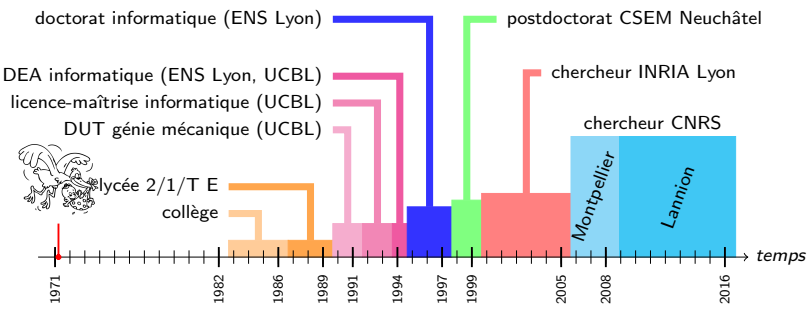
Cybersécurité: exemples d'attaques physiques et de protections de puces électroniques

Arnaud Tisserand

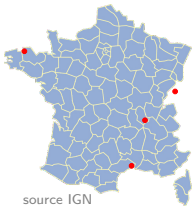
CNRS, IRISA, équipe-projet CAIRN

Immersion Science, mars 2016

Présentation personnelle



- Université Claude Bernard de Lyon
- École normale supérieure de Lyon
- Centre suisse d'électronique et microtechnique
- Institut national de recherche en informatique et automatique
- Centre national de la recherche scientifique



Centre national de la recherche scientifique

www.cnrs.fr

créé en 1939

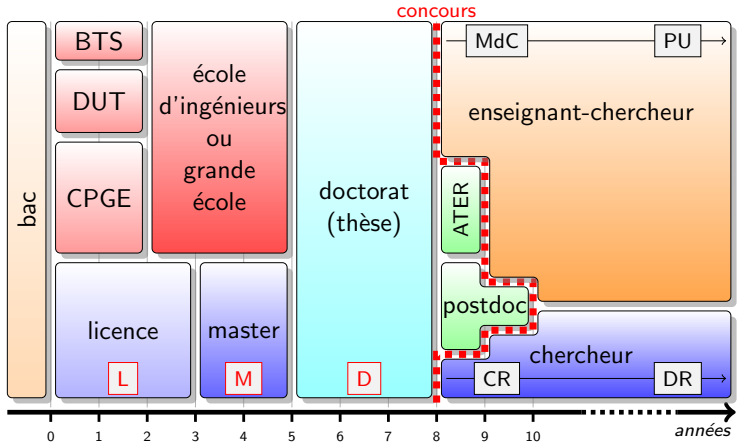
données de mars 2015

- organisme public de recherche (EPST)
- objectifs : *produire du savoir et mettre ce savoir au service de la société* (source : site web)
- personnels (approx.) :
  - 11 200 chercheurs
  - 13 750 ingénieurs, techniciens et administratifs
  - 8 000 agents non permanents (p. ex. doctorants)
  - 1 100+ laboratoires en France
  - coopération scientifique avec 60 pays
  - environ 700 entreprises créées depuis 2000
  - budget 2014 de 3.3×10^9 €

Domaines de recherche : biologie, chimie, écologie et environnement, sciences humaines et sociales, sciences de l'information et de leurs interactions, sciences de l'ingénierie et des systèmes, sciences mathématiques et de leurs interactions, physique, physique nucléaire et physique des particules, sciences de l'univers

Remarque : EPST = établissement public à caractère scientifique et technologique

Comment devenir (enseignant-)chercheur ?



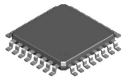
BTS : brevet de technicien supérieur
DUT : diplôme universitaire de technologie
CPGE : classe préparatoire aux grandes écoles
ATER : attaché temporaire d'enseignement et de recherche

MdC : maître de conférences
PU : professeur des universités
CR : chargé de recherche
DR : directeur de recherche

Quelques besoins en sécurité/cryptographie

Confidentialité **Intégrité** **Authenticité** **Non-répudiation**

circuit à bas coût
conception simple
haute sécurité



haute vitesse
basse énergie
faible taille/poids

Chiffrement **Signature Numérique** **Hachage** **Aléa** ...

