d'atteindre le niveau de sécurité du certificat émis.

Le processus est établi dans le cadre prédéfini de la norme commune (CC) 5 qui constitue la norme ISO 15408 ce qui permet aux certificats délivrés par toute agence nationale d'être valables internationalement (notamment en Europe mais aussi dans d'autres pays

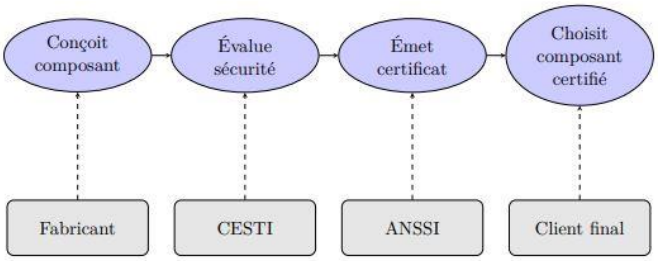

Figure 14 Certification

Un processus plus léger que la certification CC, la Certification Sécuritaire de Premier Niveau (CSPN) a été mis en place par l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI) en 2008.

6.2 Standardisation

D'après ***Louis Guillou Expert émérite Division R&D de France Telecom***, dans son livre **« Histoire de la carte à puce du point de vue d'un cryptologu**e » ou celui s'intéresse de près à la sécurisation de nos cartes à puce et notamment à travers la normalisation de celle-ci

« la carte confine des clés et des algorithmes ; elle contrôle son propre usage ; elle reconnaît son porteur. Bien sûr, la sécurité absolue n'existe pas, mais la sécurité peut toujours s'améliorer. La sécurité des cartes repose sur des logiciels spécifiques, évalués selon la méthodologie des critères communs et des profils de protection »

Louis Guillou

Aujourd'hui, le principal intérêt des cartes à puce est que leur niveau de standardisation est excellent. Peu importe si votre carte bancaire est émise par une banque française, elle peut être consultée et lue sans problème dans le distributeur situé au bout du monde

La normalisation ne concerne non seulement la puce, mais également les dimensions physiques de la carte et les pistes magnétiques ou pistes qu'elle peut prendre en charge ; pour les cartes bancaires,

Normes ISO 7816 :

Les cartes asynchrones peuvent être divisées en deux types principaux : **Programmables et non programmables.**

Les programmeurs d'applications de cartes à puce peuvent placer la logique d'application sur le terminal ou la carte (si cette dernière est programmable). Nous pouvons assimiler les cartes asynchrones non programmables au stockage externe (à l'aide d'équipements de sécurité.

Par conséquent, nous pouvons stocker des informations portables sur la carte et la logique d'application sera distribuée du côté du terminal. Mais aussi il ne faut pas oublier qu'une carte à puce programmable (telle qu'une carte Java) permet de construire partiellement la logique d'application sur la carte.

2.5. Normes

Pour définir une carte à puce, au moins trois types de paramètres différents doivent être standardisés :

- **Logiciel** qui va définir la façon de parler avec la carte, les commandes que la carte peut interpréter et son comportement
- **Électriques**, utilisés pour spécifier la tension d'alimentation et le niveau électrique utilisé, puis là la disposition des broches de la puce sur la carte
- **Physiques**, indiquant la taille de la carte et l'emplacement de la puce et de ses contacts

Cela a produit de nombreuses normes internationales :

- **ISO 7816-1 :** Les caractéristiques physiques de la carte, ça taille et limitations physiques que la carte peut prendre en charge.
- **ISO 7816-2** : La taille, la fonction et l'emplacement des contacts du micromodule sur la puce de la carte. Ces paramètres sont liés à l'alimentation, à la masse, à l'horloge, à la réinitialisation, aux ports d'entrée / sortie et à la tension de programmation sur la plupart des cartes.
- **ISO 7816-3** : signaux électriques et protocoles de transmission utilisés dans l'échange entre la carte et le terminal. Deux protocoles de communication sont définis dans ce standard et peuvent être utilisés. Le protocole T=0 et protocole T=1
- **ISO 7816-4 :** Un ensemble de commandes standardisées pour l'échange de données avec la carte. Ce standard, définit également le système de fichiers en couches pouvant exister sur la carte.
- **ISO 7816-5** : Un système de suivi et d'enregistrement ordonné pour les applications de cartes
- **ISO 7816-6** : Cette norme spécifie les données pour les applications de communication
- **ISO 7816-7 :** Cette norme spécifie les commandes du langage de requête CQL.
- **ISO 7816-8 :** Sécurité des applications intersectorielles.
- **ISO 7816-9 :** commandes et contrôles avancés dans les applications intersectorielles.
- **ISO 7816-10** : cartes synchrones.

Normes principales :

La norme ISO 7816 – 1 précisant les caractéristiques physiques de la carte ;
la norme ISO 7816 – 2 définissants la position et le brochage des contacts de la carte à puce ;
la norme ISO 7816 – 3 définissants les niveaux électriques et les chronogrammes de bas niveau qui régissent le dialogue avec les cartes à puce ;
la norme ISO 7816 – 4 enfin, définissant les différentes commandes de base des cartes à puce.

ISO 10536

Les standards ISO 10536 concernent les cartes à puce sans contact.

• **ISO 10536-1** : spécifie les caractéristiques physiques de la carte.
• **ISO 10536-2** : spécifie la taille et l'emplacement des composants de communication radio
• **ISO 10536-3** : spécifie les protocoles de communication et les signaux électriques

EMV

Depuis la mise en place du système de carte à piste en Amérique du Nord dans les années 1970, nous avons mis en place des normes qui incluent trois caractéristiques de base

- **Fiabilité, interopérabilité et sécurité**

Mais parce que la sécurité n'était pas toujours présente, les organismes ont essayé de renforcer les normes actuelles. Résultat : il y a toujours plus de clones et de fausses cartes de suivi en circulation.

Lorsqu'ils ont créé la nouvelle norme EMV, ils faisaient face à un double défi : d'un côté, ils ne voulaient pas perdre les acquis des 30 dernières années et de l'autre côté, les transactions réglementées par cette nouvelle norme devraient tenir compte des paramètres et exigences de la nouvelle méthode de paiement en ligne sur Internet.

Concernant les cartes bancaires, les institutions financières internationales Visa, Mastercard et Europay ont défini la norme EMV entre 1993 et 1996.

Ce standard couvre les protocoles, données, instructions et transactions des cartes bancaires intelligentes. Ils ajoutent de nouvelles fonctionnalités de sécurité au mécanisme de protection des données stockées

CEN

La norme CEN intervient uniquement dans le secteur financier, notamment Portefeuille électronique multifonctionnel. Il permet de définir les données de la carte et les instructions ainsi transactions, les applications qui utilisent ce PME.

Sécurisation physique à l'utilisation

L'architecture de sécurité des cartes de transactions financières est normalisée dans ISO 10102, tandis que ANSI X9.17 et ISO 8732 spécifient la gestion des clés.

Le support rectangulaire en plastique contient l'élément d'identification de l'émetteur de la carte et les paramètres personnalisés du dossier du titulaire de la carte.

