**Nous énumérons les problèmes de sécurité sans rentrer dans les détails qui dépassent le cadre de ce cours de découverte.**

**CARTES ET SECURITE**

* Sécurité
 Objectifs du fraudeur :
 Obtenir l’accès à une information
 Corrompre des informations
 Réfuter l’envoi ou la réception d’une information
 Provoquer la méfiance vis à vis d’un système
 Attaques :
 Se faire passer pour quelqu’un d’autre
 Empêcher le fonctionnement correct d’un système
 Corrompre un protocole pour obtenir des secrets
 S’insérer dans le système comme relais actif
* **Sécurité intrinsèque de la carte**
* Attaques
 Lecture au microscope électronique
 Insertion de sondes
 Provoquer des dysfonctionnements
 Mécanismes
 Détecteurs de lumière, de passivation, de température, de tension, de fréquence
 Couche de passivation, bus enterré (inaccessible de l’extérieur)
 Brouillage des adresses
 Logique sauvage des circuits
 Mode test - protection par fusibles
 Matrice de sécurité physique (RAM, ROM, EEPROM)
* **Conclusion Sécurité Physique**
 La sécurité physique esta assurée en partie par les facteurs suivants :
 Le micromodule est monolithique
 difficile de distinguer ses différents composants
 Présence d'un bloc de sécurité
 détection de tension
 détection de fréquence
 détection de lumière
 Le système d'exploitation est en ROM et ne peut donc être ni remplacé, ni altéré
* La sécurité logique

 L'Identification
-L'Authentification
-LaCertification
-L'Intégrité
- La Confidentialité

## Quelques eclaircissements sur Les attaques physiques

Dans la conception traditionnelle de la *cryptologie*, la s´ecurit´e est vue de mani`ere abstraite : pour attaquer un cryptosyst`eme, l’attaquant se borne `a echanger des messages avec celui-ci, et esp`ere en les utilisant pouvoir mettre en d´efaut les objectifs vis´es (confidentialit´e, int´egrit´e, authenticit´e, ...) par diff´erentes techniques de *cryptanalyse*. La *cryptographie* classique s’efforce donc de construire des sch´emas avec si possible des preuves relatives de s´ecurit´e contre ce type d’attaque, en admettant la difficult´e de certains probl`emes math´ematiques au sens de la *th´eorie de la complexit´e*.

Dans un mod`ele de s´ecurit´e plus ´etendu, on tient compte ´egalement, depuis quelques ann´ees, des *attaques physiques*. Ce nouveau concept prend en consid´eration non seulement la s´ecurit´e des cryptosyst`emes au sens *math´ematique*, mais aussi les aspects li´es `a la nature *physique* des calculs. Ces attaques nouvelles sont particuli`erement mena¸cantes pour les *syst`emes embarqu´es* tels que les *cartes `a microprocesseur*, contre lesquels l’adversaire peut mobiliser des moyens d’analyse de plus en plus sophistiqu´es.

Dans ce domaine, de nombreux travaux ont ´et´e effectu´es soit pour mettre en ´evidence de nouvelles strat´egies d’attaques physiques, soit pour proposer des *contre-mesures*, avec dans certains cas des *preuves de s´ecurit´e* en ´etablissant un mod`ele convenable de l’adversaire.

Dans tout ce paragraphe, les attaques physiques sont consid´er´ees en tant que menaces sur la s´ecurit´e des protocoles et algorithmes cryptographiques dans les cartes `a microprocesseur. N´eanmoins, tous les syst`emes embarqu´es utilisant la cryptographie en sont aussi potentiellement la cible.

### Aperçu et Classification des attaques physiques

Afin d’´evaluer le niveau de r´esistance de ses produits, IBM a propos´e en 1991 une taxonomie des attaquants potentiels [1] :

Les “amateurs ´eclair´es” (classe I) : ils sont souvent tr`es intelligents, mais ont une connaissance imparfaite du systeme. Ils ont acces uniquement `a du materiel de sophistication

*•*

moyenne. Ils essaient souvent de tirer avantage de faiblesses existantes du syst`eme, plutˆot que d’en cr´eer de nouvelles.

