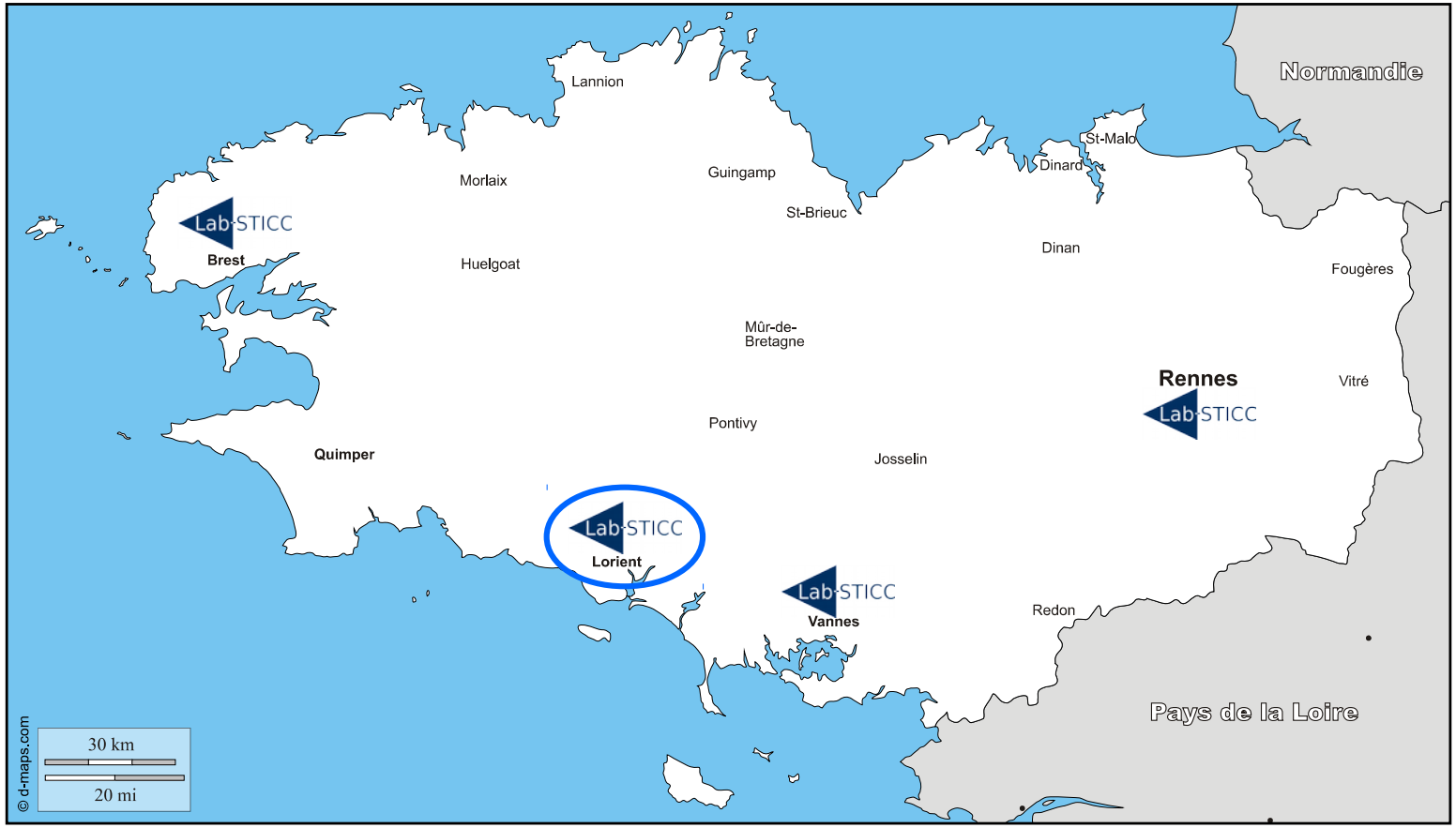
Les architectures matérielles au cœur de la sécurité

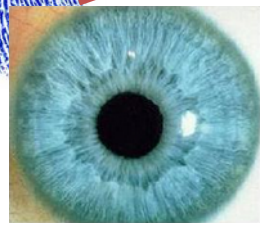
Vianney LAPOTRE
Maître de Conférences

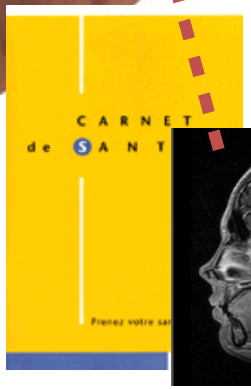
www.univ-ubs.fr
www.labsticc.fr

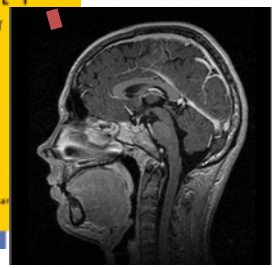
Le laboratoire Lab-STICC



Besoin de sécurité



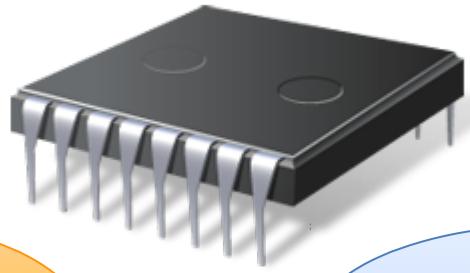




Le matériel en support

Sécurité

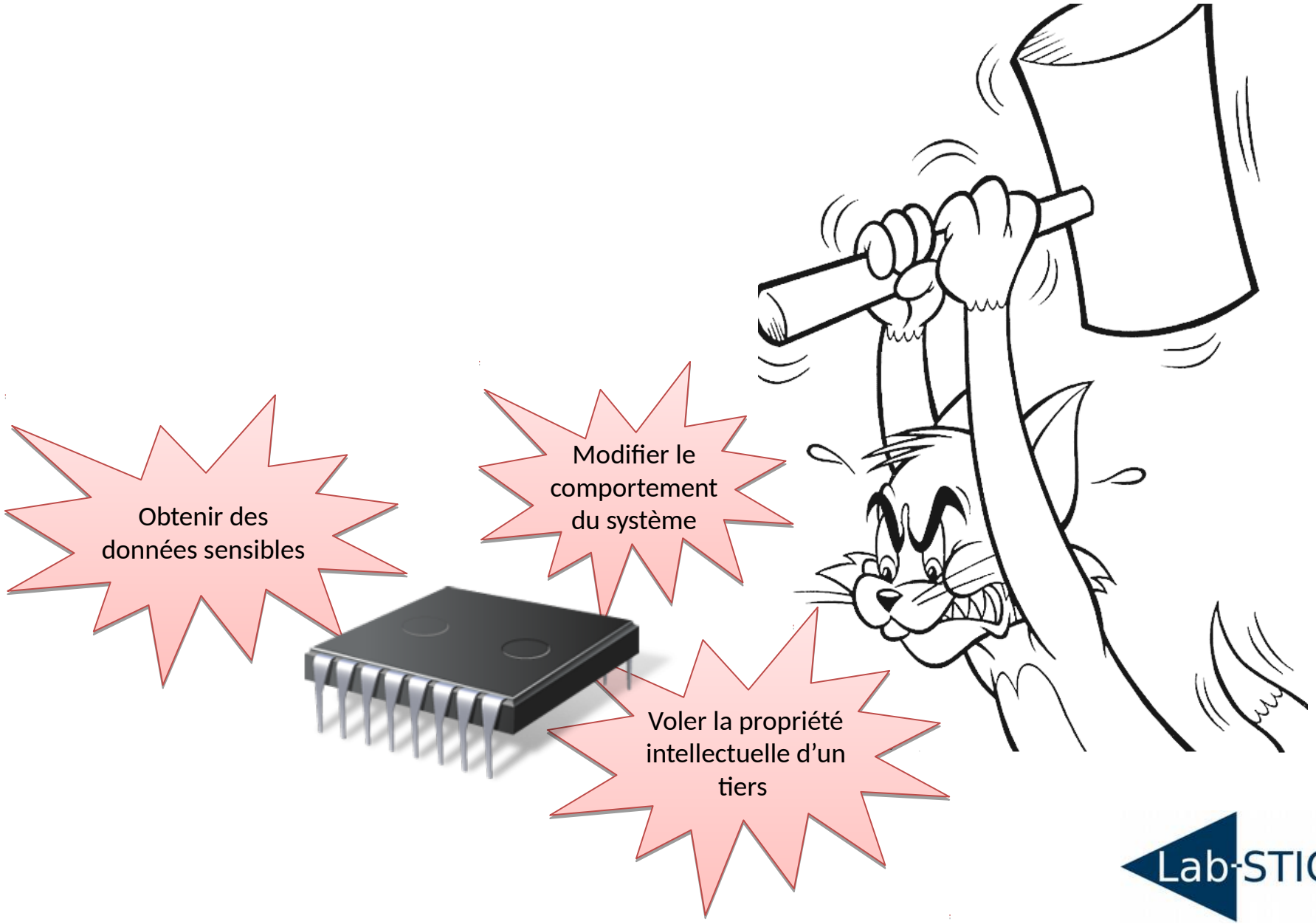
Applications



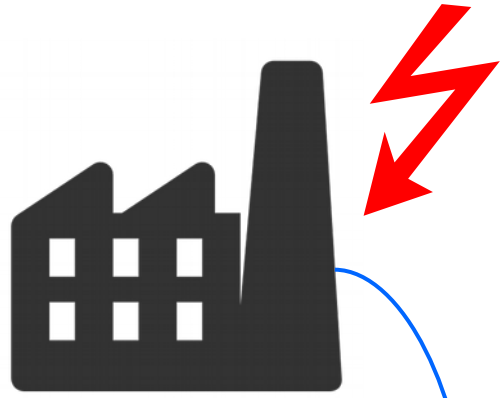
Performance

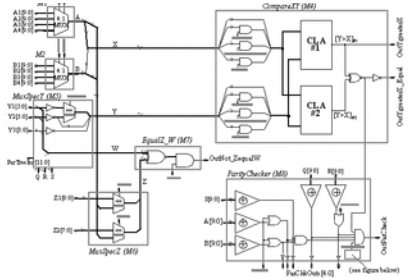
Diagnostic

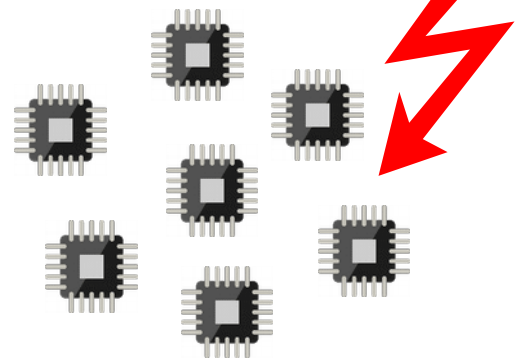
Cependant…


Obtenir des données sensibles
Modifier le comportement du système
Voler la propriété intellectuelle d'un tiers