La partie recto de la carte comporte :

- Les contacts des microprocesseurs de la carte à puce,
- Les Impressions des logos des émetteurs de cartes, des institutions financières et des réseaux de cartes bancaires ;
- L'embossage du numéro de carte, nom du titulaire, durée de validité ;
- Un hologramme est mis pour améliorer la sécurité et compliquer les tâches des fraudeurs

Partie visible au verso comporte :

- Un endroit destiné à la signature du porteur
- L'adresse en cas de perte
- Éléments d'identification et de vérification des codes confidentiels,
- La date d'expiration
- Pistes magnétiques. Avec Les fonctionnalités accessibles par le porteur qui y sont enregistrées

Il faut savoir que le numéro de carte est composé de 10 à 19 caractères, groupés par quatre chiffres. **Le premier chiffre** du premier groupe indique le réseau d'acceptation (Visa est 4, MasterCard est 5). **Le second les codes** du pays, de l'établissement et de la banque émetteur.

Les quatre derniers chiffres constituent une clé de vérification, appelée "**clé de Luhn**"

Les cartes à puce contiennent un circuit résistant et qui est robuste face aux intrusions, qui bloquera la fonction de sortie une fois qu'une attaque physique est détectée. Une couche diélectrique va permettre une résistance passive, qui non seulement protège la puce de la poussière et saleté, mais qui va surtout la protège également des radiations.

Il faut savoir que si la couche passive est détruite ou éliminée, la puce réagira aux différences de lumière, de température ou de la tension. L'enregistrements de mots consécutifs peuvent être distribués sur des unités de stockage non adjacentes afin de compliquer la tâche aux l'attaquants. Des fusibles peuvent être placer avant la distribution pour désactiver le mode de test utilisé par le fabricant.

2.3 Les acteurs

Les acteurs d'une certification de produit sont : Le fabricant qui va concevoir un produit de sécurité qu'il voulait vendre.

Il va donc rédiger une exigence d'évaluation à l'organisme national de certification. Après avoir accepté la demande, il va donc contacter le laboratoire d'essais.

- **Le Centre d'Évaluation de la Sécurité des Technologies de l'Information (**CESTI), Il s'agit d'un laboratoire d'évaluation agréé par l'organisme national de certification. Le centre d'évaluation évalue d'abord puis génère un rapport d'évaluation technique.
- **L'organisme national de certification** reçoit le rapport d'évaluation technique, le vérifie et délivre un certificat. En France, c'est **l'ANSSI** qui joue ce rôle

Les clients finaux sont concernés par le produit et ses caractéristiques de sécurité vont donc acheter le produit et utilise le guide des composants sécurisés pour connaître les règles d'utilisation du produit

Sécurisation pendant la production

La fabrication, la personnalisation et la distribution des cartes à puce se déroulent en sept étapes :

1. La conception et le développement des circuits intégrés ;
2. La conception et le développement du progiciel de la carte
3. La fabrication des galettes de silicium ;
4. L'insertion du progiciel, la mise sous boitier du circuit intégré et le contrôle final ;
5. La pré-personnalisation de la carte en offrant des programmes relatifs à l'usage final avec vérification de leur fonctionnement ;
6. La personnalisation du circuit intégré, c'est-à-dire l'enregistrement des noms de l'organisme émetteur et du porteur et l'insertion du logiciel des applicatifs ;
7. L'information de la carte sur le support plastique après l'embossage, l'impression des logos en vue de sa distribution.

De multiples acteurs sont donc créés dans la production de cartes à puce, en particulier :

- Les concepteurs des circuits intégrés et des logiciels de sécurité ;
- Les fabricants des circuits intégrés et les producteurs des logiciels de sécurité.
- Les autorités de certification : les développeurs de l'applicatif.
- Les producteurs des cartes (embosseurs, imprimeurs.) ;
- Les émetteurs des cartes, qui sont les entités légalement responsables du contenu de la carte et des livraisons de chaque carte individuelle pour son destinataire.

La sécurité d'une carte à puce doit tenir compte de toutes les étapes de sa production et de sa transmission entre les différents participants et acteur. Avant de passer à l'étape suivante, chaque étape du cycle de production doit garantir une sécurité adéquate
Au stade de **la conception**, la sécurité implique la protection des spécifications des circuits intégrés, des documents de conception, des logiciels, des programmes prédéfinis et le contrôle de l'ensemble de l'environnement de production.

La stratégie de sécurité doit établir une liste des menaces possibles et des contre-mesures possibles pendant la fabrication et le transport.
Le contrôle de l'environnement de production comprend par conséquent, les matériaux et les outils utilisés, la production terminée, la ferraille et l'inventaire

Il existe plusieurs menaces potentielles comprennent les divulgations réglementaires, les modifications ou le vol de biens ou de matériaux et la manipulation logicielle au niveau du micrologiciel des circuits intégrés ou des systèmes d'exploitation

C'est le travail des circuits intégrés d'assurer la sécurité des tranches de silicium pendant le processus de fabrication. A ce stade, la puce est sondée individuellement tout en restant dans la tranche de silicium pour vérifier le fonctionnement du microprocesseur

Le chiffrement symétrique utilisant est alors utilisé via une clé de fabrication si la puce est déclarée bonnes ce qui va bloquer la celle-ci ainsi que le numéro de lot et le numéro de fabricant sont également gravés. On utilise donc un algorithme dit "diversifié" pour générer la clé de fabrication à partir de la clé principale
Cet algorithme permet d'utiliser le numéro de série de la carte pour dériver la clé de fabrication de la clé mère.

Cette méthode permet **d'authentifier** tous les lots sans stocker toutes les clés. A l'issue de cette étape, les puces défectueuses sont extraites et les puces testées sont livrées au fournisseur de la carte. Pendant la phase de pré-personnalisation, le fournisseur des cartes découpe la galette pour détacher les puces individuelles

Dans la phase de pré-personnalisation, le fournisseur de cartes coupe la tranche pour séparer les puces individuelles. Celles-ci sont de nouveaux testés avant d'être moulées sous pression dans les cartes en plastique fraisées. Une fois la puce installée, puis vérifiez si les composants fonctionnent correctement, le fournisseur utilise la clé de fabrication pour déverrouiller le microprocesseur, ajouter le système d'exploitation, écrire le numéro de série de la carte puis l'empêcher accès directs à la mémoire.

A ce stade seul un adressage logique permet de terminer le dialogue avec la mémoire afin de protéger les données stockées de toute modification ou accès non autorisé.

Avant la remise à l'émetteur, la carde est de nouveau bloquer par chiffrement à l'aide de la clé de pré-personnalisation ou de transmission associée.

Lors de la personnalisation de la carte à puce, on enregistre tout un ensemble de données sur la carte puis les informations relatives à l'identité du titulaire, son code secret et son code de déverrouillage sont également stockés. L'issue de cette étape, la carte est distribuée à ses titulaires.

Selon la situation spécifique, le porteur peut modifier certains paramètres personnalisés, notamment le code confidentiel.

