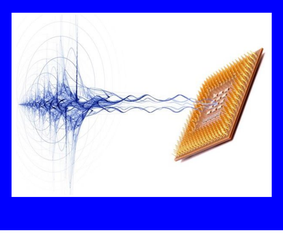
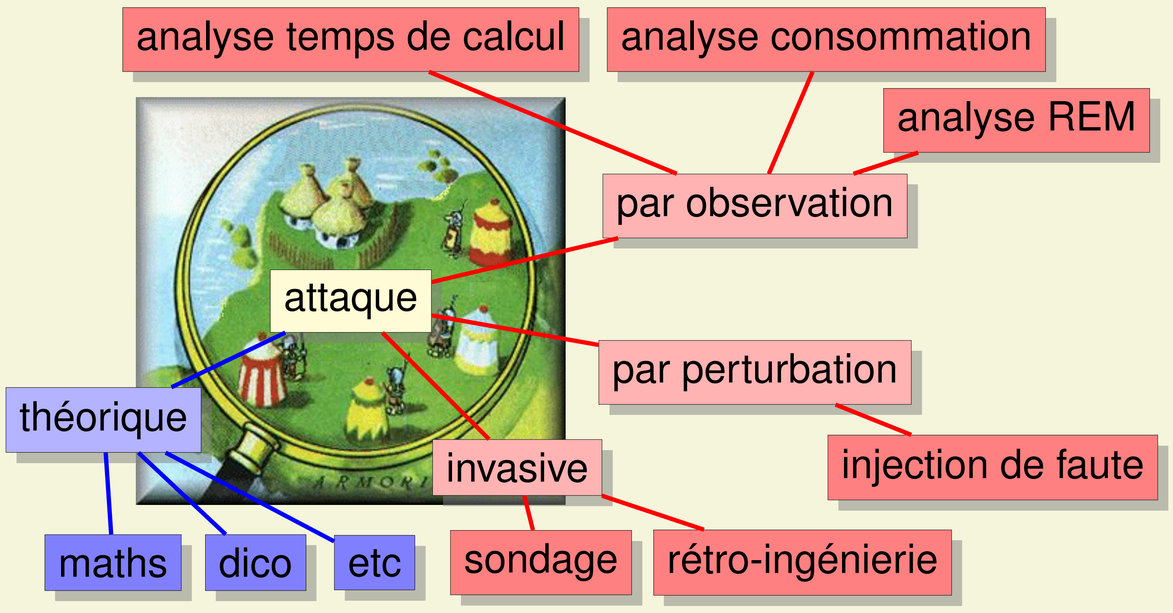
Puces électroniques et sécurité numérique