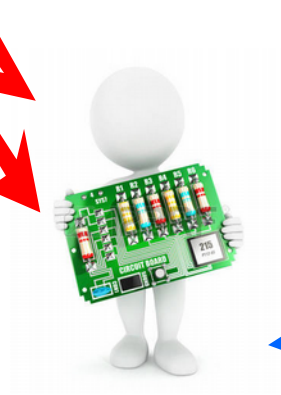
Les menaces liées au cycle de vie des circuits



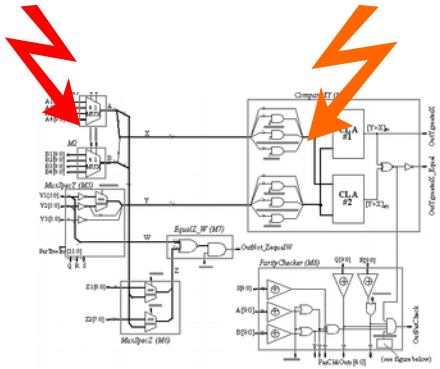




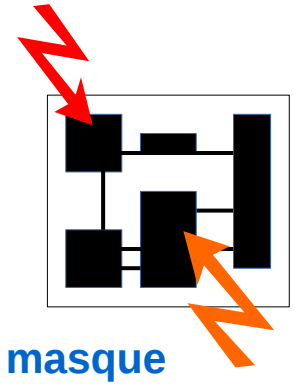
?



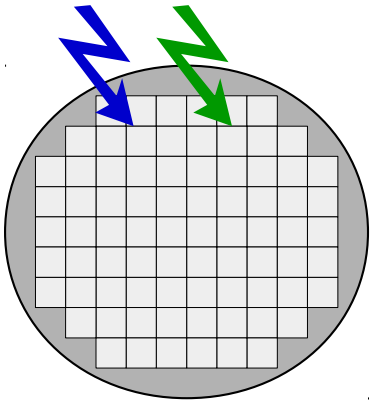
Les menaces liées au cycle de vie des circuits



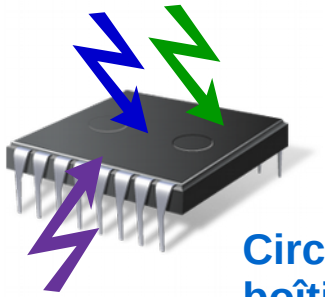
Netlist



masque



Wafer



Circuit en boîtier

Vol de propriété intellectuelle

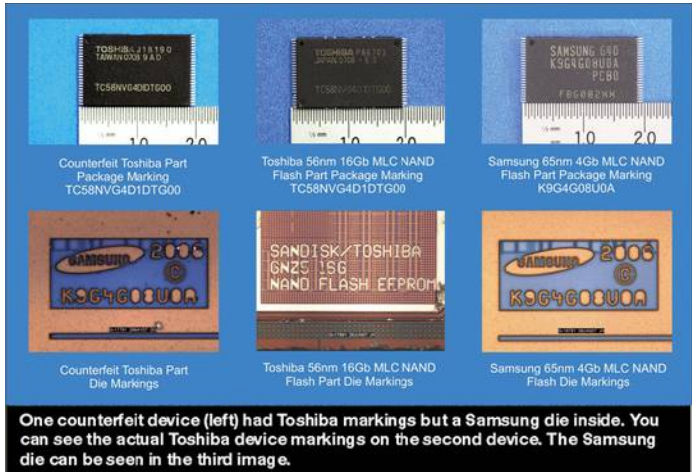
Surproduction

Tests non réalisés

Circuits non fonctionnels

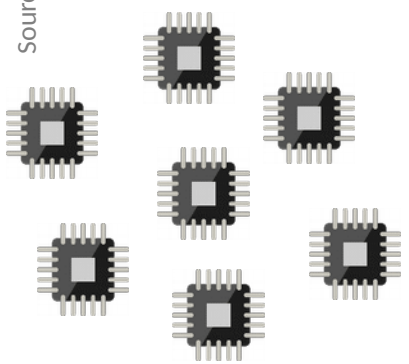
Modification des fonctionnalités

Les menaces liées au cycle de vie des circuits



Source : EE Times, August 2007

Changement de boîtier



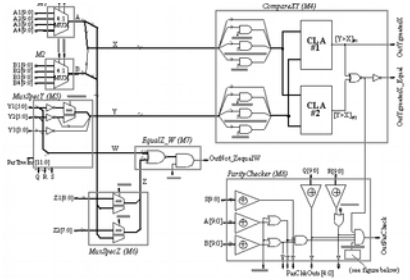
Circuit de distribution

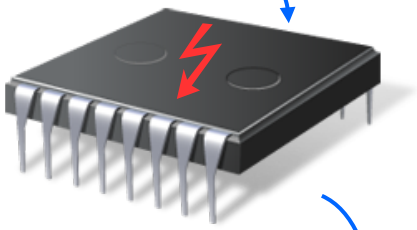
Re-marquage[1]

Recyclage de circuits intégrés

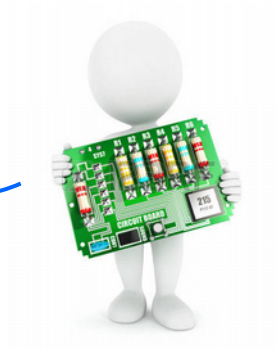
[1] Components Technology Institute. Counterfeit Examples, Electronic Components. http ://www.cti-us.com/pdf/CCAP-101InspectExamplesA6.pdf, 2013.

Les menaces liées au cycle de vie des circuits

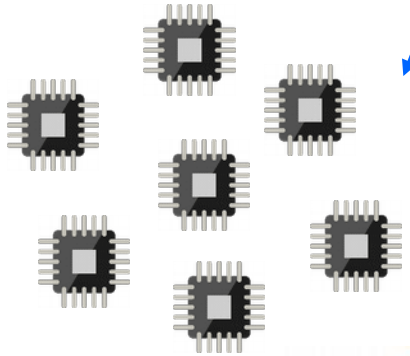




Retro-ingénierie

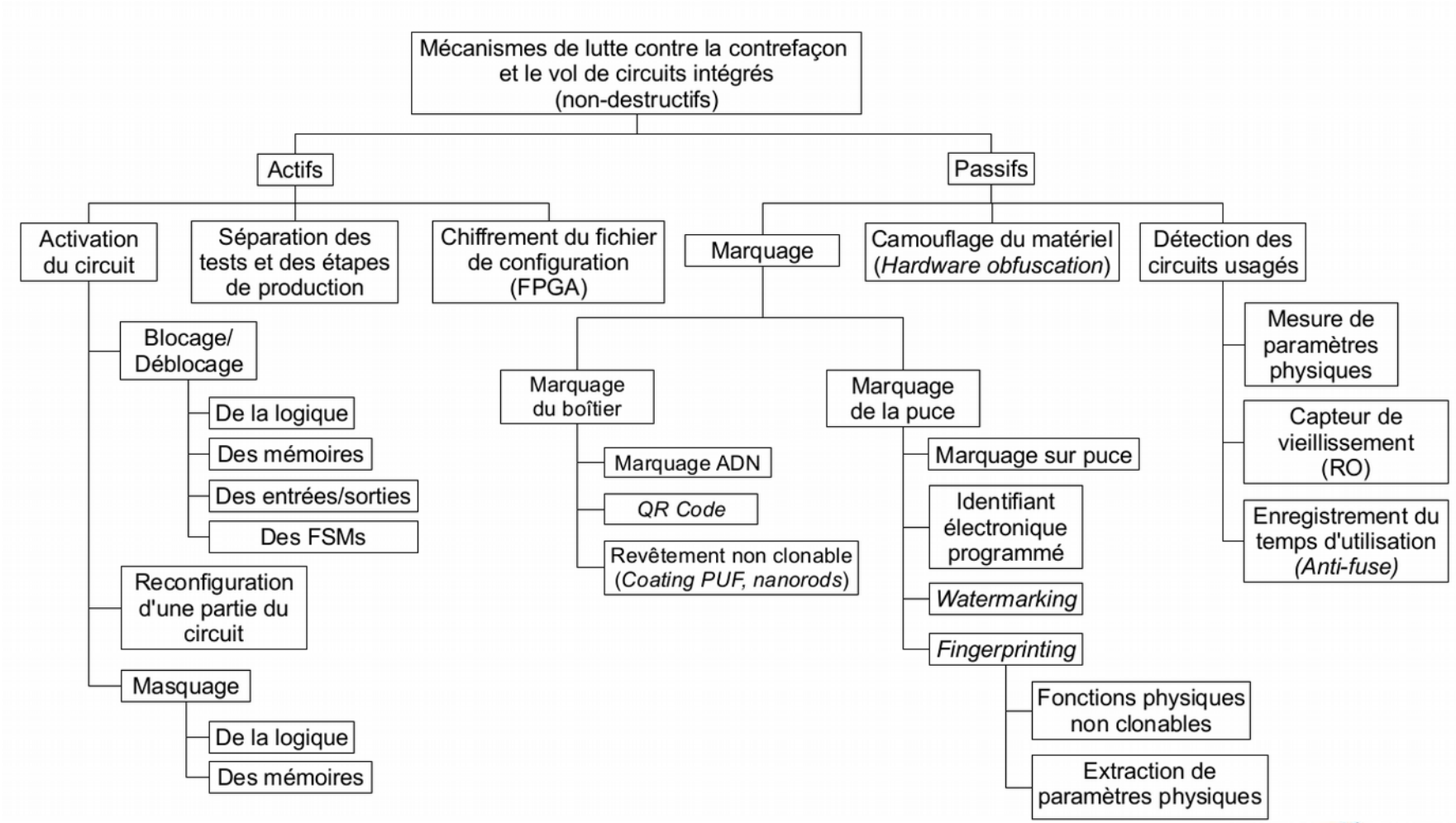


Concurrent



Circuit de distribution

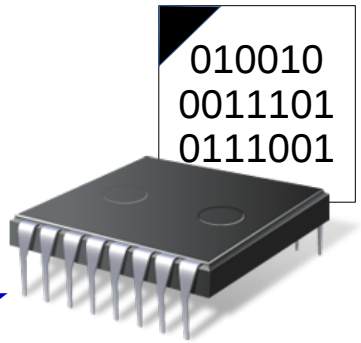
Mécanismes de protections



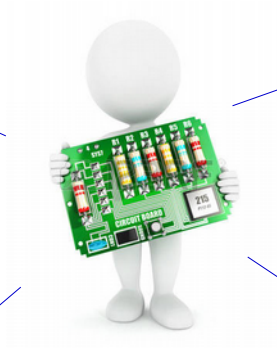
C. Marchand, "Conception de matériel salutaire pour lutter contre la contrefaçon et le vol de circuits intégrés". Thèse de doctorat, 2016