La plupart des cartes à puce enregistrent les tentatives d'accès infructueuses. Après un accès réussi, ce compteur sera remis à zéro, une fois que le compteur atteint le seuil limite, selon la situation, la carte bloque l'accès total ou des fichiers spécifiques mais certaines cartes laissent au porteur le choix de cette limite ;

Invalidité d'une carte

Une carte peut être invalidée pour plusieurs raisons :

- Quand La date d'expiration est arrivée à son terme. Attention tout de même car dans une carte à mono-application, la date d'expiation de l'application est aussi celle de la carte la plupart du temps. Pour les cartes multifonctions, le délai d'expiration de la carte correspond au délai d'expiration du fichier maître.
  Ce qui va générer une invalidité car lorsque l'application est obsolète, le système d'exploitation bloque les opérations d'écriture et de mise à jour, mais elle peut toujours être lue pour analyse.

- Quand tous les emplacements de la zone de stockage qui peuvent être utilisés pour collecter des données liées est saturé. Néanmoins, la carte peut toujours être lue avec un code secret, mais de nouvelles données ne peuvent pas être écrites. De nouvelles cartes doivent être émises pour éviter toute interruption de service.

- La carte n'est pas valide en raison d'une utilisation frauduleuse ou d'une déclaration de vol (y compris le blocage du code secret et du code de déverrouillage)
  Le blocage partiel (tel que le blocage de codes confidentiels spécifiques) n'affecte que les applications qui l'utilisent, et les propriétaires peuvent débloquer la carte avec le code de déblocage correspondants

3 Les attaques physiques

« La grande majorité des défaillances de sécurité se produisent au niveau des détails de mise en œuvre. »

Ross Anderson (1993)

« The great practicality and the inherent availability of physical attacks threaten the very relevance of complexity-theoretic security. Why erect majestic walls if comfortable underpasses will always remain wide open ? »

Silvio Micali et Leonid Reyzin (2003)

Les cartes à puce offrent un environnement sécurisé pour exécuter plusieurs programmes et traiter les données. De plus, elle propose des mécanismes d'authentification très robustes.
La sécurité de la carte à puce est qu'elle encapsule les données de sécurité que le microprocesseur embarqué peut traiter selon les instructions fournies par le lecteur de carte.
Pour garantir la sécurité de ces opérations, plusieurs dispositifs de protection ont été ajoutés à la carte à puce.

La sécurité est la principale qualité des cartes à puce. En effet, elle offre une haute sécurité. Elle a donc été sélectionné pour les transactions bancaires, notamment en France une haute sécurité. Il a donc été sélectionné pour les transactions bancaires, notamment en France. Cette sécurité accrue est rendue possible grâce à un ensemble de techniques variées au niveau matériel, les matériaux qui composent le corps de la carte sont conçus pour surmonter l'attaque chimique des micromodules extraits, de plus, tous les composants sont sur le même silicium.

Le microprocesseur et ses capteurs sont recouverts de résine, ce qui rend difficile le placement des sondes sur le bus interne pour la surveillance. Contrairement à la pratique dans tout le monde informatique, les attaques basées sur des vulnérabilités logicielles sont rares pour les raisons suivantes :

- Accès difficile au code
- La saisie par l'utilisateur est généralement très simple (les commandes passées via le terminal, les cartes à puce ne sont généralement pas utilisées comme lecteurs)
- Les développeurs utilisent de bonnes pratiques de développement qui ont été vérifiées dans le cadre du programme de certification
- La complexité du programme qui est limitée par l'aspect « embarqué » (en particulier, il n'y a pas de raison pour l'allocation dynamique)

Par conséquent, l'attaquant s'est tourné vers un nouveau type d'attaque sur d'autres médias, qui a donné au composant de sécurité une caractéristique particulière : **l'attaque physique**.

Les attaques physiques se déclinent en trois catégories :

- **Les attaques par canaux cachés (non invasives)**
- **Les attaques invasives**
- **Les attaques semi-invasives**

Ce nouveau concept : l'attaque physique ne considère pas seulement la sécurité du système de cryptage au sens mathématique, mais prend également en compte les aspects liés aux propriétés physiques de l'informatique.

Ces nouvelles attaques constituent une menace particulière pour les systèmes embarques tels que les cartes à microprocesseur, qui peuvent être utilisées par les attaquants pour mobiliser des outils d'analyse de plus en plus sophistiqués. Dans ce domaine, de nombreux travaux ont été menés pour mettre en avant de nouvelles stratégies d'attaque personnelle ou proposer des contre-mesures afin de prouver la sécurité en établissant des modèles adverses appropriés. C'est notamment le cas de IBM va proposer une **classification des attaques.**

Malgré tous ces mécanismes de sécurité, un attaquant peut toujours contourner ces dispositifs de protection et accéder directement à la carte.

3.1. Deux types d'Attaques sur cartes à puce standards

Il existe deux principaux types d'attaques contre les cartes à puce, à savoir les **attaques physiques** ou **matérielles** contre les cartes à puce en tant que composants matériels électroniques, et les **attaques logiques** qui exploitent des failles algorithmiques ou des défauts dans les mécanismes d'isolation. Au sein de ce mémoire nous allons étudier les attaques physiques ou matérielles.

3.2 Classification des attaques physiques

Afin d'évaluer le niveau de résistance de ses produits, IBM a proposé une taxonomie en 1991 Attaquant potentiel en **3 catégories :**

"Amateurs éclairés" (catégorie I) : Ils sont généralement très intelligents, mais avec une connaissance incomplète du système. Ils essaient souvent de tirer parti des faiblesses existantes du système plutôt que d'en créer de nouvelles

"Attaquant Expert" (Catégorie II) : Considéré comme expert Ils ont reçu une solide formation technique et ont de l'expérience. Ils ont une compréhension différente des différentes parties du système, mais il est possible d'accéder à toutes ces parties. Ils possèdent généralement des outils et des instruments analytiques très sophistiqués.

« Organisations financées » (catégorie III) : avec le soutien d'un grand nombre de fonds, elles peuvent réunir une équipe d'experts aux capacités complémentaires.
Ils peuvent effectuer une analyse approfondie du système, développer des attaques complexes et utiliser les outils d'analyse les plus modernes.

Les attaques physiques selon deux critères : **les attaques invasives ou non-invasives** et **semi-invasives**, et les **attaques actives ou passives**

4.Attaques non-invasives

Les attaques non-invasives (par canaux auxiliaires) ne touchent pas directement à la carte, mais visent plutôt à acquérir des informations sur son système, cela consiste en analysant le comportement du circuit sans affecter son intégrité en regroupent les attaques qui ne modifient pas le composant comme les temps d'exécution, la puissance ´électrique consommée, le rayonnement électromagnétique, etc.