Les “attaquants experts” (classe II) : ils ont re¸cu une solide formation technique et ont de l’exp´erience. Ils ont une compr´ehension variable des parties du syst`eme, mais ont un acc`es potentiel `a toutes ces parties. Ils poss`edent souvent des outils et des instruments d’analyse hautement sophistiqu´es.

*•*

Les “organisations financ´ees” (classe III) : elles sont capables de rassembler des ´equipes de sp´ecialistes ayant des capacit´es compl´ementaires, soutenues par des financements importants. Elles sont capables d’analyser en profondeur le syst`eme, de mettre au point des attaques complexes, et d’utiliser les outils d’analyse les plus modernes. Des attaquants de la classe II peuvent faire partie de ces ´equipes.

*•*

De mˆeme, on a pris l’habitude de classer les attaques physiques selon deux crit`eres : les attaques *invasives* ou *non-invasives*, et les attaques *actives* ou *passives*.

#### Attaques invasives ou non-invasives

Une attaque *invasive* n´ecessite la suppression de l’enveloppe du micro-module, afin de pouvoir acc´eder directement `a sa structure interne. Un exemple typique consiste `a brancher une d´erivation sur un *bus de donn´ees* afin d’intercepter les transferts de donn´ees.

Au contraire, dans une attaque *non-invasive*, l’adversaire n’utilise que les informations disponibles `a l’ext´erieur du syst`eme, comme les temps d’ex´ecution, la puissance ´electrique consomm´ee, le rayonnement ´electromagn´etique, *etc*.

On parle aussi parfois d’attaque *semi-invasive* [104], lorsque l’attaquant enl`eve l’enveloppe de la puce pour acc´eder `a sa surface, mais garde intacte la couche de protection du micro- module (ces attaques ne n´ecessitant pas l’´etablissement d’un contact ´electrique avec la surface de m´etal).

Les cartes `a microprocesseur sont munies de m´ecanismes de protection pour contrecarrer les attaques invasives. La technologie actuelle utilis´ee met ainsi en jeu (entre autres) plusieurs couches m´etalliques de protection, des d´etecteurs d’intrusion, ou encore un stockage des donn´ees sous des formats particuliers qui rendent tr`es difficile leur interpr´etation. En revanche, les attaques non-invasives sont par d´efinition ind´etectables. Comme elles sont en g´en´eral ´egalement les moins on´ereuses, ce sont elles qui constituent le principal danger pour la s´ecurit´e des cartes `a puce.

#### Attaques actives ou passives

Dans une attaque *active*, on tente de perturber le fonctionnement normal du syst`eme. Ainsi les attaques par *injection de fautes* ont pour objectif de provoquer des erreurs au cours de certains calculs effectu´es par le syst`eme .

Une attaque active implique une modification de l’environnement physique de la carte pour la placer dans des conditions anormales de fonctionnement. Plusieurs moyens sont `a la disposition de l’attaquant7 :

L’*alimentation* : selon le standard ISO/IEC 7816-2 [53], le micro-module doit pouvoir supporter une tension d’alimentation *Vcc* comprise entre 4,25 et 5,25 volts. Pour ces valeurs, la carte doit fonctionner normalement. En revanche, si une variation brusque de l’alimentation (appel´ee *spike*) fait sortir *Vcc* de l’intervalle de tol´erance, cela peut provoquer un r´esultat faux, `a supposer que la carte soit capable de finir compl`etement le calcul.

*•*

L’*horloge* : de fa¸con analogue, le standard ISO/IEC 7816-2 d´efinit une fr´equence de r´ef´erence pour l’horloge externe ainsi qu’un intervalle de tol´erance. L’utilisation d’une fr´equence anormalement haute ou basse peut ´egalement r´esulter en des erreurs8.

*•*

La *temp´erature* : placer la carte dans des conditions de temp´erature extrˆemes est un moyen potentiel de provoquer des fautes, mˆeme s’il est assez peu utilis´e aujourd’hui dans la pratique.