Les menaces liées au cycle de vie des circuits

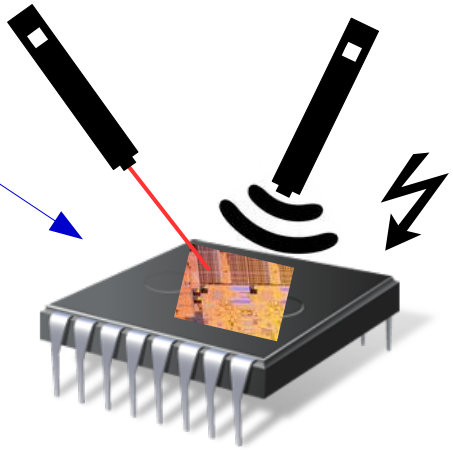
Retro-ingénierie



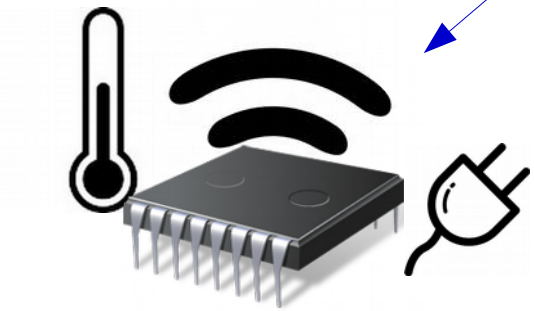
Logiciel malveillant



Attaquant



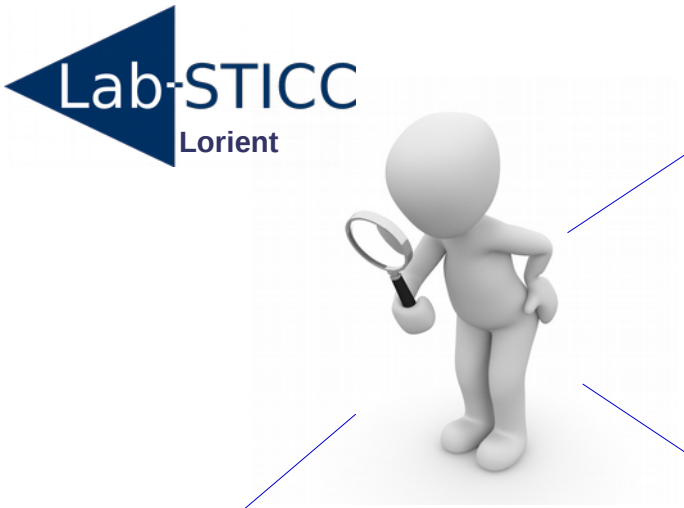
Attaques en faute

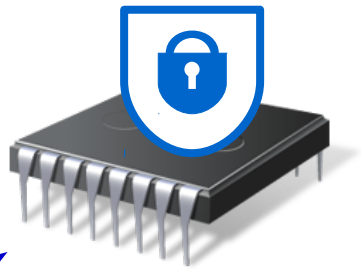


Attaques par canaux cachés

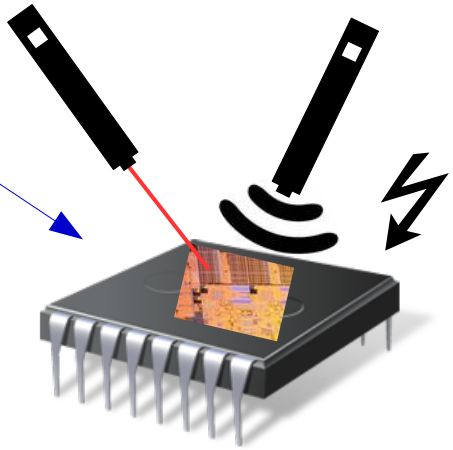
Lab-STICC

Nos travaux

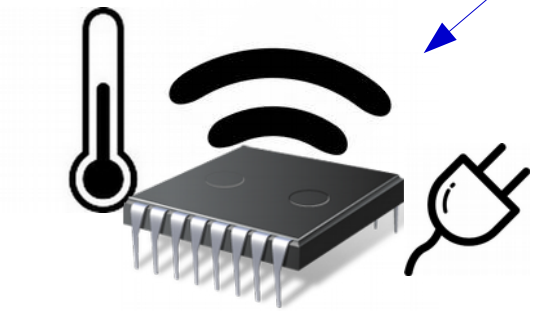




Conception de systèmes:
- **sécurisés**
- **pour la sécurité**

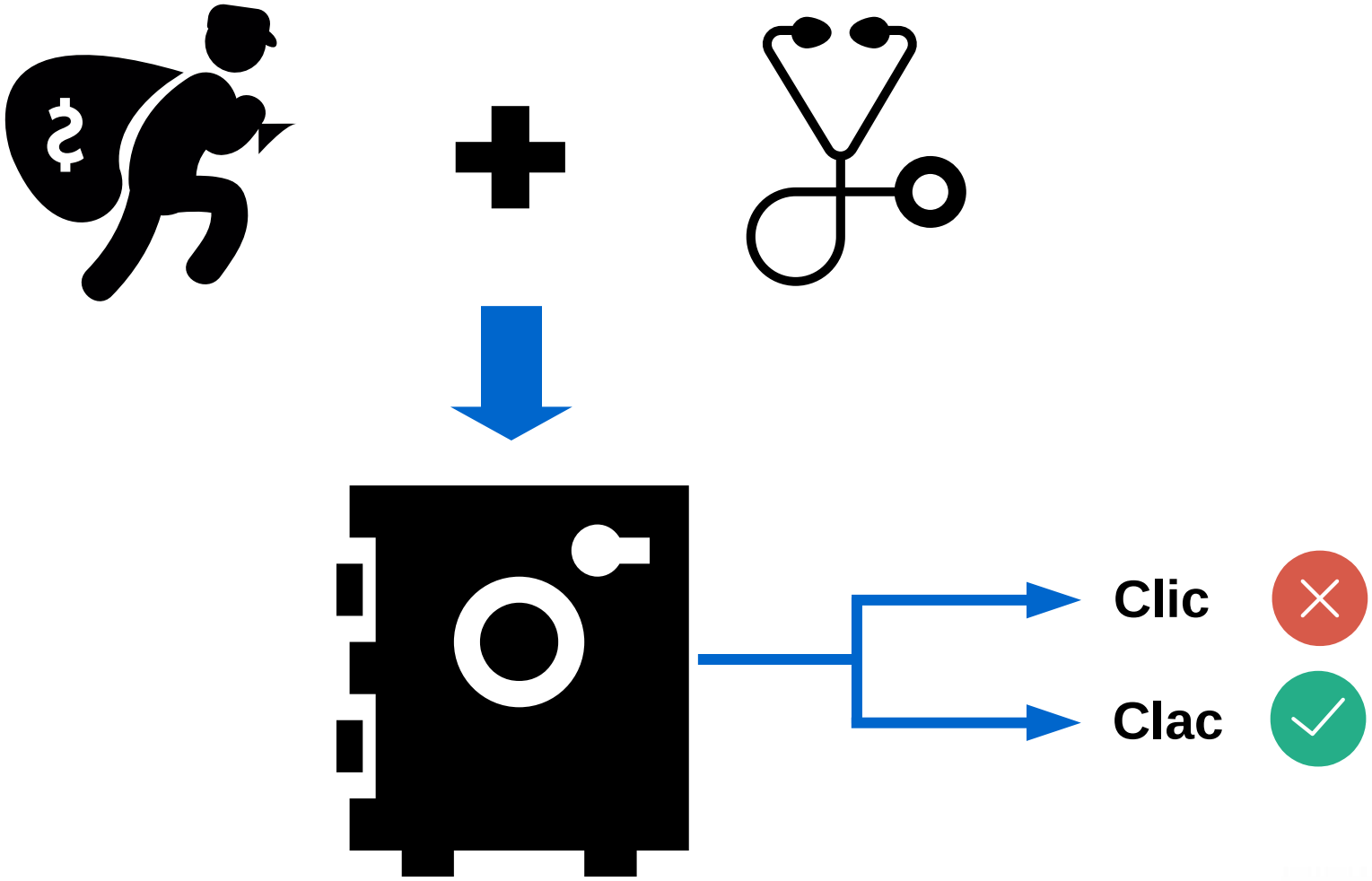


Attaques en faute



Attaques par canaux cachés

Les attaques par canaux cachés

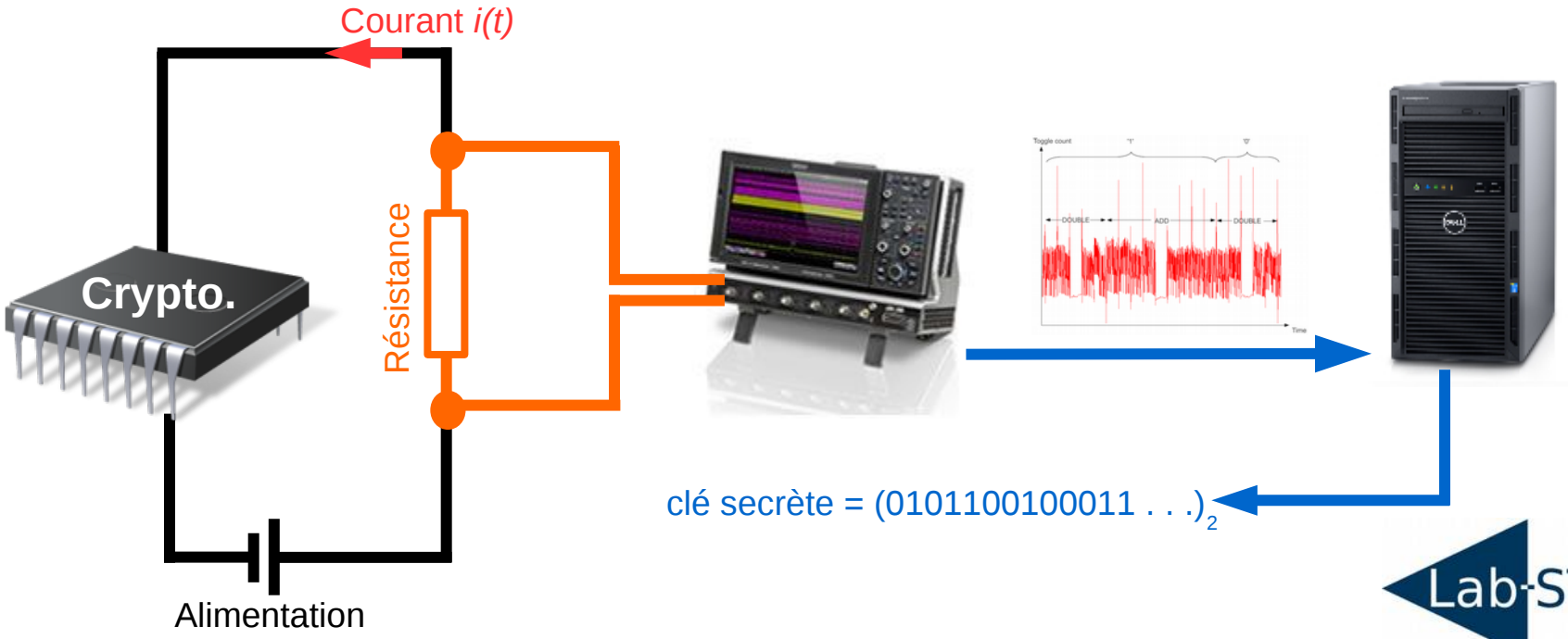


Les attaques par canaux cachés

- Les grandeurs physiques mesurées
  - Temps de calcul
  - Consommation d’énergie
  - Rayonnement électromagnétique
  - Température
  - Bruit
  - Nombre et type des messages d’erreur
  - Nombre de défauts de cache d’un ordinateur
  - ...

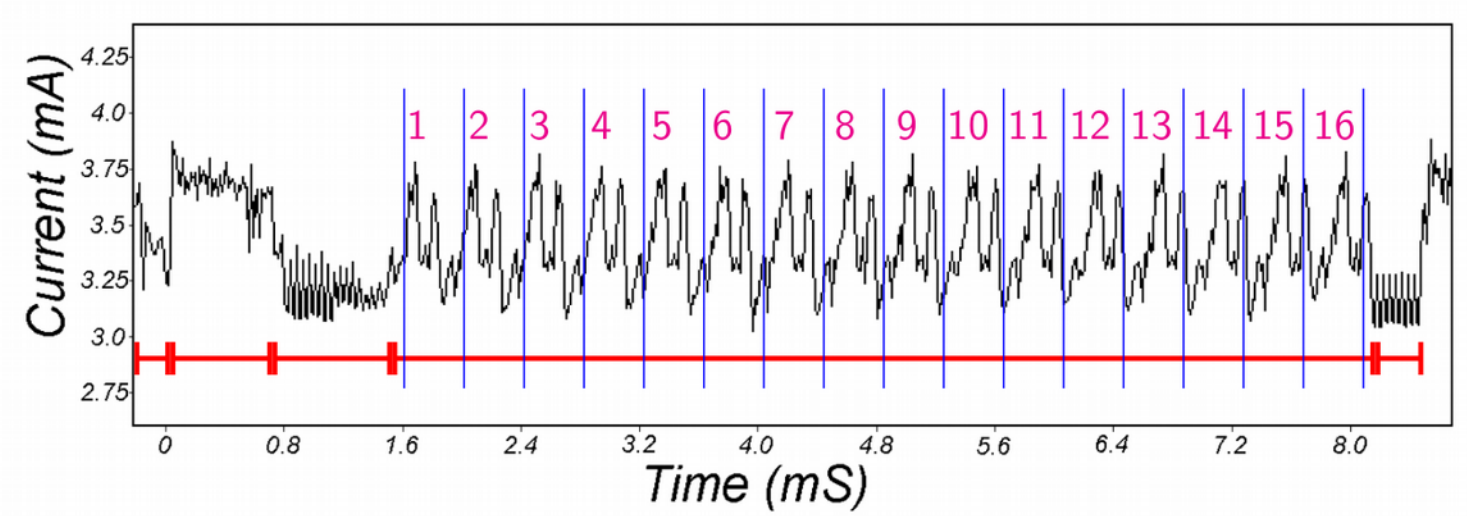
Les attaques par canaux cachés

- Attaque par analyse de consommation d'énergie
  - Mesurer le courant *i(t)* dans le circuit
  - Utiliser ces mesures pour *déduire* des informations secrètes



Attaque par analyse de consommation d'énergie

- Anatomie d'une trace
  - Étapes de l'algorithme analysé
  - Détection des tours de boucle (calculs répétitifs)