Terminologie (1/3)

Cryptographie : étymologiquement « écriture secrète », méthodes et outils pour rendre les messages incompréhensibles sans avoir la clé

⇝ art du secret

Cryptanalyse : analyse des cryptogrammes pour retrouver les informations secrètes (clé ou message en clair)

Cryptologie : cryptographie + cryptanalyse

Stéganographie : cacher un message dans un autre message

⇝ art de la dissimulation

Terminologie (2/3)

Vulnérabilité : faiblesse/faille dans un système

Attaque : méthode pour exploiter une vulnérabilité

Menace :

- utilisateur étourdi/insouciant
- sinistre : vol, inondation, incendie...
- programme malveillant (virus, vers, trojan...)
- personnes/groupes malveillants
  - individu seul (p. ex. *hacker*)
  - société concurrente
  - gouvernement étranger

puissance d'attaque ↓

Protection ou contre-mesure : méthode ou dispositif qui contre une attaque ou qui supprime/limite une vulnérabilité

Terminologie (3/3)

Confidentialité : garantit que les données sont compréhensibles seulement par les personnes autorisées

⇝ les données semblent totalement aléatoires à toute autre personne

Authentification : garantit que l'origine des données est la bonne

⇝ authentification d'une source ou d'un tiers (identité)

Intégrité : garantit que les données ne sont pas altérées

⇝ les données sont complètes et sans aucune modification

Non répudiation : garantit qu'une action ne peut être niée

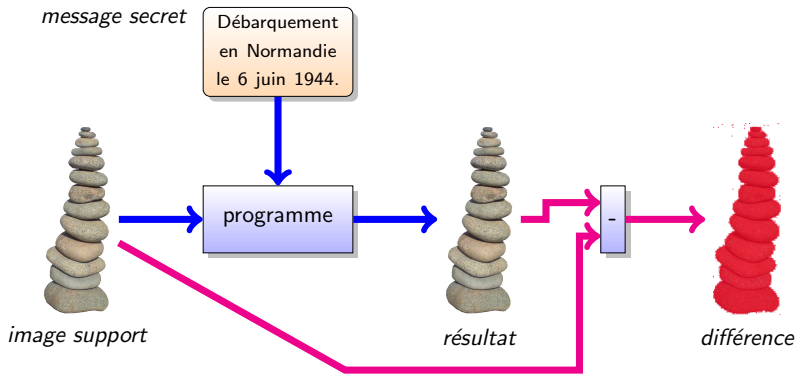
⇝ impossibilité de se dédire

Autres caractéristiques souvent utilisées : disponibilité, identification, contrôle d'accès...

Stéganographie

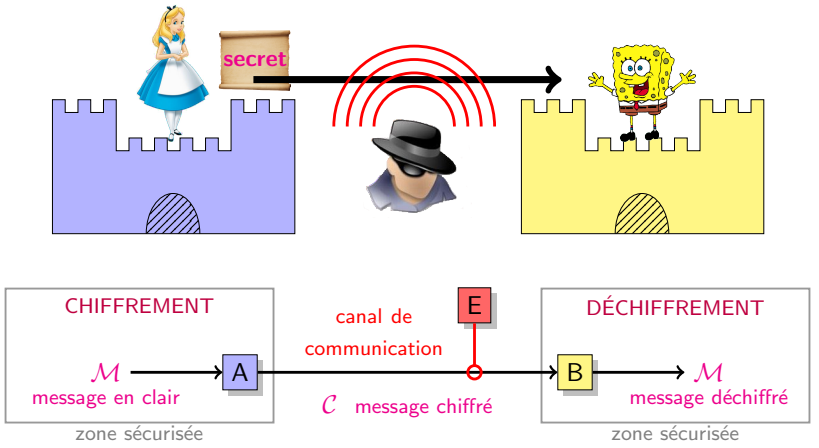
Cryptographie : art du secret
Stéganographie : art de la dissimulation

Principe : cacher un message (secret) dans un autre message (support)