*•*

Les *rayonnements* : le folklore pr´esente souvent les attaques par injection de faute comme les “attaques au micro-ondes” (l’attaquant pla¸cant la carte `a puce dans un four

*•*

`a micro-ondes pour lui faire calculer des r´esultats erron´es). Au del`a de cette vision un peu caricaturale, il est reconnu que des rayonnements correctement dirig´es peuvent influencer le comportement de la carte.

La *lumi`ere* : Skorobogatov et Anderson [104] ont r´ecemment observ´e que l’illumination d’un transistor peut le faire basculer temporairement dans son ´etat conducteur, provoquant ainsi une erreur. En appliquant une source de lumi`ere intense (produite par une lampe flash d’appareil photographique, amplifi´ee par un microscope), ils ont pu changer la valeur de bits individuels dans une m´emoire SRAM (*Static* RAM). Par la mˆeme technique, ils ont pu ´egalement interf´erer avec les instructions jump, perturbant ainsi des sauts conditionnels.

*•*

Les *courants de Foucault* (*Eddy currents*) : Quisquater et Samyde [88] ont ´egalement montr´e r´ecemment que les courants de Foucault induits par un champ magn´etique dans une bobine peuvent produire par exemple provoquer des erreurs dans une cellule de m´emoire (qu’elle soit de type RAM, EPROM, EEPROM ou Flash).

*•*

A` l’inverse, dans une attaque *passive*, l’adversaire se contente d’observer le comportement de la carte dans son fonctionnement normal. L`a encore, plusieurs types d’informations de nature physique sont potentiellement utilisables par l’attaquant :

Le *temps d’ex´ecution* : le temps pris par un syst`eme pour ex´ecuter un algorithme est parfois variable. Cela peut ˆetre duˆ `a certaines instructions dont le temps d’ex´ecution

*•*

d´epend des donn´ees, ou bien `a des optimisations du compilateur, ou encore `a l’existence de plusieurs branches dans l’algorithme. L’id´ee des *attaques temporelles* (*timing attacks* qui en d´ecoulent a ´et´e publi´ee par Paul Kocher en 1996 [61], avant d’ˆetre appliqu´ee `a de nombreux cryptosyst`emes tels que DES [50], AES [95], RSA [31, 94] ou les sch´emas

`a base de courbes elliptiques [66, 65, 77].

La *consommation ´electrique* : la plupart des micro-modules actuels s’appuient sur une logique CMOS (*Complementary Metal-Oxyde Semiconductor*), dont on peut car- act´eriser la consommation ainsi : `a chaque coup d’horloge, les portes logiques changent d’´etat simultan´ement, provoquant le chargement ou le d´echargement des capacit´es in- ternes, ce qui se traduit par une variation de l’intensit´e du courant, mesurable de l’ext´erieur. En pratique, l’attaquant utilise soit une carte d’acquisition de donn´ees, soit un oscilloscope num´erique pour collecter les donn´ees. L’intensit´e du courant peut

*•*

ˆetre mesur´ee soit directement avec une sonde, soit en branchant une r´esistance en s´erie avec la masse ou l’entr´ee de l’alimentation de la carte.

Le *rayonnement ´electromagn´etique* : le chargement et le d´echargement des capacit´es des portes logiques a ´egalement pour cons´equence la cr´eation d’un champ ´electromagn´etique. On distingue les ´emanations directes, dues au courant qui circule lors de l’ex´ecution de l’algorithme, et les ´emanations indirectes, provoqu´ees par des effets de couplage entre des composants tr`es proches9. Des mises en œuvre concr`etes d’attaques ´electromagn´etiques sont d´ecrites dans [37, 87, 2].

*•*

### Attaques par injection de fautes

Si les *timing attacks* sont les attaques passives les plus faciles `a mettre en œuvre10, c’est en essayant de provoquer des erreurs de calcul que l’on obtient les attaques actives les plus simples `a mener (et les moins couˆteuses). Ces attaques constituent d’ailleurs une menace non seulement pour les algorithmes cryptographiques, mais aussi pour d’autres composantes logicielles, comme les *machines virtuelles* Java11, ou plus globalement le *syst`eme d’exploitation* dans son ensemble, pour lequel L. Goubin a r´ecemment propos´e une m´ethode g´en´erique de protection semi-automatique avec M.-L. Akkar et O. Ly [4].