    - Temps constant dans un tour ?

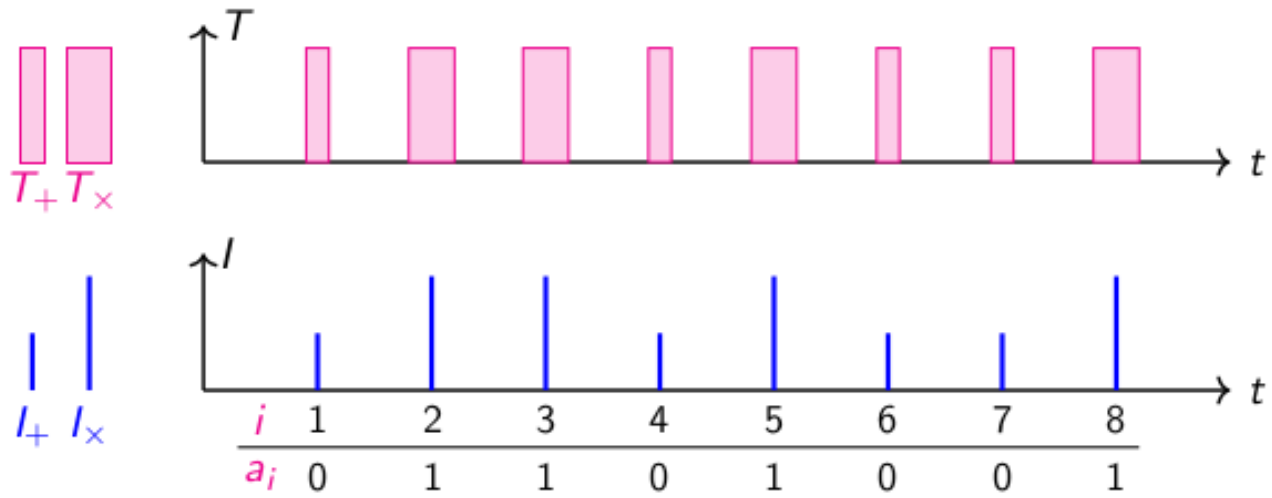


P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis," technical report, 1998; later published in Advances in Cryptology - Crypto 99 Proceedings, Lecture Notes In Computer Science Vol. 1666, M. Wiener, ed., Springer-Verlag, 1999.
Illustrations : Arnaud Tisserand - « Cybersécurité et puces électroniques », 2017

Attaque par analyse de consommation d'énergie

- Exploitation
  - Signature en courant
  - Signature temporelle

$r = c_0$
POUR i **DE** 1 **À** n
  SI $a_i = 0$ **ALORS**
    $r = r + c_1$
  SINON
    $r = r \times c_2$



Illustrations : Arnaud Tisserand - « Cybersécurité et puces électroniques », 2017

Lab-STICC

Les attaques par canaux cachés

- Attaque par analyse du rayonnement électromagnétique

Jeu de sondes EM

Table XY
(Cartographie)

clé secrète = $(0101100100011\ldots)_2$

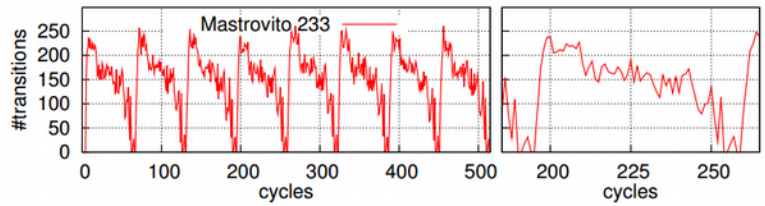
Les attaques par canaux cachés

- Principales techniques de protection
  - Un nouveau dispositif de protection
  - Modification / sécurisation d'un dispositif existant
  - Exemples :
    - Blindage
    - Uniformiser les temps de calcul
    - Uniformiser la consommation d'énergie
    - Introduire du bruit (instructions inutiles)
    - Reconfigurer le circuit
      - Changer le codage des données
      - Changer les algorithmes