En général, on désigne par ce terme des attaques basées sur l'observation de canaux auxiliaires, ou canaux cachés c'est-à-dire l'observation émises par le composant, et qui renseignent de façon indirecte sur celui-ci certaines fonctionnalités physiques de la carte à puce sont alors perturber sans pour autant altérer son fonctionnement. La carte est alors réutilisable après l'attaque.
En revanche, les attaques non-invasives sont par définition indétectables. Comme elles sont en général également les moins onéreuses. Prenons donc un exemple pour comprendre les attaques par canaux cachés entre un composant et un coffre-fort, le coffre-fort a pour but **de protéger son contenue**, mais il doit pouvoir s'ouvrir si nous disposons **de la combinaison**, sont ouverture repose donc sur son **code secret d'ouverture** (sécurité) donc si l'utilisateur entre la **bonne combinaison** (le code) **l'ouverture de** celui-ci est possible. En Utilisent un stéthoscope on peut écouter les sons émis par le coffre-fort pendant une attaque, ce qui permettra à l'attaquant de pouvoir tester des combinaisons d'ouverture.

Une attaque classique sur un coffre-fort est l'utilisation d'un stéthoscope pour écouter les sons émis par le coffre-fort pendant que l'attaquant teste une combinaison. Avec une écoute attentionné celui-ci peut retrouver la combinaison (code) il récupère donc le code secret en écoutant les canaux auxiliaires qui sont des artefacts d'implémentation dus au fonctionnement du coffre-fort.
Les travaux de Kocher et al sont particulière intéressant à ce sujet.

4.1. Attaques par observation non -Invasives SCA (Side Channel Analysis)

Les attaques par observation ou par canaux auxiliaires notées SCA (Side Channel Analysis) se basent sur l'observation du circuit pendant l'exécution des calculs liées au chiffrement.

En théorie, l'algorithme peut être sûr, mais le circuit qui implémente l'algorithme ne l'est pas nécessairement.

Dans la mise en œuvre simple de l'authentification par code PIN, le numéro saisi sera vérifié une fois dans une boucle. Une fois le mauvais numéro détecté, nous sortirons de la boucle.
En mesurant le temps de réponse de la carte en fonction du code PIN saisi, on peut savoir si le premier chiffre saisi est correct, ce qui limite considérablement l'espace des codes PIN possibles
Même si le mauvais numéro est détecté, il suffit de vérifier tous les chiffres du code PIN pour résoudre cette attaque.

Ces paramètres physiques peuvent affecter la sécurité de l'algorithme de chiffrement.
Ces paramètres sont difficiles à prévoir en théorie, nous parlons de fuite d'informations via le canal auxiliaire.

Seules les valeurs mesurées de ces paramètres physiques peuvent être obtenues, de sorte que ces valeurs mesurées dépendent non seulement de la fuite, mais également de l'équipement de mesure. Ce type d'attaque est non invasive. En pratique, un attaquant peut vouloir obtenir les résultats de mesure à l'emplacement précis du circuit, et finalement réaliser une attaque invasive ou semi-invasive.

4.2. Timing Attack

Timing Attack a été proposée par Paul Kocher en 1996. Cette attaque consiste à mesurer le temps d'exécution d'un algorithme, plus précisément le temps pris par un système pour exécuter un algorithme est parfois variable. Cela peut être du a certaines instructions dont le temps d'exécution L'attaque est basée sur l'observation que le temps d'exécution d'un algorithme dépend généralement de ses données, donc l'observation du temps d'exécution peut déterminer une certaine quantité d'informations sur les données, y compris quand il s'agit de données protégées en confidentialité par la carte. Cela dépend donc des données, de l'optimisation du compilateur ou de l'existence de plusieurs branches dans l'algorithme.

Prenons un exemple d'une vérification d'un code confidentiel cela peut inclure une boucle qui vérifie séquentiellement chaque chiffre du code. Si la comparaison est arrêtée immédiatement après avoir détecté le mauvais numéro, l'attaquant obtiendra des temps de réponse différents de la carte en fonction du nombre de chiffres corrects entrés, réduisant ainsi considérablement l'espace de craquage possible.

Cette attaque sont applicables à de nombreux algorithmes, y compris le chiffrement.
Comment s'y prémunir : pour éviter cela est de concevoir l'algorithme dit "équilibré", c'est-à-dire que son temps d'exécution ne dépend pas des données (au moins des données confidentielles). Tout repose donc sur la création d'un bon algorithme. Afin qu'une telle implémentation ne doive pas quitter la boucle prématurément et utilise souvent des opérations virtuelles sur des données indésirables pour effectuer les mêmes opérations quelles que soient les données.

4.3. Attaques par analyse de consommation électrique

Les attaques passives, présentent l'avantage (pour l'attaquant) de ne pas perturber le fonctionnement du système. Certaines d'entre elles ont connu depuis quelques années un retentissement tout particulier. Il s'agit des attaques par analyse de consommation électrique (power

analysis). L. Goubin et J. Patarin ont étudié en détail les attaques utilisant le principe d'analyse différentielle de consommation (Differential Power Analysis – ou DPA – en anglais).

4.3.1 Simple Power Analysis :

Consiste à mesurer directement la consommation actuelle des composants de sécurité avec un oscilloscope lors de l'exécution du code afin d'obtenir des informations sur les instructions d'exécution ou les données traitées (qui peuvent être des données à protéger).

Il est donc possible de trouver des clés privées utilisées dans RSA par une simple analyse de consommation. Dans la mise en œuvre de l'algorithme exponentiel rapide simple, pour chaque bit clé, si le bit est 1, la multiplication de la somme des carrés est effectuée ; uniquement lorsqu'il est 0, le carré est effectué.
En effet, les différentes instructions exécutées par le processeur du composant de sécurité ont chacune une consommation de courant identifiable.
En utilisant cette signature et si l'algorithme n'est pas équilibré, vous pouvez obtenir des informations sur les données traitées.
Messerges et al. Appliquent par exemple l'attaque à un algorithme d'exponentiation modulaire sur carte à puce

Figure 15 La consommation d'un carré

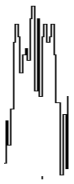

Figure 16 La consommation D'une multiplication

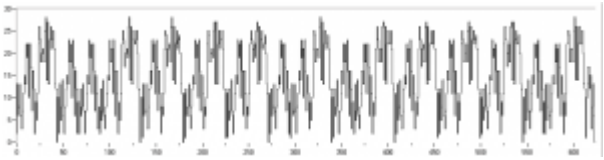

Figure 17 La clé x

Si votre bit de clé est 0, vous le multipliez par d'autres données non liées à l'opération d'alimentation, L'exponentiation modulaire est utilisée dans de nombreux algorithmes à clé publique. Les figures A.1 et A.2 montrent la différence entre une élévation au carré et une multiplication. La figure A.3, De cette façon, la clé x peut être lue directement. En effet, multiplier le carré par la multiplication correspond au bit clé égal à 1, tandis que le carré isolé correspond au bit clé égal à 0.

Aujourd'hui, Simp**le Power Analysis** n'est généralement plus disponible pour obtenir des clés de chiffrement, et toutes les implémentations peuvent résister à ce type d'attaque, mais elles fournissent toujours aux attaquants des informations utiles pour les aider à trouver des moyens de réaliser leurs l'attaques.

4.3.2 Differential Power Analysis

Comme la **Simple Power Analysis, la Differential Power Analysis (DPA)** est basée sur l'analyse de la consommation actuelle lors de l'exécution, mais contrairement à la première, la seconde est basée sur un traitement statistique du courant actuel pour identifier les corrélations liées aux données
Cette méthode consiste à diviser toutes les traces en différentes catégories et à calculer la valeur moyenne de chaque catégorie.
Si les partitions ne sont pas liées aux valeurs de mesure contenues dans la trace, la moyenne convergera vers zéro lorsqu'avec une augmentation du nombre de traces dans chaque catégorie qui augmentera.