En ce qui concerne les cryptosyst`emes, c’est en septembre 1996 que trois chercheurs de Bellcore, Boneh, DeMillo et Lipton proposent un nouveau mod`ele d’attaque physique sur les cartes `a microprocesseur, qu’ils baptisent “cryptanalysis in the presence of hardware faults” [15, 16, 17]. Ce mod`ele d’attaque est dirigé contre plusieurs algorithmes cryptographiques `a cl´e publique : le sch´ema de signature RSA et les sch´emas d’authentification de Fiat-Shamir ou de Schnorr.

Dans le cas de la signature RSA, les auteurs montrent que :

si l’impl´ementation utilise le th´eor`eme des restes chinois (CRT), une signature erron´ee et la signature correcte correspondante suffisent `a factoriser le module ;

*•*

si l’impl´ementation n’utilise pas les restes chinois, l’attaque peut fonctionner avec un nombre de signature erron´ees de l’ordre du nombre de bits du module.

*•*

Tr`es peu de temps apr`es, Lenstra, puis Joye et Quisquater [64, 56] remarquent que, pour une impl´ementation du RSA avec CRT, il suffit d’avoir un message et une signature erron´ee de ce message pour retrouver la factorisation du modulo. Le cas du RSA, ainsi que des algorithmes de signature ElGamal, Schnorr et DSA, est ´egalement ´etudi´e dans [8, 57]. Pour RSA, des contre-mesures ont ´et´e propos´ees dans [101, 102, 110, 7].

Biham et Shamir s’int´eressent ensuite au cas des algorithmes cryptographiques `a cl´e secr`ete. Ils montrent [11], que l’algorithme DES est aussi potentiellement vuln´erable aux at- taques “`a la Bellcore”, qu’ils rebaptisent *Differential Fault Analysis* (DFA). Il faut pour cela r´eussir, pour 200 ex´ecutions de l’algorithme, `a perturber `a chaque fois un bit, et `a r´ecup´erer les 200 messages chiffr´es erron´es. Pour un mod`ele d’attaque l´eg`erement diff´erent, Anderson et Kuhn [5, 6] r´eduisent `a 10 le nombre de messages erron´es n´ecessaires pour retrouver la cl´e secr`ete du DES. Ils supposent que l’on peut perturber la carte de mani`ere `a ce qu’une instruction assembleur bien choisie ne soit pas ex´ecut´ee par le microprocesseur.

Tous les algorithmes cryptographiques sont potentiellement vuln´erables aux attaques par injection de fautes. Ainsi Biehl, Meyer, Mu¨ller [10] et Ciet, Joye [21] ont montr´e que les attaques du type *Differential Fault Analysis* peuvent ´egalement ˆetre efficaces contre les cryp- tosyst`emes `a base de courbes elliptiques. Le cas de l’AES a quant `a lui ´et´e ´etudi´e par Bl¨omer, Seifert [13], Giraud [38], Dusart, Letourneux, Vivolo [33] et Piret, Quisquater [84].

Par ailleurs, les attaques DFA ont ´et´e g´en´eralis´ees dans plusieurs directions. Ainsi Biham et Shamir [11] montrent que dans certains cas on peut retrouver la cl´e secr`ete, ceci mˆeme sans connaˆıtre la sp´ecification de l’algorithme impl´ement´e dans la carte. Paillier a poursuivi l’´etude de ce mod`ele d’attaque dans [82]. Par ailleurs Joye, Quisquater, Yen et Yung montrent que v´erifier la justesse du r´esultat des calculs cryptographiques n’est pas toujours suffisant [109], et que cela peut mˆeme parfois aider l’attaquant [58].

### Attaques par analyse de consommation ´electrique

Les attaques passives, d´efinies au paragraphe 2.2, pr´esentent l’avantage (pour l’attaquant) de ne pas perturber le fonctionnement du syst`eme. Certaines d’entre elles ont connu depuis quelques ann´ees un retentissement tout particulier. Il s’agit des attaques par *analyse de consommation ´electrique* (*power analysis* en anglais).