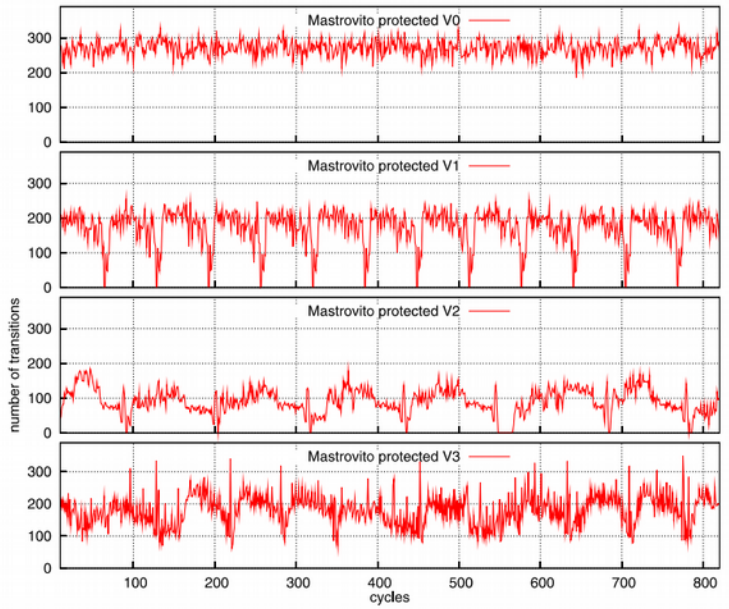
Les attaques par canaux cachés

- Exemple de contre-mesure :
  - Opérateurs arithmétiques sécurisés

Multiplieur non protégé



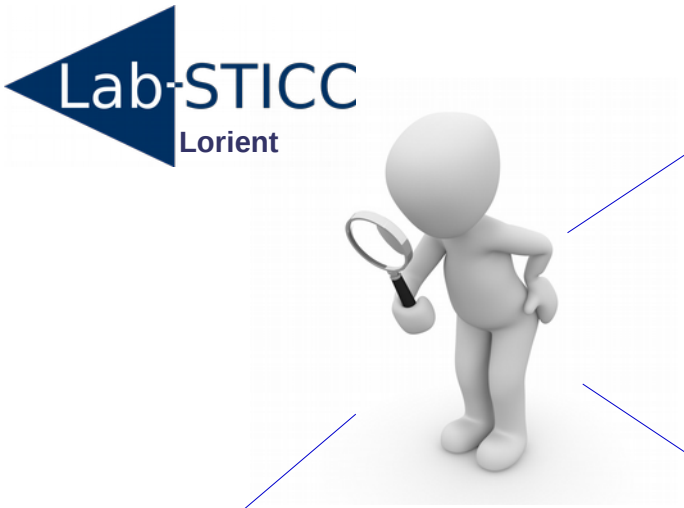
Multiplieurs protégés

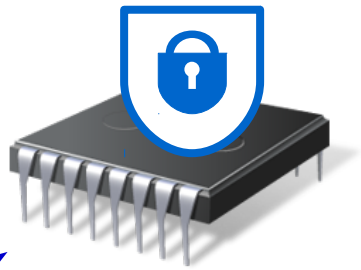


Illustrations : Arnaud Tisserand - « Cybersécurité et puces électroniques », 2017

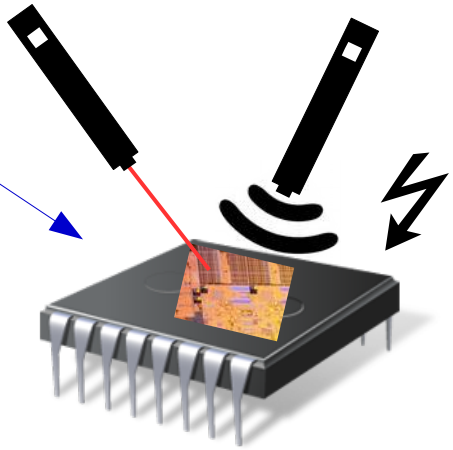
Lab-STICC

Nos travaux

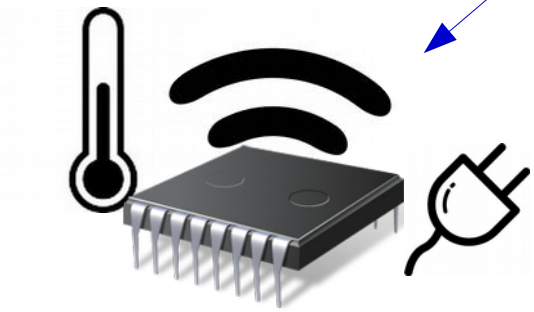




Conception de systèmes:
- **sécurisés**
- **pour la sécurité**



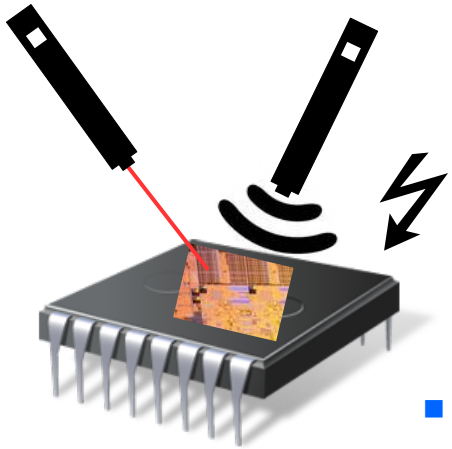
Attaques en faute



Attaques par canaux cachés

Les attaques en faute

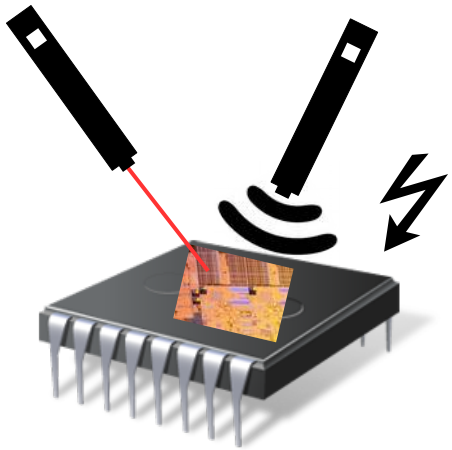
- Perturber le fonctionnement normal du circuit pour engendrer des erreurs
  - Désactivation de protection
  - Obtention d'informations secrètes



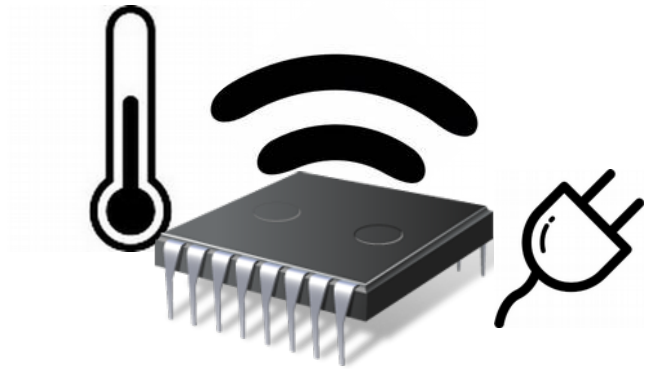
- Variation de paramètres
  - Température
  - Alimentation
  - Horloge
- Bombardement du circuit
  - Laser
  - Flash de lumière
  - Particules radioactives