Inversement, si la partition est liée à des données (par exemple, les mots de passe secrets), la moyenne de chaque catégorie aura tendance à être différente de zéro.
Par conséquent, les attaques DPA sont parfois effectuées dans des algorithmes de chiffrement (cryptographique)
Ont mesures ces métriques selon une hypothèse clé, puis ont les tests exhaustivement en détail jusqu'à ce que nous trouvions une convergence des moyennes de chaque classe (catégorie) vers une valeur différente de zéro

Hypothèse qui fait converger la moyenne de chaque catégorie vers une valeur non nulle : l'hypothèse correspond à la bonne clé. Cette hypothèse correspond à la bonne clé.

En 2004, Brier et al. Proposent la Corrélation Power Analysis.
« Cette méthode vise à améliorer le DPA en formalisant les facteurs de corrélation en utilisant la corrélation de Pearson et en interprétant le modèle de fuite basé sur la distance de Hamming. »

4.4. Attaque par lumière focalisée

Un nouveau type d'attaque a été annoncé En 2003 par Skorobogatov et Anderson : l'illumination locale du transistor par le laser qui permet de faire conduire le courant, ce qui perturbe ainsi sa fonction. Les auteurs utilisent cette méthode pour effectuer l'attaque BellCore (attaque sur RSA). Aujourd'hui encore, les lasers restent le premier choix des attaquants, avec un excellent contrôle du temps et de l'espace (lumière focalisée).

L'inconvénient de cette méthode est son coût élevé par rapport aux autres méthodes, et que les composants doivent être ouverts pour accéder au silicium, ce qui nécessite une attaque invasive
Les contre-mesures matérielles ont été proposées, telles que des photodétecteurs de lumière , mais ces contre-mesures sont coûteuses, ne protègent pas correctement les composants et augmentent considérablement le risque de faux positifs.

4.5. Attaque par champ électromagnétique

Quisquater et Sadyme ont testé le champ magnétique haute tension généré par la bobine de la sonde électromagnétique en 2002, les calculs ont été perturbés, mais ce n'est qu'en 2007 que Schmidt et Hutter ont utilisé ce principe pour effectuer une attaque BellCore (RSA) à l'aide d'un générateur d'impulsions électromagnétiques. Plusieurs expériences ont été mener par Ordas et al en 2014, ce qui a permis à cette attaque de gagner en popularité.

La démocratisation des équipements d'attaque s'est accompagnée de l'émergence de COTS dédiés à l'injection EM (utilisés à l'origine pour conserver les aliments dans l'industrie).
Le principal avantage théorique de l'injection électromagnétique sur les lasers est la capacité d'attaquer à distance sans ouvrir les composants.

En fait, il doit généralement être ouvert sur la partie fixe. Le contrôle temporel de l'attaque électromagnétique est légèrement moins fin que le contrôle temporel du glitch et du laser, car il est nécessaire de charger le générateur d'impulsions pendant un certain temps avant de commencer l'attaque. A l'inverse Le contrôle de l'espace est bien meilleur que l'attaque de glitch, et est similaire au contrôle laser, même dans la pratique, il n'est toujours pas aussi concentré.

4.6. Attaque par glitch

Quand nous pensons aux attaques par glitch deux grand nom ressort Andersen et Kuhn, en effet ils se sont beaucoup intéressés à ce sujet en 1998.

Cette attaque est basée sur des impulsions électriques brutales et évidement importante envoyée à l'alimentation ou à la masse du composant.
Le contrôle de l'espace est presque inexistant, et les deux seuls points d'accès sont la puissance et la masse du composant.

Le contrôle du temps est avantageux pour l'application du glitch en lui-même, mais est défavorable pour la durée du glitch L'avantage de cette méthode est que son coût est très faible (un générateur d'impulsions électriques), et qu'il n'est pas nécessaire d'avoir un accès au silicium (pas besoin d'ouvrir le composant par une attaque invasive). Les **contre-mesures matérielles** pour de telles attaques sont très efficaces, et les composants de sécurité certifiés AVA_VAN5 doivent tous résister aux défauts que porte leurs résistances face au glitch.

4.7. Attaques par conditions anormales

Ces attaques consistent à perturber le fonctionnement normal de la carte pour modifier son comportement. Cela peut être fait en interférant avec l'entrée de la carte (comme la tension ou la fréquence d'alimentation) Ces perturbations peuvent également être externes, par exemple en modifiant la température.

Cependant, les cartes à puce sont généralement équipées d'un détecteur d'état anormal, ce qui rend ce type d'attaque difficile.

4.8. Semi-Invasive

Les attaques semi-invasives sont des attaques physiques qui ne modifient pas la carte de façon permanente ou temporaire pendant le fonctionnement de la carte.
Lorsqu'un attaquant retire l'enveloppe de la puce accéder à sa surface, mais garde intacte la couche protectrice du micromodule (ces attaques ne nécessitent pas de contact électrique avec la surface métallique).
Les attaques semi-invasives les plus courantes sont les attaques par interférence, qui peuvent être accomplies par des lasers, des champs électromagnétiques ou même de simples interférences électriques (***vue plus haut dans le mémoire***).
L'idée est, par exemple, d'interrompre occasionnellement l'alimentation de la carte à puce ou d'utiliser des rayons ultraviolets pour interférer avec le fonctionnement des transistors, provoquant une panne matérielle.
En réponse à ces problèmes de sécurité spécifiques, deux solutions peuvent être distinguées, selon qu'elles reposent entièrement sur des processus logiciels ou qu'elles impliquent la conception et l'usage de matériels spécifiques.
Il faut savoir qu'une attaque par interférence ont toujours pour effet d'introduire des défauts dans le code que la carte exécute.
Certaines de ces pannes peuvent amener les attaquants à exploiter ces vulnérabilités Étant donné que l'impact de ces défauts peut être très divers, les défauts sont actuellement modélisés à l'aide de modèles de fautes, qui décrivent la nature des fautes. Ensuite, nous trouvons la vulnérabilité en appliquant le modèle de défaillance au code

4.8. Attaque par injection de fautes

Les attaques par injection de faute FIA (Fault Injection Analysis) profitent des effets des interférences intentionnelles sur le fonctionnement du circuit.

Les attaques par injection de faute sont basées sur l'idée d'interrompre le circuit. Pour une attaque, une ou plusieurs injections peuvent être effectuées.
C'est l'une des attaques physiques les plus courantes, basé sur les caractéristiques du silicium et peut modifier les propriétés électriques dans certains cas.

Par conséquent, l'attaque consiste à utiliser cette propriété pour perturber l'exécution des programmes (tels que les algorithmes cryptographiques) intégrés dans la puce, afin qu'ils aient un comportement anormal qui peut être exploité.