Équipe de recherche CAIRN



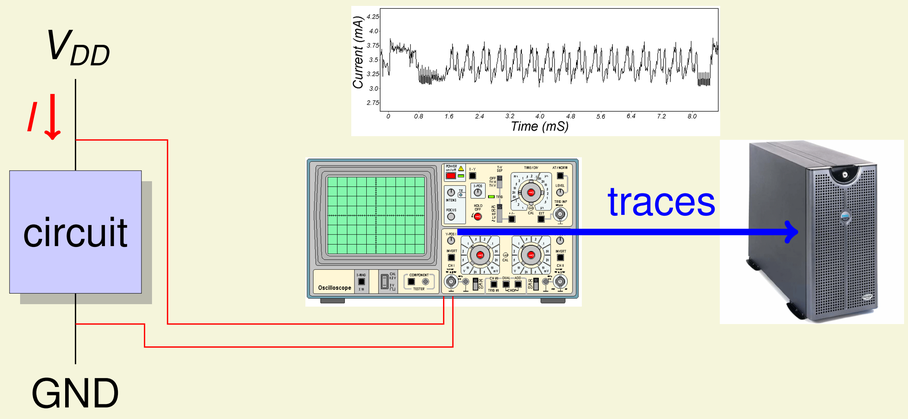
Types d'attaques



REM = rayonnement électromagnétique

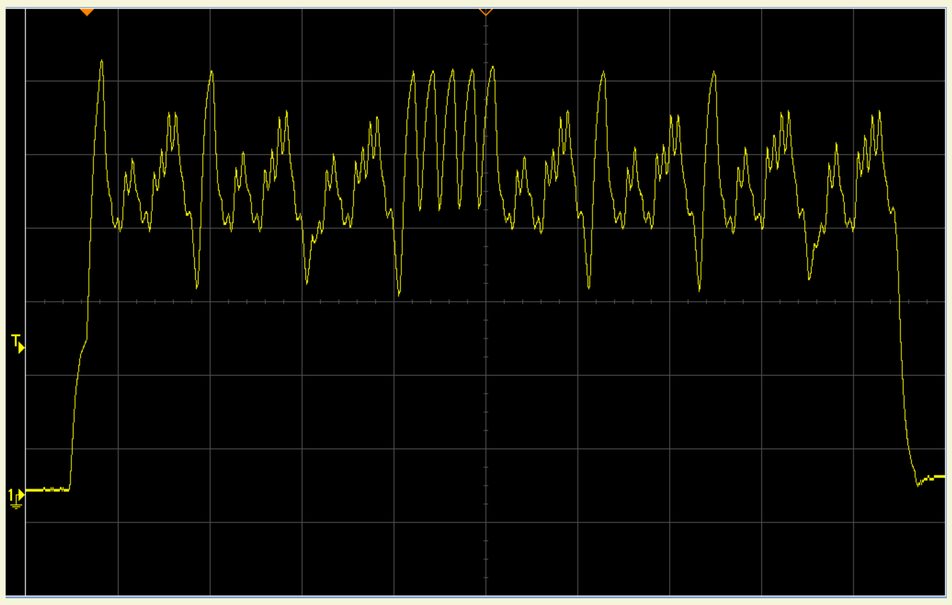
Attaque par mesure de la consommation d'énergie

Principe : mesurer le courant I qui alimente le dispositif

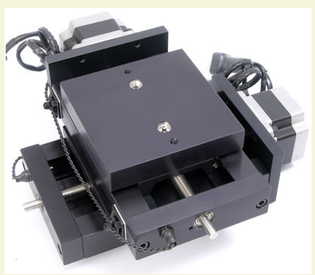


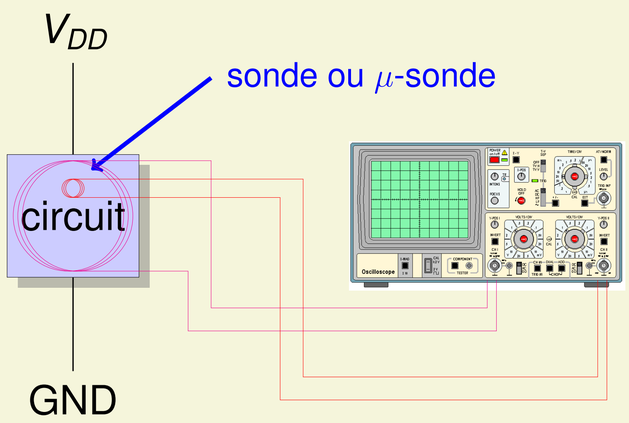
Notations : V_{DD} tension d'alimentation (5, 3, 2.5, 1.2, 0.9 V), GND masse