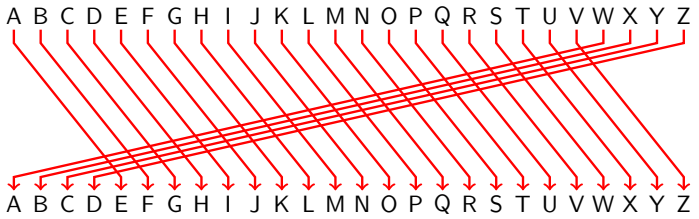
Cadre cryptographique : transmission d'un message secret

Alice souhaite envoyer un message secret à Bob sans que l'espion puisse avoir des informations sur ce message



Méthode de chiffrement très simple (mais peu fiable)

Idée : remplacer les lettres de l'alphabet par une version décalée de l'alphabet (chiffre de César)

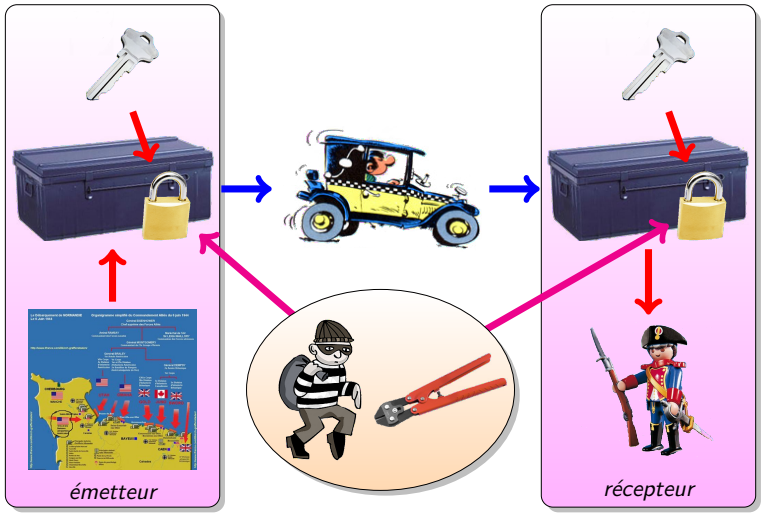


La clé secrète est la valeur du décalage

Exemple :

I	M	M	E	R	S	I	O	N		S	C	I	E	N	C	E	S
↓	↓	↓	↓	↓	↓	↓	↓	↓		↓	↓	↓	↓	↓	↓	↓	↓
M	Q	Q	I	V	W	M	S	R		W	G	M	I	R	G	I	W

Analogie avec un coffre et un cadenas



Attaques par force brute

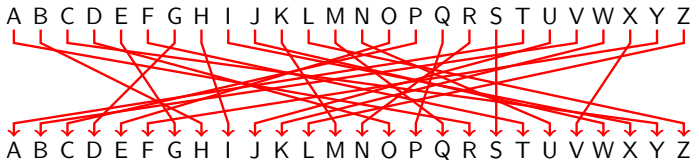
Principe : tester toutes les clés possibles

Limite : possible que si le nombre de clés possibles est raisonnable

Exemple du chiffrement par décalage de l'alphabet :

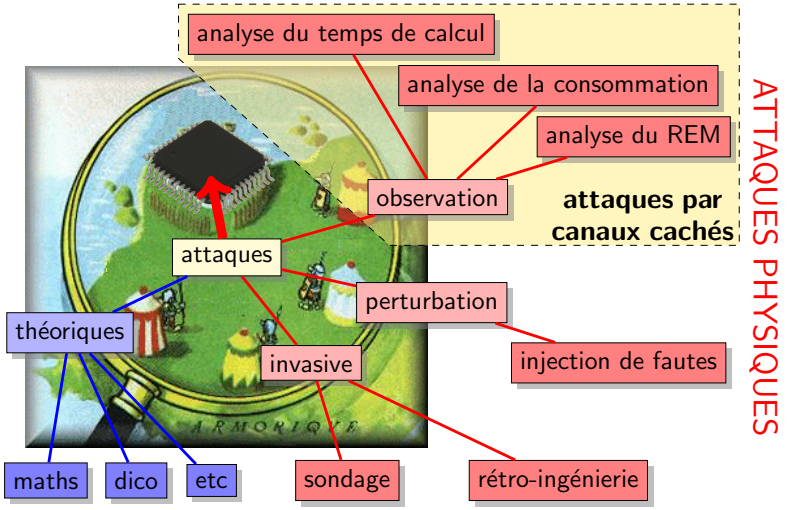
seulement 26 clés possibles

Exemple du chiffrement par permutation des lettres de l'alphabet :