Ces attaques sont des menaces non seulement pour les algorithmes cryptographiques, mais aussi pour d'autres composants Logiciel, tel que la machine virtuelle
Christophe Giraud. Attaques d'écosystèmes embarqués et contre-mesures associées. PhD thesis, Université de Versailles Saint-Quentin-en-Yvelines, 2007.

Le fonctionnement des circuits électroniques peut être perturbé par des rayonnements tels que les rayons ultraviolets, les EM, les rayons X et la lumière blanche. Le but est de modifier le contexte d'exécution de l'application intégrée ou de changer une partie du contenu de la mémoire.

L'attaque en faute peut avoir deux conséquences différentes :

- **Permanent, afin de modifier en permanence la valeur de l'unité de stockage ;**
- **Pendant la transmission sur le bus de données, modifiez temporairement les valeurs des opérations et / ou des variables temporairement.**

Chaque injection entraînera une défaillance, appelée défaillance ou erreur évidente
En d'autres termes, il existe des différences évidentes de comportement ou de sortie de programme, et certaines erreurs sont Vulnérabilité, c'est-à-dire qu'un attaquant peut utiliser la vulnérabilité pour saper les attributs de sécurité fournis par le programme.

Mais Les attaques FIA sont généralement puissantes, cependant, ce sont généralement des attaques Invasives ou semi-invasives, elles impliquent un risque non négligeable, à savoir des dommages, voir la destruction du circuit. En fait, les outils d'injection tels que les lasers peuvent Détruisez une partie du circuit

C'est pourquoi les attaquants dans les « attaques par injection de faute » Essayez généralement de minimiser le nombre de défauts à injecter pour limiter le risque de défaillance.
Il existe de nombreuses façons d'injecter des défauts dans le circuit : laser, modification Tension, modification de l'horloge interne du circuit, etc.
Ainsi que **différente type d'attaque à injection** :

- Injection de fautes et **attaque par perturbation** : les conséquences des attaques par interférence peuvent être simulées en injectant des **erreurs dans le code** exécuté par le composant de sécurité.
- Injection de fautes et code : touche à la nature du code
- Attaques de type **DFA (Differential Fault Analysis)** : une technique de cryptanalyse qui exploitent des résultats erronés obtenus par injection de fautes. L'analyse de ces résultats se fait au niveau des données.

Cependant, la présence de détecteurs embarqués dans la puce permet de limiter ces attaques.
Les cartes à puce sont généralement équipées de contre-mesures adaptées à ces attaques, qui incluent l'insertion de retards aléatoires dans l'exécution du programme afin qu'ils ne soient pas si facilement observés et même certaine carte bancaire possèdent des détecteurs d'illuminations laser

3.Attaques invasives :

Les attaques invasives, c'est un peu la « méthode agressif » des attaques physiques.
Elle consiste à retrouver la localisation des informations sur la carte en modifiant les informations de manière irréversible (et éventuellement destructrice) sans hésitation.

Par exemple, il se peut que la couche métallique du circuit soit retirée pour exposer la ROM et que le code qu'elle contient puisse être lu directement.

L'attaque dite invasives se caractérise par une modification physique permanente du matériel attaqué. Indépendamment de la nécessité de détruire les composants de sécurité qui les appliquent, ils sont divisés en deux catégories. Pour le premier cas, on parle d'attaques destructrices. En termes de temps et d'équipement spécifique, c'est généralement l'attaque la plus coûteuse. Ils sont généralement exécutés par des experts et se déroulent en deux étapes :
Préparer le circuit puis vient l'attaque.

Ces attaques pénètrent réellement dans le circuit afin d'opérer sur observation directe ou modification. Ils sont très efficaces, mais présentent deux inconvénients principaux :

- **Ils endommagent parfois le fonctionnement du circuit**
- **Présentent un taux de d'échec élevé**.

Les cartes à microprocesseur sont munies de mécanismes de protection pour contrecarrer les attaques invasives. La technologie actuelle utilisée met ainsi en jeu (entre autres) plusieurs couches m´métalliques de protection, des d´détecteurs d'intrusion, ou encore un stockage des données sous des formats particuliers qui rendent tr es difficile leur interprétation.

Un certain nombre de contre-mesures matérielles peuvent être mises en œuvre pour se protéger des attaques invasives, dont le Layer Anti-Probing, qu'il faut contourner pour pouvoir attaque.

3.2 prépare l'attaque

Les attaques intrusives nécessitent un accès physique aux composants internes de la carte Par conséquent, avant qu'une telle attaque puisse être effectuée, il est nécessaire de révéler le circuit de la puce.
Le processus de « préparation » d'une attaque intrusive nécessite peu d'équipement et d'expérience, de sorte que tout le monde peut jouer aussi longtemps que l'équipement nécessaire est disponible. De plus, on comprend que ces opérations qui nécessitent l'utilisation de fortes concentrations d'acide nécessitent certaines précautions : l'utilisation de hottes, de lunettes de protection, etc.

3.2.1 Décapsulation de composants :

La décapsulation des composants consiste à retirer l'emballage du composant sécurisé afin que le silicium soit accessible directement.

Une petite quantité de solution acide est généralement appliquée au troue formé dans la puce préchauffée avec une pipette. Elle est réalisée sur les composants chauffés à une concentration

élevée d'acide nitrique fumant à 60 °, la colle est ramollie et le module de la puce peut alors être enlevé par pliage. Il est alors nécessaire de former des cavités par erosion mécanique pour que l'acide n'agisse que sur des zones bien définies.

Bien que cette opération soit dangereuse, elle ne nécessite pas de connaissances en chimie ou en électronique, et ses connaissances, de simple connaissance qu'on peut avoir au secondaire suffisant. Cette opération est généralement effectuée sur le composant de manière non destructive, c'est-à-dire que le composant peut toujours fonctionner après décapsulation.

Cette attaque est très utile car elle permet par la suite d'autres attaques : dans les attaques intrusives, la rétro-ingénierie matérielle nécessite une décapsulation et un micro-palpage
Dans les attaques semi-intrusives, les attaques au laser sont possibles par décapsulation, tandis que les attaques électromagnétiques sont grandement facilitées.

3.2.2 Rétroconception matérielle

La rétroconception matérielle Conçu pour comprendre toutes les opérations de démontage des composants de sécurité pour en savoir plus sur leurs natures et on va comprendre la structure et la fonction des dispositifs internes à un système.
Il s'agit d'une attaque destructrice car elle nécessite une élimination continue de toutes les couches (métal, silice) Que comprend le composant, qui sont photographiées avant leur élimination. Dans le cas d'une carte à puce attaquée, il s'agit de déterminer l'architecture de la puce.

Avec suffisamment de détails, on peut observer directement les transistors qui composent le composant et sa logique de mémoire. Ensuite, le code du programme du composant de sécurité peut être lu directement dans la ROM, afin que le logiciel puisse être rétro conçu. En étudiant les schémas de connexion et en dessinant des lignes qui connectent clairement différents modules, vous pouvez identifier rapidement les structures de base telles que les circuits de données et d'adresses.

Normalement, tous les modules sont connectés au bus principal via un bus facilement identifiable. Malheureusement, la rétro-ingénierie (rétroconception) du matériel est très difficile sur le matériel actuel, en particulier en raison de la finesse de la gravure et parce que le contenu de la ROM est généralement crypté dans des composants de sécurité.