Dans [39], L. Goubin et J. Patarin ont ´etudi´e en d´etail les attaques utilisant le principe d’*analyse diff´erentielle de consommation* (*Differential Power Analysis* – ou DPA – en anglais).

#### Analyse ´el´ementaire de la consommation

On appelle g´en´eralement *trace* la courbe de consommation ´electrique (en fonction du temps) obtenue pour une ex´ecution d’un algorithme cryptographique. Le principe de l’*analyse*

*´el´ementaire de consommation* (*Simple Power Analysis* – ou SPA – en anglais) consiste `a

essayer d’obtenir des informations sur la cl´e secr`ete de l’algorithme `a partir d’une seule trace. Ceci n’est possible que si les variations de consommation ´electrique sont suffisamment im- portantes pour ˆetre d´ecel´ees visuellement de mani`ere directe. En outre, cela suppose qu’il y ait un lien simple et exploitable entre les informations observ´ees et la cl´e secr`ete elle-mˆeme. C’est pourquoi ce type d’attaque vise particuli`erement les impl´ementations qui utilisent des branchements d´ependant de la cl´e.

Pour mener `a bien une attaque SPA, on utilise souvent le fait que les valeurs de la con- sommation ´electrique sont fortement corr´el´ees au *poids de Hamming* des donn´ees manipul´ees par les instructions assembleur. Cette id´ee a ´et´e d´evelopp´ee par Biham et Shamir [12] pour le DES, par Mangard [67] pour l’AES, ou encore par Rao, Rohatgi et Scherzer [91] pour l’algorithme COMP128-1 [41, 19] utilis´e dans le standard GSM de t´el´ephonie mobile12. Par ailleurs Schramm, Wollinger et Paar ont r´ecemment montr´e que le principe de la SPA pou- vait ´egalement ˆetre utilis´e pour d´etecter des collisions internes, notamment dans l’algorithme DES : ce sont les *attaques par collision* (*collision attacks*) [97].

Les algorithmes asym´etriques sont aussi potentiellement vuln´erables face aux attaques de type SPA. En particulier pour les algorithmes (tels RSA) faisant intervenir l’*exponentiation* d’une valeur connue, par un exposant secret, un sc´enario d’attaque utilisant `a nouveau la notion de *poids de Hamming* est d´ecrit par Kl´ıma et Rosa dans [59]. De mˆeme, la *multipli- cation scalaire* d’un point connu d’une courbe elliptique, par un scalaire secret, donne lieu

`a des attaques : ainsi Oswald [81] utilise le *mod`ele de Markov* pour retrouver la cl´e dans le cas d’une impl´ementation avec des *chaˆınes d’addition-soustraction*. Clavier et Joye [22] ont

´etabli un mod`ele g´en´eral de ces attaques SPA, ouvrant la voie `a des protections g´en´eriques et prouv´ees suˆres pour ce type d’algorithmes asym´etriques.

#### Analyse diff´erentielle de la consommation

L’*analyse diff´erentielle de consommation* (*Differential Power Analysis* – ou DPA – en anglais) a ´et´e introduite par Kocher, Jaffe et Jun en 1998 [62] et publi´ee en 1999 [63]. L’id´ee est d’exploiter les *corr´elations* ´eventuelles entre les donn´ees manipul´ees par le microprocesseur et les valeurs instantan´ees de consommation ´electrique. Comme ces corr´elations sont sou- vent tr`es faibles, il faut avoir recours `a des m´ethodes *statistiques* pour en tirer le maximum d’information.

Dans une attaque de type DPA, le principe consiste `a comparer des valeurs mesur´ees lors du fonctionnement du *v´eritable* dispositif physique (par exemple la carte `a microprocesseur) avec des valeurs calcul´ees grˆace `a un mod`ele *hypoth´etique* de ce dispositif (les hypoth`eses portant notamment sur la nature de l’impl´ementation, et surtout sur une partie de la cl´e secr`ete). En comparant ces deux ensembles de valeurs, on s’efforce ensuite de retrouver tout ou partie de la cl´e secr`ete.