$403\,291\,461\,126\,605\,635\,584\,000\,000 \approx 4.03 \times 10^{26}$ clés possibles

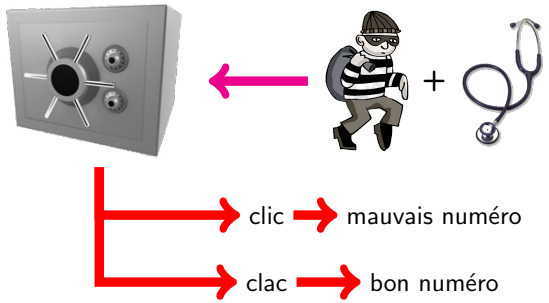
Principaux types d'attaques



REM = rayonnement électromagnétique

Attaques par canaux cachés, une nouvelle technique ?

Pas vraiment ! Vous connaissez tous des attaques par canaux cachés...



Quelles grandeurs physiques mesurer ?

Réponse : tout ce qui ≪ entre ≫ ou ≪ sort ≫ dans le ou du circuit

- temps de calcul
- consommation d'énergie (c.-à-d. courant électrique)
- rayonnement électromagnétique
- température
- bruit
- nombre de défauts de cache d'un ordinateur
- nombre et type des messages d'erreur
- ...

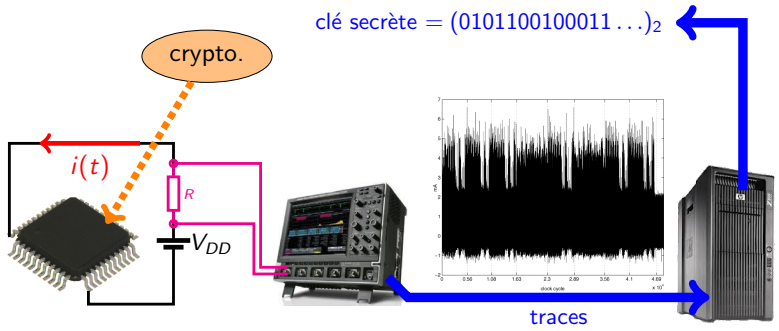
Les valeurs mesurées peuvent révéler des informations sur :

- le comportement global (conso., REM, température, bruit ...)
- le comportement local (REM local, nb. déf. cache ...)

Attaque par analyse de la consommation d'énergie

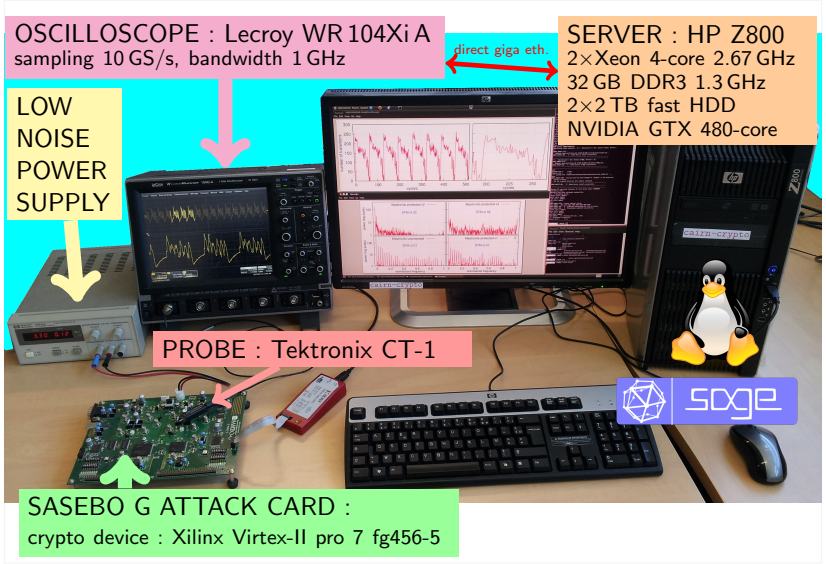
Principe général :