3.2.3 Déprocessing

Il ne faut pas oublier qu'une puce standard possède de nombreuses couches :

- La couche la plus profonde du substrat constitue le transistor
- Une couche d'oxyde isole la porte de la zone active des transistors.
- Une couche de poly silicium
- Les couches métalliques, généralement faites d'aluminium
- Couche intercalaire d'oxyde isole les couches conductrices
- Couche de passivation faite d'oxyde de silicium

Il existe deux applications principales pour le deprocessing des puces :

- **Retirer la couche de passivation et à exposer la couche métallique supérieure pour une attaque par microsonde.**
- **Pénétrer dans la couche la plus profonde pour étudier la structure interne de la puce**

Il existe différentes méthodes de traitement : **par gravure chimique, par gravure plasma ou par gravure mécanique**. En cas d'attaque chimique, des produits spécifiques sont retirés de chaque

couche. Le trou résultant dans la couche peut être suffisamment petit pour qu'un seul fil du bus soit exposé. Cela évite des contacts accidentels avec les fils voisins et le trou stabilise également la position de la sonde, la rendant moins sensibles aux vibrations et aux variations de température

3.3. Micro-sondage

Une attaque par microsonde est une **attaque invasive** et non destructive qui vise à placer la sonde sur des fils très spécifiques du composant afin que le courant traversant ces fils puisse être observé. Ce type d'attaque nécessite beaucoup d'équipement, généralement : ***microscopes, micromanipulateurs, différents types de sondes, équipements de test.***

Les sondes installer peut soit être **passive ou active** :

- Des **sondes passives** peuvent être utilisées pour détecter ou injecter des signaux, mais elles doivent être connectées à un oscilloscope. Il est impossible d'utiliser des sondes passives sur le circuit interne de la puce,
  Elle peut permettre également de se connecter à la puce décapsulée.
- Une **sonde active** possède un transistor. Il offre une large bande passante et une capacité électrique et une résistance élevée

Généralement, afin d'extraire des informations, telles que le contenu d'une mémoire ou d'une
Il est difficile d'observer l'intégralité du bus à un moment donné et certaines techniques sont utilisées pour surmonter ce problème.

3.4. Sonde ionique focalisée (FIB)

En raison de l'effet de pulvérisation, la FIB est utilisée comme un outil de micro-fabrication, pour modifier ou pour usiner la matière à l'échelle micrométrique ou nanométrique.
Il peut être utilisé non seulement pour créer des points de mesure, mais aussi pour afficher et réparer ou même créer de nouveaux circuits.

Une FIB peut également être utilisée pour déposer des matériaux. On parle de « déposition induite par faisceau d'ions ». Le FIB se compose d'une chambre à vide et d'un pistolet à particules équivalent à un microscope électronique à balayage, sauf que les ions gallium sont accélérés au lieu d'électrons et émettent un faisceau lumineux d'un diamètre de 5 à 10 nm à partir de la cathode en métal liquide.il peut donc afficher des échantillons d'images avec une résolution de 10 nm.
Contrairement aux microscopes électroniques à balayage, les FIB sont destructives. Quand des ions gallium de haute énergie sont projetés sur un échantillon, ils pulvérisent les atomes de la surface de l'échantillon.

5.Contre mesure des attaques par faute

Principe de détection des intrusions : Il existe deux classes de détection d'intrusions classiquement implémentées dans les composants de sécurité.

5.1. Capteurs physiques

La première catégorie vise à utiliser des capteurs d'amplitude physique pour détecter les interférences (perturbations) causées par les attaquants. Divers capteurs ont été installés pour détecter les changements anormaux de la tension d'alimentation, de la fréquence d'horloge, de la température et de l'éclairement des composants. Ce dernier type de détection est généralement effectué dans la direction opposée. Avant d'utiliser un photo-diodes

5.1Détection d'erreur

La deuxième catégorie vise à détecter les erreurs causées par ces perturbations dans le circuit. Il existe deux sous-classes de détection

La différence entre ces sous-catégories est illustrée par le schéma du système illustré à la figure 2.1 (qui peut être matériel et logiciel). Chaque sommet du graphe (numéroté de 1 à 5 dans l'exemple) est associé à l'état interne du système, et chaque bord du graphe est associé à une séquence possible d'états du système

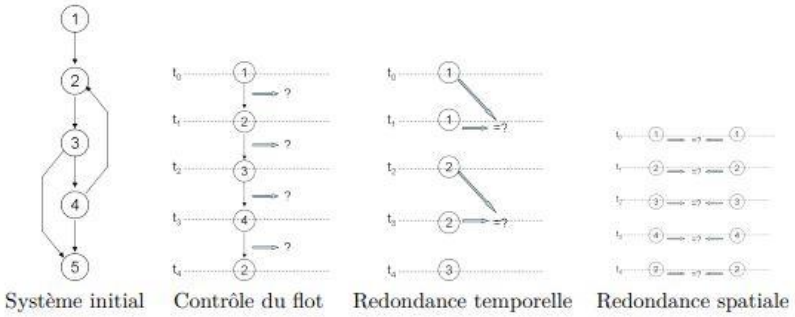

Figure 18 Schéma détection d'erreur

6.Contre-mesures contre les attaques par observation

Le principe des contre-mesures contre les attaques par observation se base généralement sur la réduction du rapport entre le signal et le bruit. Celle-ci est parvenue soit en réduisant l'amplitude du signal soit en ajoutant du bruit.

6.1Réduction du signal

On distingue deux techniques permettant de réduire le signal :

Équilibrage : te technique vise à maintenir une grandeur physique du circuit (consommation, temps de calcul, etc) constante quelles que soient les données manipulées. Afin d'équilibrer la consommation du circuit, de nombreuses études ont suggéré d'utiliser un circuit logique à double rail basé sur le code 1 en 2 pour maintenir la symétrie entre les bits "1" et "0". L'architecture de ce circuit est généralement composée de circuits logiques complémentaires au circuit d'origine pour équilibrer la conversion

Filtrage : implanter dans une puce un circuit dédié servant à isoler l'alimentation externe de celle interne du circuit en utilisant deux capacités de découplage. Dans un premier temps, la capacité 1 est chargée par la source d'alimentation externe tandis que la capacité 2 est déchargée en alimentant le circuit. Dans un second temps, les rôles de ces deux capacités sont inversés. Ainsi, le courant observé à l'extérieur est uniforme, ce qui rend le circuit immunisé contre l'attaque en consommation.

7.Contre mesure Cryptographie

7.1Analyse de la consommation

Afin de répondre aux attaques par l'analyse actuelle, différentes techniques existent.
Par exemple, qu'un algorithme qui ne modifie pas la consommation d'énergie pendant l'exécution peut être dessiné.
Cependant, comme ces changements ne peuvent pas être réduits à zéro, il est difficile à mettre en œuvre. Par conséquent, au contraire, une autre méthode consiste à intégrer le bruit dans la mesure de la consommation d'énergie. Par conséquent, la lecture ne peut pas être directement liée à l'algorithme, ce qui complique l'exécution de cette attaque.