Trace mesurée sur un oscilloscope



Attaque par mesure du rayonnement électromagnétique

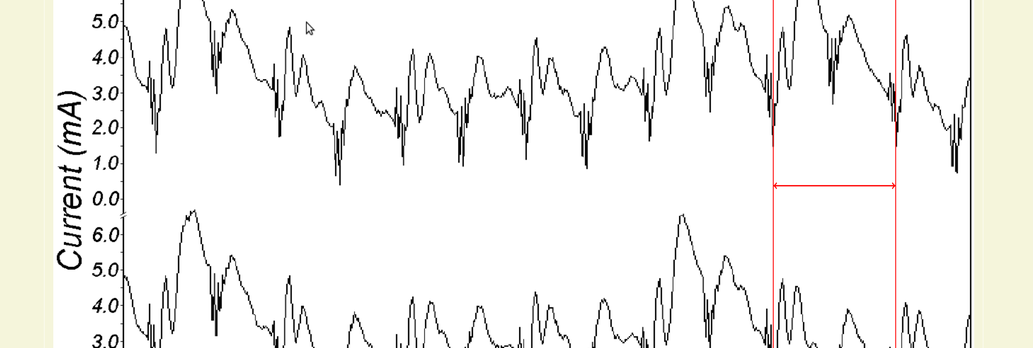




Comment ça marche ?

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

$r = 0$
`pour` i `allant de` 1 `à` n `faire:`
  `si` $a_i = 0$ `alors`
    $r = r + c_1$
  `sinon`
    $r = r \times c_2$



Principe : exploiter les corrélations entre les chiffres de la clé secrète et la consommation énergétique du circuit

Analyse simple

Limites : différences de consommation d'énergie trop petites pour être significatives, elles sont « noyées » dans du bruit

Analyse différentielle

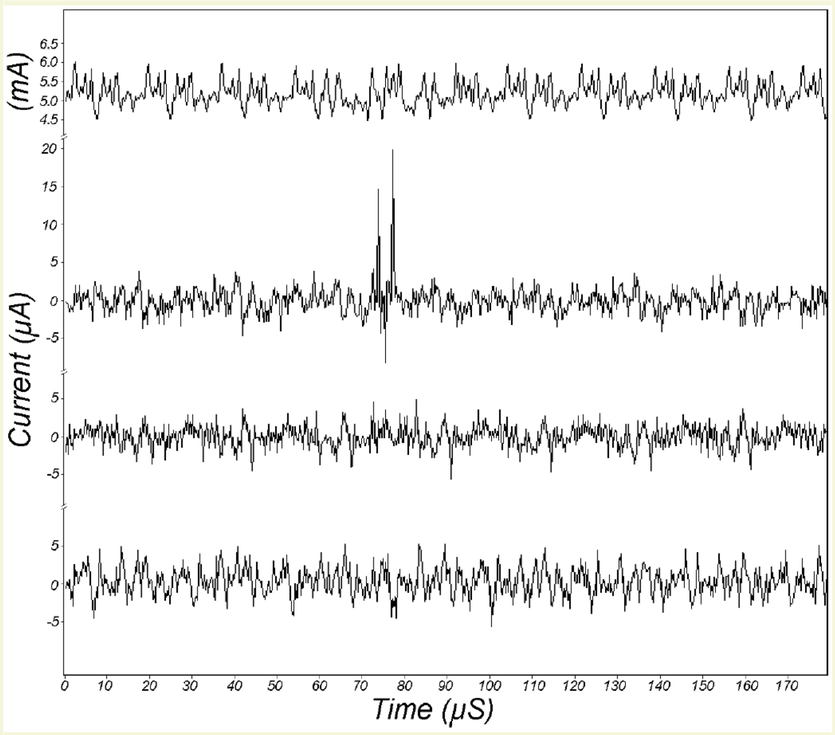
Principe : utiliser de nombreuses traces et des techniques de détection de corrélations statistiques

moyenne

hyp. correcte

hyp. incorrecte

hyp. incorrecte



http://www.irisa.fr/cairn/

cnrs
ens CACHAN BRETAGNE
ENSSAT LANNION
INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE
INRIA
centre de recherche RENNES - BRETAGNE ATLANTIQUE
UMR IRISA
UNIVERSITÉ DE RENNES 1