Les attaques en faute

- En général, les attaques en faute sont couplées aux attaques par canaux cachés

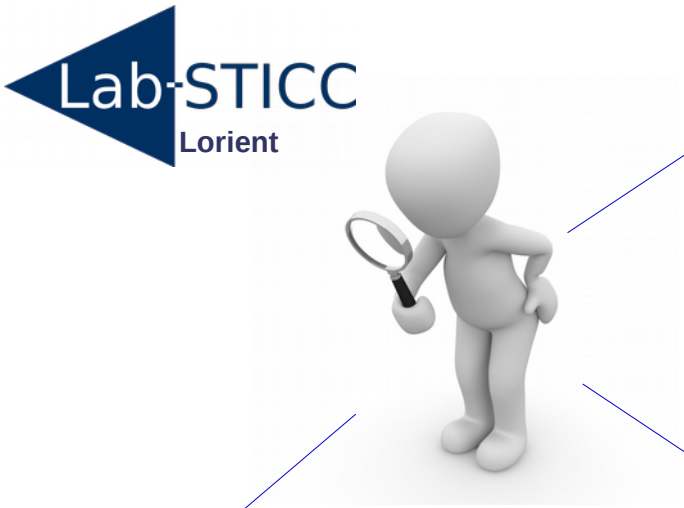


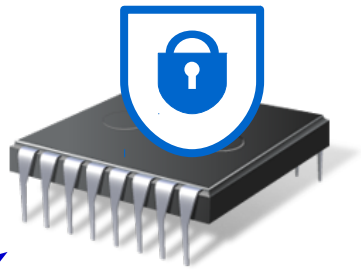
Attaques en faute



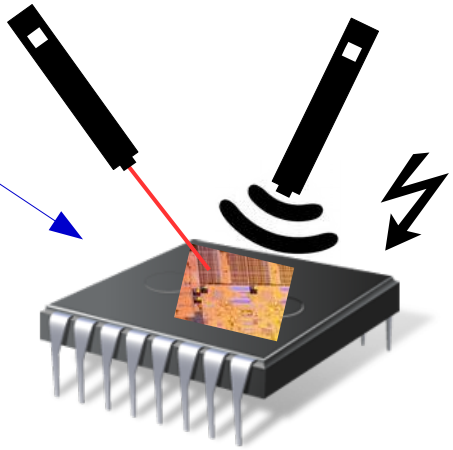
Attaques par canaux cachés

Nos travaux

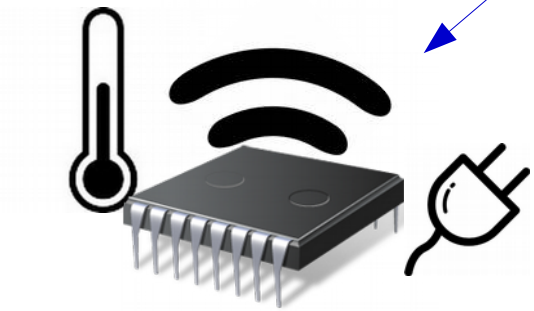




Conception de systèmes:
- **sécurisés**
- **pour la sécurité**



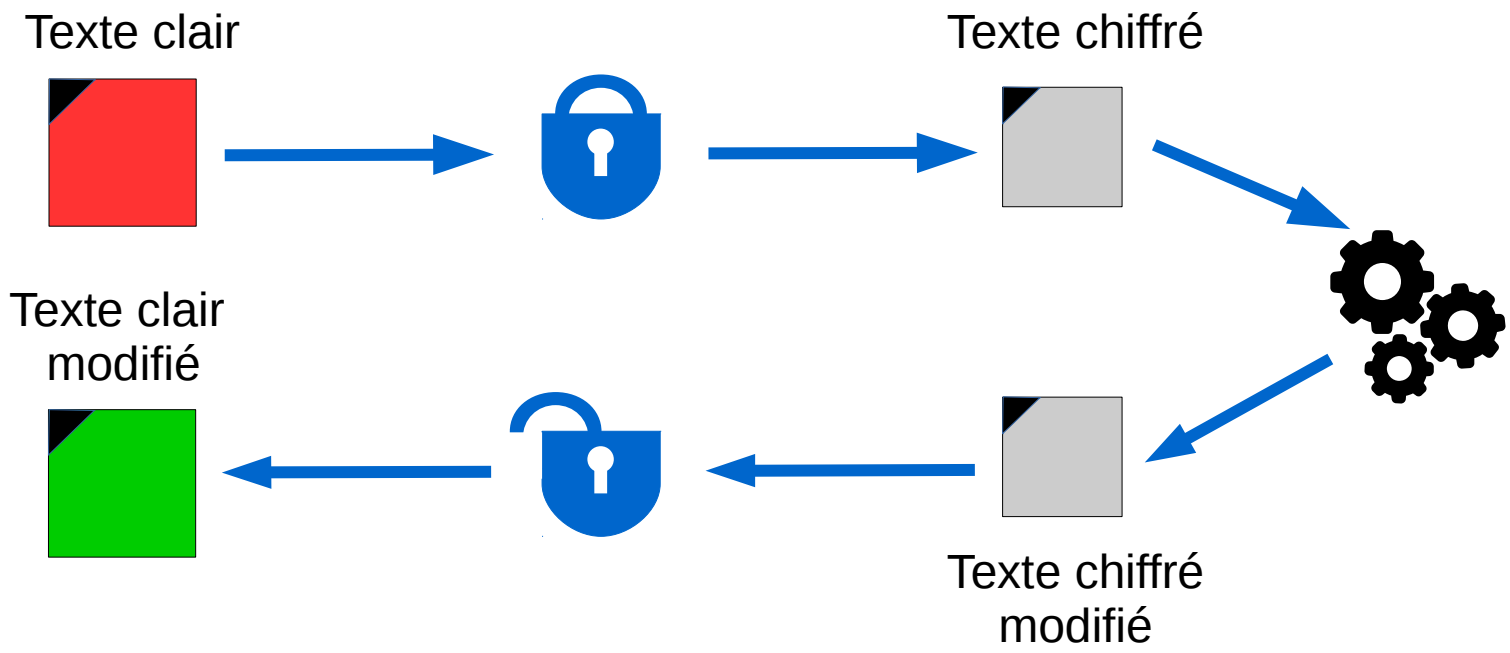
Attaques en faute



Attaques par canaux cachés

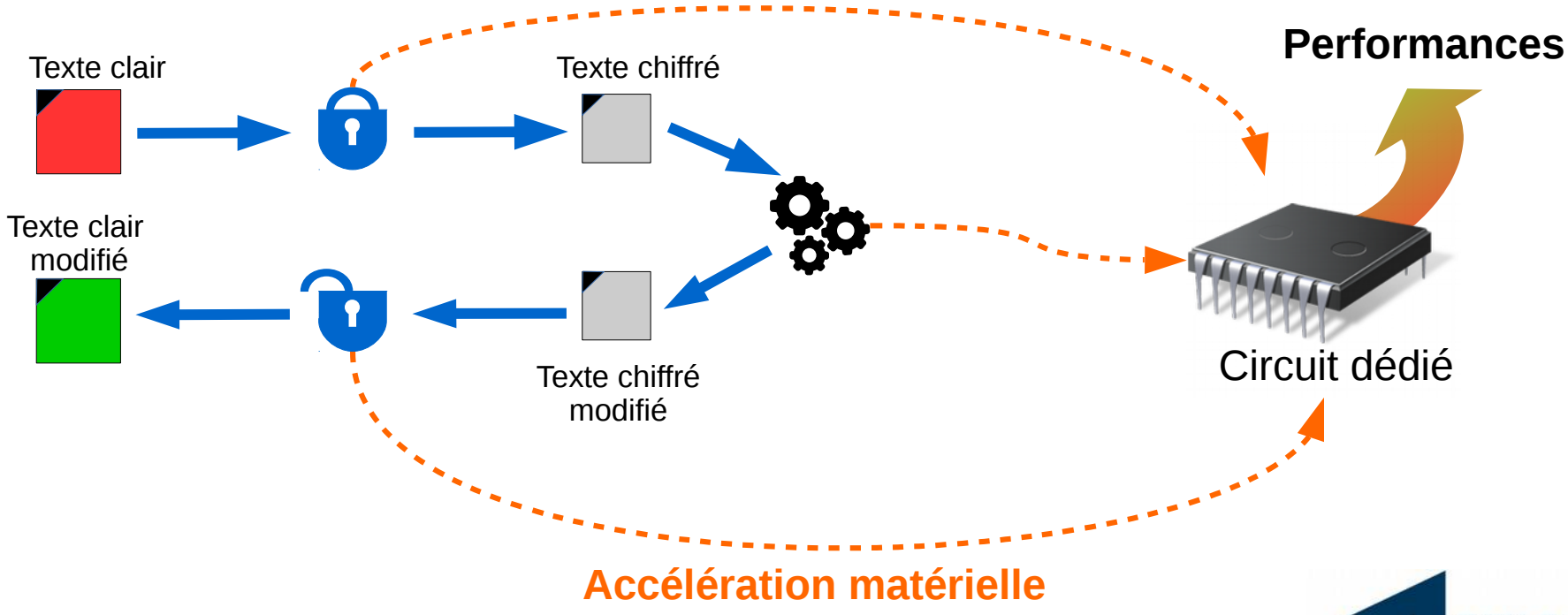
Accélération matérielle pour la cryptographie

- Exemple du chiffrement homomorphe



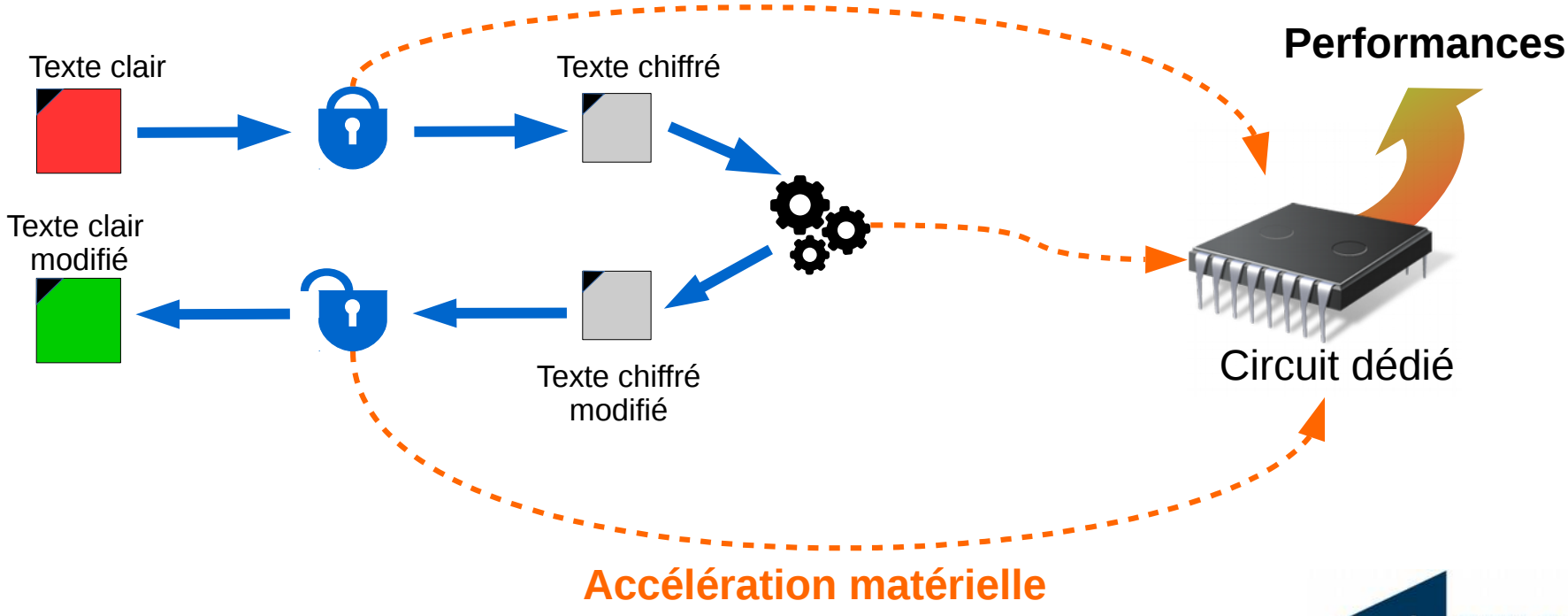
Accélération matérielle pour la cryptographie

- Exemple du chiffrement homomorphe
  - Cependant, les temps de calcul et les besoins en mémoire sont importants



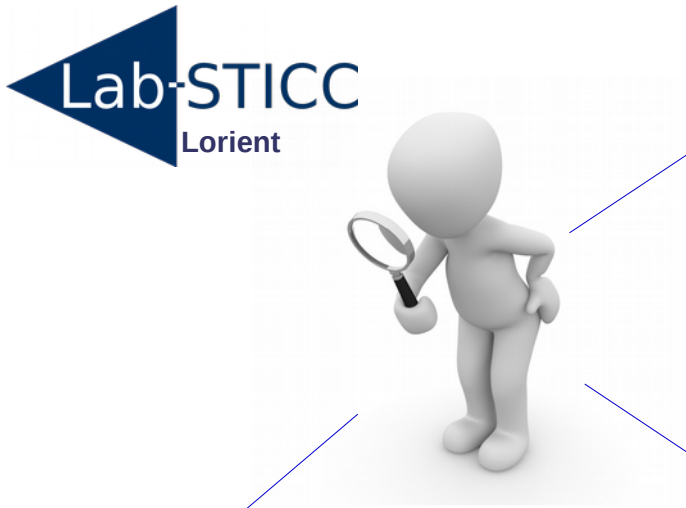
Accélération matérielle pour la cryptographie

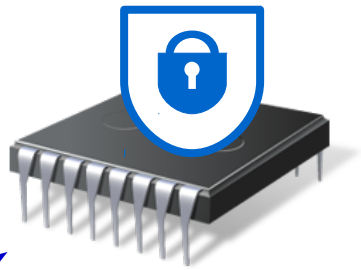
- Exemple du chiffrement homomorphe
  - L'opération de multiplication est critique
    - Une implémentation matérielle permet un gain ~ 35%[1]