Une façon de procéder consiste à ne pas décrypter directement le mot de passe, mais à décrypter l'emplacement du mot de passe en mémoire avant de le comparer avec le mot de passe indiqué par l'utilisateur. Ce type d'attaque ne peut pas identifier uniquement l'emplacement du mot de passe et ne peut pas le décrypter sans posséder physiquement la carte.

8.Contre mesure matérielles

8.1. Rendre les composant toujours plus petit

Du fait des progrès de la miniaturisation, un grand nombre de transistors peuvent désormais être rassemblés sur une très petite surface. Cette capacité permet aux fabricants de cartes à puce de produire des puces en plusieurs couches, chaque couche contenant de nombreux composants différents, et les couches sont interconnectées. De cette façon, l'architecture de la puce a trois dimensions, ce qui rend la tâche de l'ingénierie inverse de l'attaquant et de toutes les attaques invasives voire semi-invasives plus difficile.

8.2. Sondes pour contre les attaques

Les techniques d'attaques de brouillage et autres attaques sur les canaux auxiliaires tentent de changer l'environnement de la carte.
Les stratégies développées pour ces attaques incluent l'utilisation de capteurs sur la tension, la fréquence et la température du circuit. Mais la sonde ne peut pas détecter tous les signaux injectés

8.3. Réunir et regrouper les composants

De réunir dans une seule et unique pusse tout le matérielles électronique ce qui rend plus difficile les attaques invasives de type rétroconception matérielle pour ce faire on réunit et regroupe tous les composant ensemble ce therme prend parfois l'appellation de : colle logique. Cela augmente la difficulté d'un attaquant qui souhaite faire de l'ingénierie inverse, et augmente également la difficulté d'une attaque qui nécessite l'installation d'une sonde ou même endommage le fusible de sécurité.

8.4. Dissimulation :

La principale contre-mesure est de mettre en œuvre une sécurité par la dissimulation : de cette façon, moins un attaquant dispose d'informations sur le système mieux les informations sont cachées.

8.5. Rajouter un maximum de couche :

L'ajout d'une couche métallique qui agit comme une couche de protection au-dessus de la puce peut éviter la plupart des attaques invasives ou semi-invasives

8.6. Moins d'information :

De plus, dans les circuits impliquant des puces électroniques, une contre-mesure évidente est de supprimer les informations afin de pouvoir identifier les puces en question, à savoir leurs numéros de série, les informations de référence du fabricant, Par conséquent, l'attaquant dispose de moins d'informations pour identifier la nature du circuit à détruire.

Conclusion

Les cartes à puce sont des dispositifs sûrs et sont de plus en plus utilisées dans le monde. Leur succès est principalement dû à leur aspect tamper-resistant, qui permet de stocker de manière sécurisée des informations sensibles (clés de chiffrement).

Compte tenu des nombreux domaines sensibles de l'utilisation des cartes à puce (banque, médical, téléphone), certaines recherches se sont concentrées sur la sécurité et les attaques possibles sur ces appareils il en va de ce mémoire qui s'intéresse tout particulière à cette notion de sécurité car en effet durant Ces dernières années, des attaques de plus en plus sophistiquées ont été développées qui permettent d'extraire des données sensibles et de perturber les fonctions prévues de la carte. Tout au long de ce mémoire, nous avons présenté l'architecture physique d'une carte à puce afin de mieux cerner les vulnérabilités en cas d'attaques physiques. Nous avons aussi donné l'intuition nécessaire pour comprendre ce que l'attaquant cherche réaliser grâce à ces attaques.

Pour ce faire, nous avons expliqué comment fonctionnais une carte à puce à travers sa communication ainsi que les composants matériels de l'architecture en présentent l'aspect fonctionnel des considérations en sécurité en mettant en évidence le besoin d'exprimer des garanties de sécurité. En effet, les composants de sécurité tels que les cartes à puce sont des types spécifiques de matériel qui fournissent des attributs de sécurité.
Pour garantir que ces fonctionnalités contre un large éventail d'attaquants puissants, des règles strictes ont été adoptées, telles que des normes ou des spécifications communes.
Des laboratoires dédiés, les CESTI, sont chargé d'évaluer la sécurité de ces composants dans le cadre de cette réglementation. Une partie de cette évaluation consiste à déterminer la robustesse des composants qui sont effectués à l'aide d'un équipement dédié pour prévenir des différentes attaques (lasers, injecteur électromagnétique). Lors de la mise en œuvre de mon mémoire, s'intéresse particulièrement protéger les cartes à puce par la standardisation, les normes et la certification.
Mais il faut retenir que les composants de sécurité, parce qu'ils contiennent des informations confidentielles, font l'objet d'attaques.

Celles-ci tentent généralement de violer la confidentialité, l'intégrité ou l'authenticité des données protégées par des algorithmes cryptographiques intégrés à ces composants.
Les attaques dites matérielles ou physiques tirent parti des faiblesses de ces algorithmes dans la mise en œuvre matérielle.
Je me suis donc intéressé aux différentes attaques sur les composants qui protègent des informations confidentielles, parmi ces attaques, celles dites par « canaux cachés » (« Side Channel Attacks » sont particulièrement efficaces : elles utilisent la corrélation qui existe entre les données traitées (dont celles qui sont sensibles) et la consommation, le rayonnement électromagnétique ou le temps de réponse du composant.

Un autre type d'attaques, dites par « injection de fautes » consiste à modifier volontairement le fonctionnement du circuit pour contourner les protections logicielles et matérielles destinées aux informations sensibles. Par exemple, le fonctionnement du composant peut être affecté, grâce à l'éclairage laser, modifiez la tension d'alimentation ou Fréquence d'horloge.
Puis un troisième type d'attaques, plus difficile à mettre en œuvre, consiste à analyser la conception de la puce à l'aide de procédés invasifs (abrasion, gravure chimique, laser, SEM, etc.)

Détectez ensuite le signal par lequel passent les informations secrètes (notamment en raison du faisceau d'ions focalisé). Face à l'ensemble de ses attaques des protections qui ont été proposées ces dernières années pour contrer celle-ci. Deux types de protections sont principalement mis en œuvre aux attaques par injection de faute. La première consiste à détecter les tentatives d'injection de pannes, puis à appliquer une stratégie de réponse appropriée lorsqu'une attaque se produit.

Pour cette raison, des capteurs et des mécanismes de détection d'erreur pour détecter les changements anormaux dans l'environnement du circuit, Les réactions communément proposée va de la simple coupure de la communication à l'effacement complet des informations stockées dans la mémoire. Le deuxième type de protection vise à augmenter la robustesse du circuit aux différentes attaques. À cette fin, des méthodes de correction des erreurs (également basées sur la redondance) et des équipements techniques tels que des couvercles métalliques et des filtres sont utilisés.

Les contre-mesures proposées pour contrer les attaques par canaux cachés. Il s'agit soit d'ajouter du bruit sur les canaux soit de réduire le signal informatif. Enfin viens, les contre mesure matérielles avec plusieurs solutions proposer pour éviter la réalisation d'attaques