1. mesure du courant $i(t)$ dans le circuit (ou le crypto-système)
2. utiliser ces mesures pour « déduire » des informations secrètes

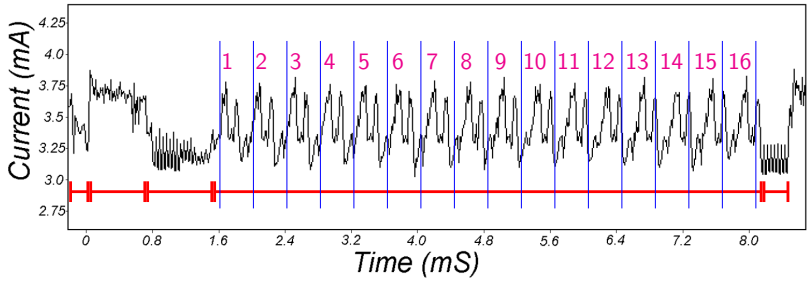


V_{DD} est la tension d'alimentation du circuit

Notre banc d'attaque par analyse de consommation



Que « *lire* » dans les traces ?

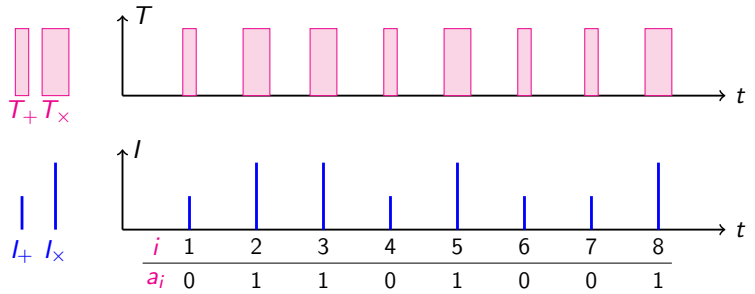


- algorithme $\Longrightarrow$ découpage en étapes
- détection des tours de boucle (calculs répétitifs)
  - temps constant dans un tour
  - ou pas ? ? ?

Exploiter les différences

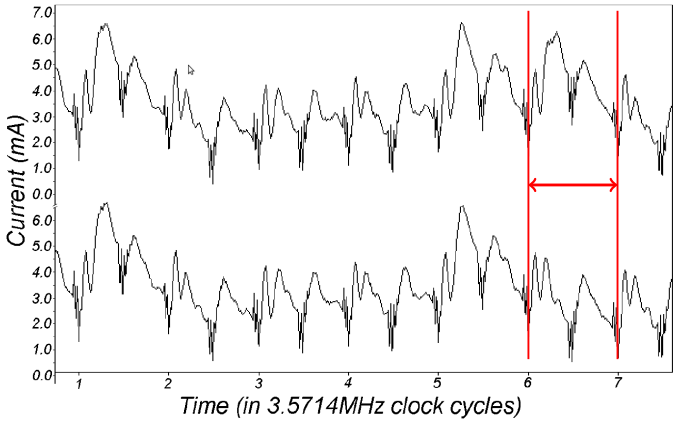
Un algorithme a une signature en courant et en temps de calcul :

```
r = c0
for i from 1 to n do
  if ai = 0 then
    r = r + c1
  else
    r = r × c2
```



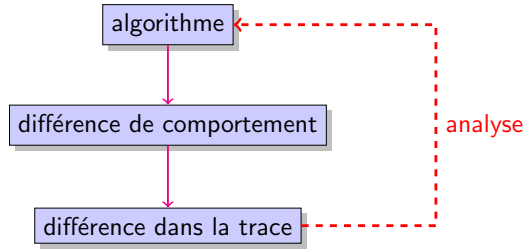
Analyse simple de la consommation (SPA)

En anglais : SPA *simple power analysis*



La SPA en pratique

Principe :

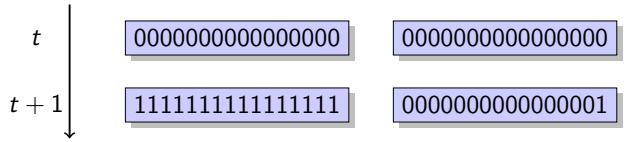


Techniques : exploiter les différences dans

- le contrôle
- le temps de calcul
- les valeurs des opérandes (temps de calcul, conso., REM...)
- ...