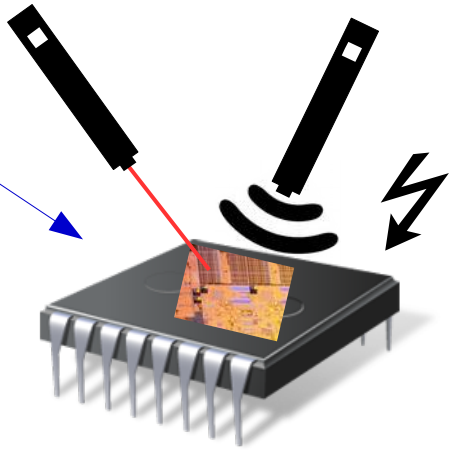
[1]V. Migliore, M. Mendez Real, V. Lapotre, A. Tisserand, C. Fontaine, G. Gogniat, "Hardware/Software co-Design of an Accelerator for FV Homomorphic Encryption Scheme using Karatsuba Algorithm," in IEEE Transactions on Computers , vol.PP, no.99, pp.1-1

Nos travaux

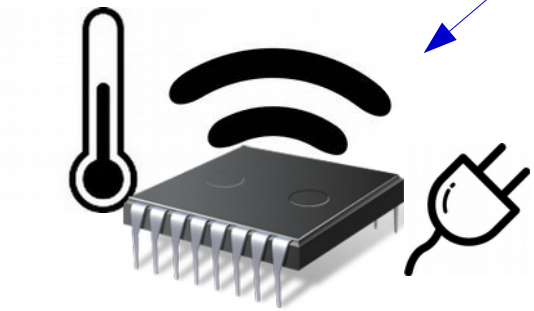




Conception de systèmes:
- **sécurisés**
- **pour la sécurité**



Attaques en faute

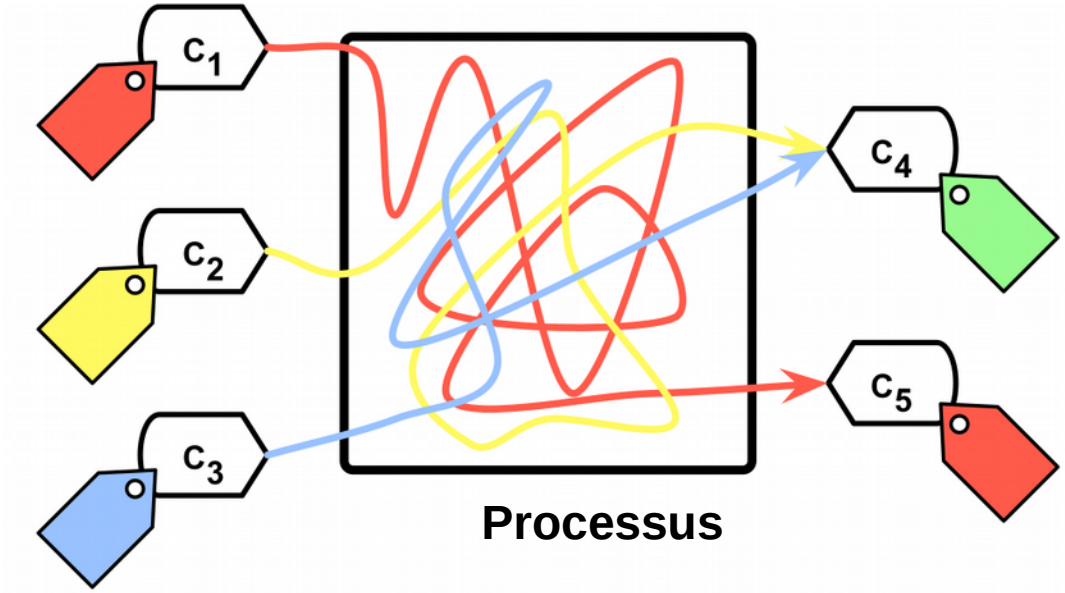


Attaques par canaux cachés

Lab-STICC

Accélération matérielle pour le DIFT

- Dynamic Information Flow Tracking
  - Les objets du système sont vus comme des conteneurs d'information.
    - Fichiers, variables, etc.
  - Des tags sont alors associés aux conteneurs d'information



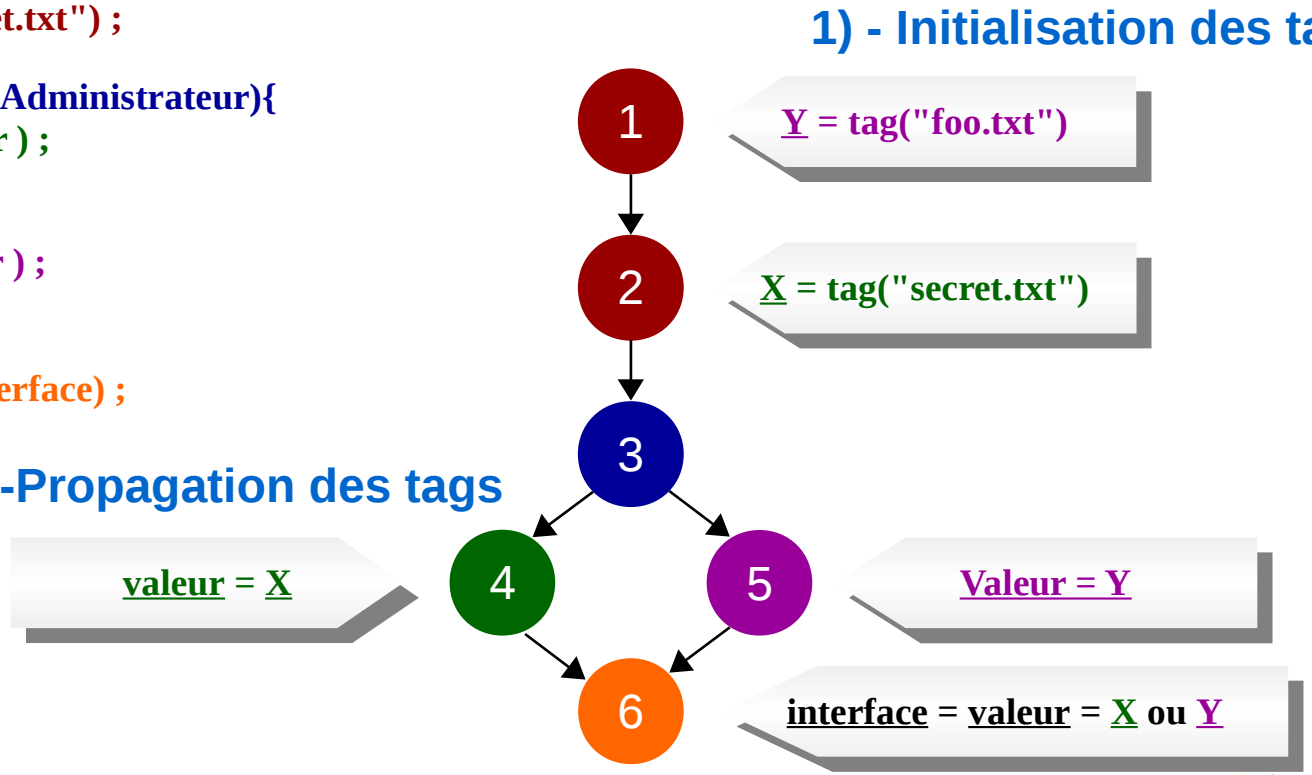
Accélération matérielle pour le DIFT

- Dynamic Information Flow Tracking
  - Exemple

```
1. Y = ouvrir("foo.txt") ;
2. X = ouvrir("secret.txt") ;

3. SI (utilisateur == Administrateur){
4.     Lire( x , Valeur ) ;
   }
   ALORS {
5.     Lire( y , valeur ) ;
   }

6. écrire (valeur, interface) ;
```



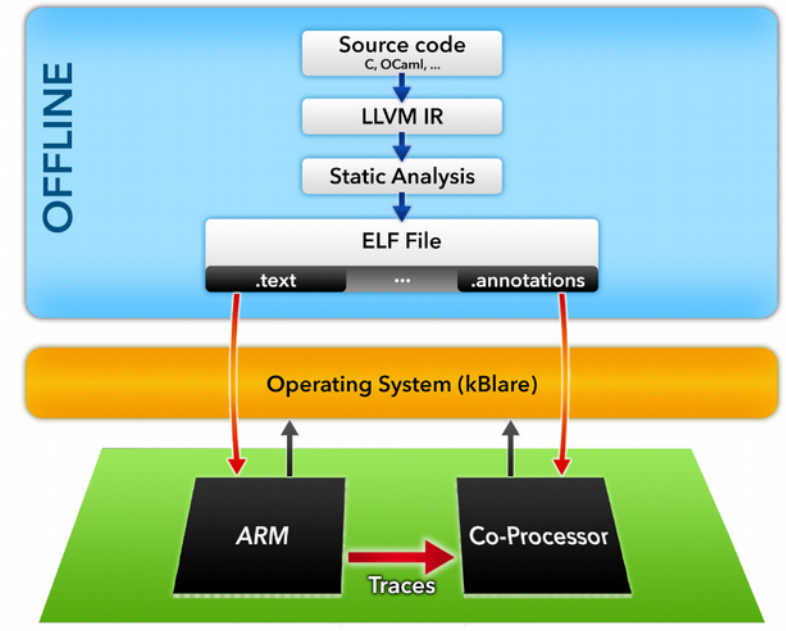
Accélération matérielle pour le DIFT

- Dynamic Information Flow Tracking
  - Approche logicielle vs. approche matérielle

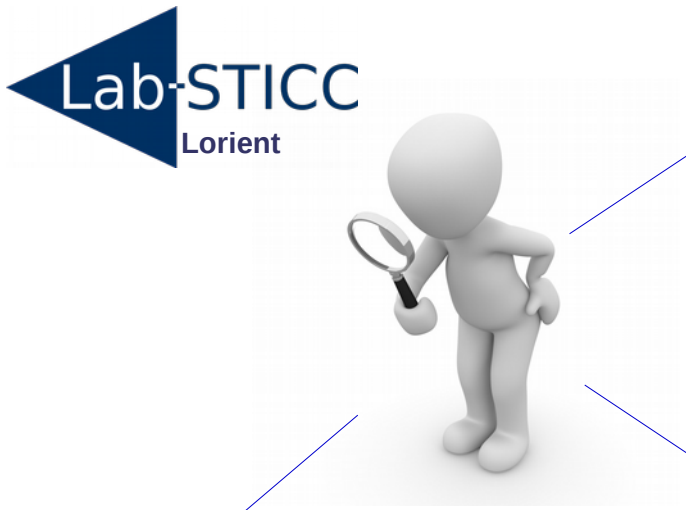
	Avantages	Inconvénients
Logicielle	Politique de propagation des tags flexible Large spectre d'attaques détectées	Fort impact sur les performances (de 300 % à 3700%)
Matérielle	Faible impact sur les performances (~10%)	De 1 à quelques Politiques de propagation des tags Coût des ajouts/modifications matérielles

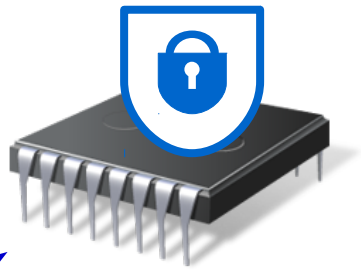
Accélération matérielle pour le DIFT

- Dynamic Information Flow Tracking
  - Le projet HardBlare
    - http://www.hardblare.cominlabs.ueb.eu/

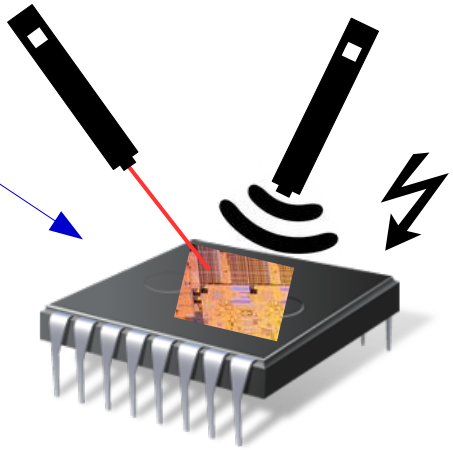


Nos travaux …

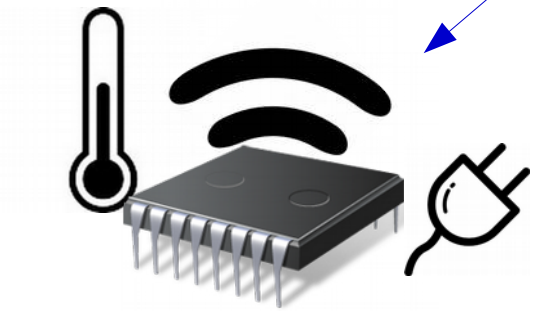




Conception de systèmes:
- **sécurisés**
- **pour la sécurité**



Attaques en faute



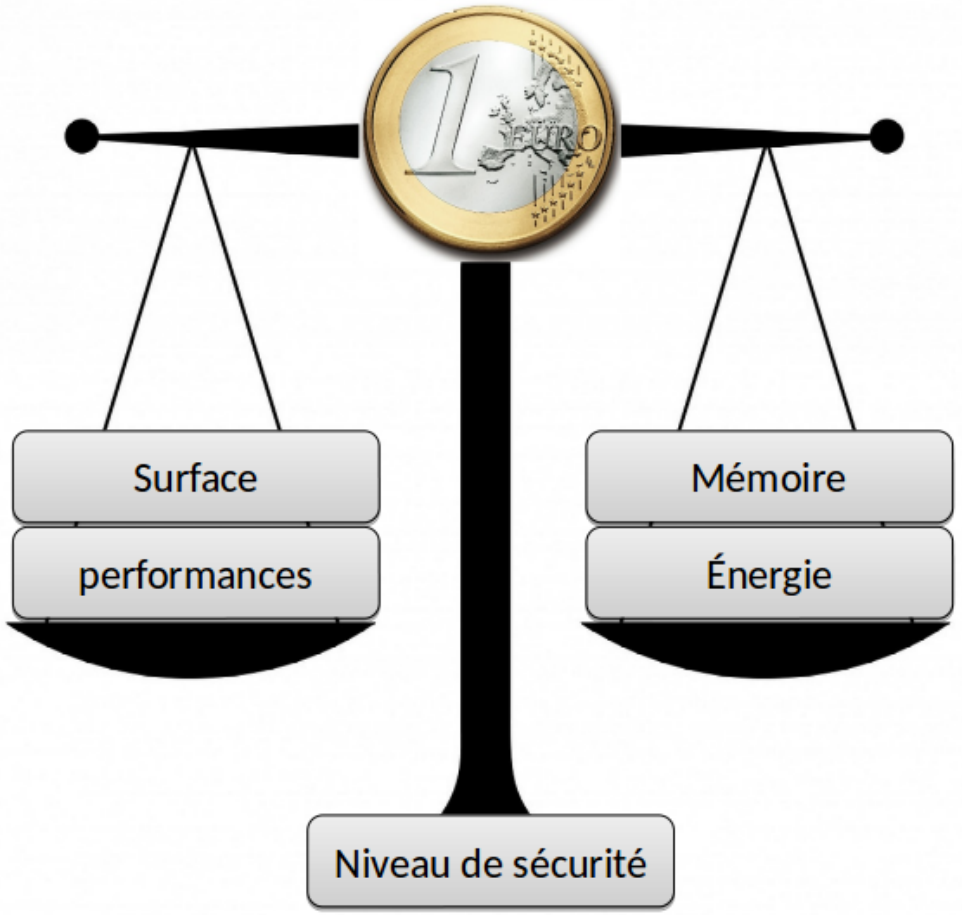
Attaques par canaux cachés

Pour conclure

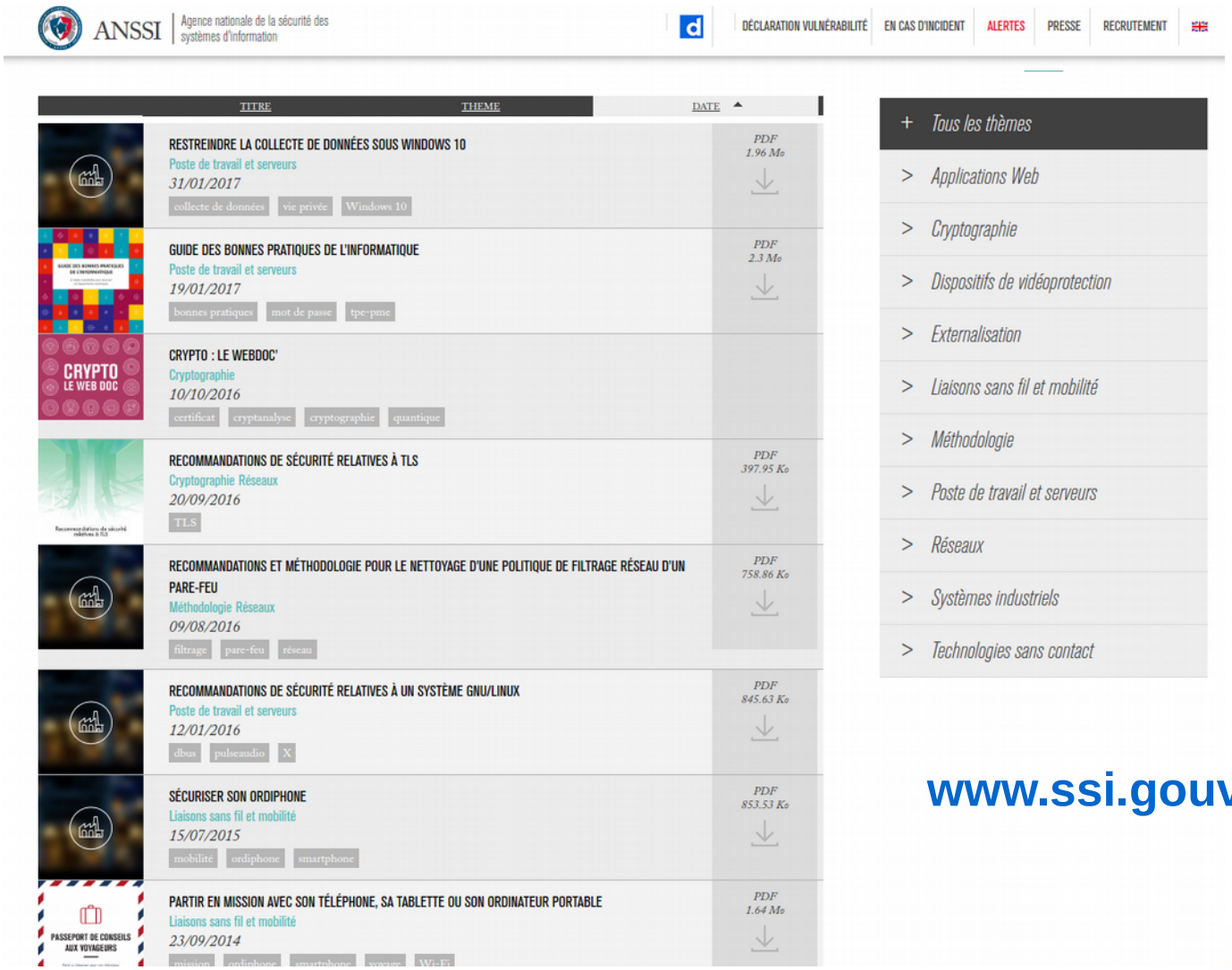
- Les attaques sont toujours plus performantes
- La sécurité doit être prise en compte à tous les niveaux
  - Théories, algorithmes, opérations, implémentations, utilisateurs

Pour conclure

- De plus, il faut faire certains compromis



Pour conclure



www.ssi.gouv.fr

Lab-STICC

Questions ?

- Contact
  - vianney.lapotre@univ-ubs.fr
  - http://www-labsticc.univ-ubs.fr/~lapotre/
  - Laboratoire Lab-STICC CNRS UMR 6285
    Université Bretagne Sud
    Centre de recherche C. Huygens, Rue St Maudé
    BP 92116, 56321 LORIENT Cedex
    FRANCE

Lab-STICC