Limites de la SPA

Exemple de différence de comportement : (activité dans un registre)

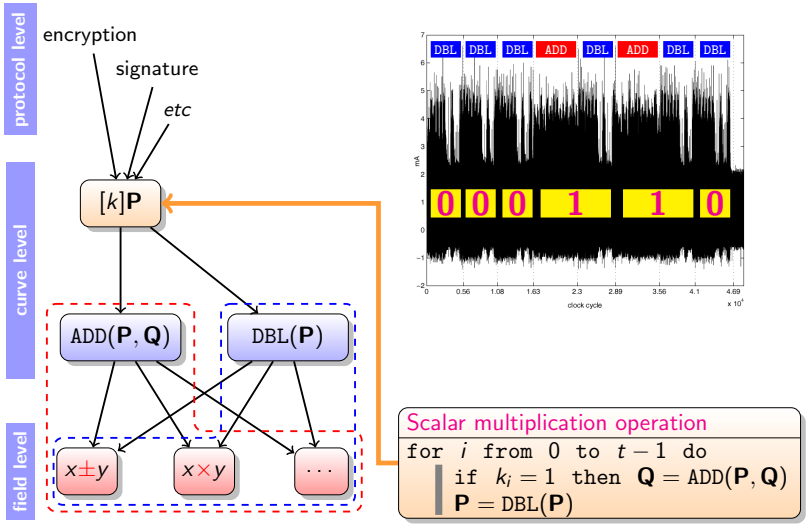


Important : une petite variation de comportement peut être plus ou moins cachée par du bruit $\Longrightarrow$ les traces ne sont plus discernables

Question : que faire quand les différences sont (trop) petites ?

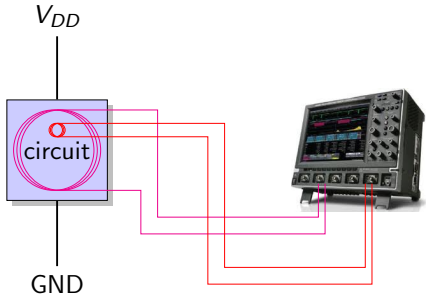
Réponse : utiliser des statistiques sur des nombreuses courbes

SPA Example on ECC (Elliptic Curve Cryptography)



Attaque par analyse du REM

Principe général : utiliser une sonde pour mesurer le REM



Mesures du REM :

- global avec une sonde large
- local avec une micro-sonde
- cartographie fine du circuit avec une table XY

Principales techniques de protection

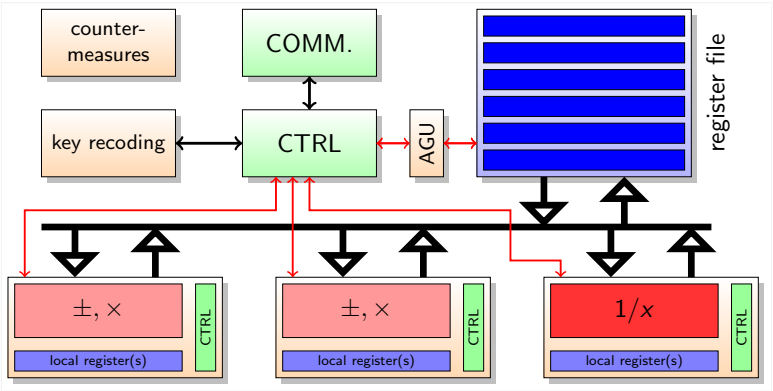
Empêcher une (ou des) attaques par :

- un nouveau dispositif de protection
- la modification/sécurisation du dispositif original

Exemples :

- blindage
- uniformiser les temps de calcul
- uniformiser la consommation d'énergie
- utiliser des codes détecteurs/correcteurs d'erreurs
- introduire du bruit (instructions inutiles)
- reconfigurer le circuit
  - changer le codage des données
  - changer les algorithmes

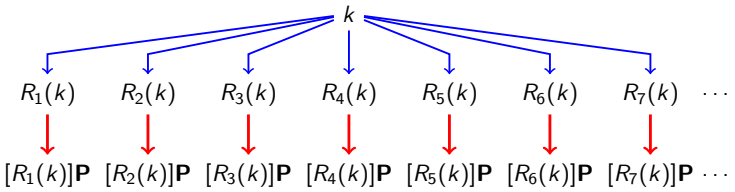
Notre crypto-processeur pour courbes elliptiques



Contre-mesure : recodage arithmétique des clés secrètes

Système redondant d'écriture des nombres =

- un moyen d'accélérer certains calculs
- un moyen de représenter une avec différentes représentations

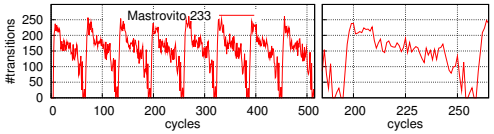


Propriété importante : $\forall i \quad [R_i(k)]\mathbf{P} = [k]\mathbf{P}$

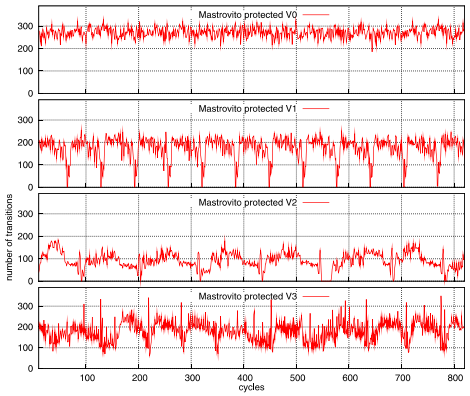
Notre solution : utiliser des représentations aléatoires de k

Contre-mesure : opérateurs arithmétiques sécurisés

Multiplier non protégé



Multiplieurs protégés



Conclusion & perspectives

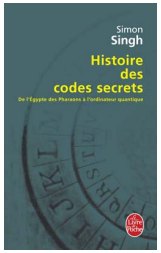
- Attaques de plus en plus performantes
- Sécurisation nécessaire à tous les niveaux (théorie, algorithmes, opérations, implantations, formation des utilisateurs, . . .)
- Sécurisation = compromis performances / robustesse
- Coût de sécurisation = *fonction*(valeur secret, type attaquant)
- Sécurité = mathématiques + informatique + micro-électronique + . . .

On estime qu'il faut environ 10 000 ingénieurs et techniciens formés dans les métiers de la cyber-sécurité en France pour les prochaines années !

La Bretagne est un acteur majeur du domaine avec le Pôle d'Excellence Cyber (PEC) aux niveaux industriel, recherche et formation.

Livres en français (1/2)

Histoire des codes secrets
Simon Singh
1999
Livre de poche



Mathématiques, espionnage et piratage informatique
Joan Gomez
2010
Le monde est mathématique, RBA

Livres en français (2/2)

Cryptographie appliquée
Bruce Schneier
1997, 2ème édition
Wiley
ISBN: 2–84180–036–9

Micro et nano-électronique
Bases, Composants, Circuits
Hervé Fanet
2006
Dunod
ISBN: 2–10–049141–5

Quelques références

- *Differential Power Analysis*. Paul Kocher, Joshua Jaffe, and Benjamin Jun. Whitepaper from Cryptography Research, Inc. `http://www.cryptography.com`
- *A Tutorial on Physical Security and Side-Channel Attacks*. François Koeune and François-Xavier Standaert. `http://www.dice.ucl.ac.be/crypto/`
- *The Sorcerer's Apprentice Guide to Fault Attacks*. Hagai Bar-El, Hamid Choukri, David Naccache, Michael Tunstall and Claire Whelan `http://citeseer.ist.psu.edu/old/694897.html`
- `http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html`
- `http://www.schneier.com/`

Fin, des questions ?

Contact:

- `mailto:arnaud.tisserand@irisa.fr`
- `http://people.irisa.fr/Arnaud.Tisserand/`
- Equipe-projet CAIRN `http://www.irisa.fr/cairn/`
- Laboratoire IRISA, CNRS–INRIA–Univ. Rennes 1
  6 rue Kerampont, CS 80518, F-22305 Lannion cedex, France

Merci

Niveau de sécurité

Nombre d'opérations à effectuer pour ≪ casser ≫ le système