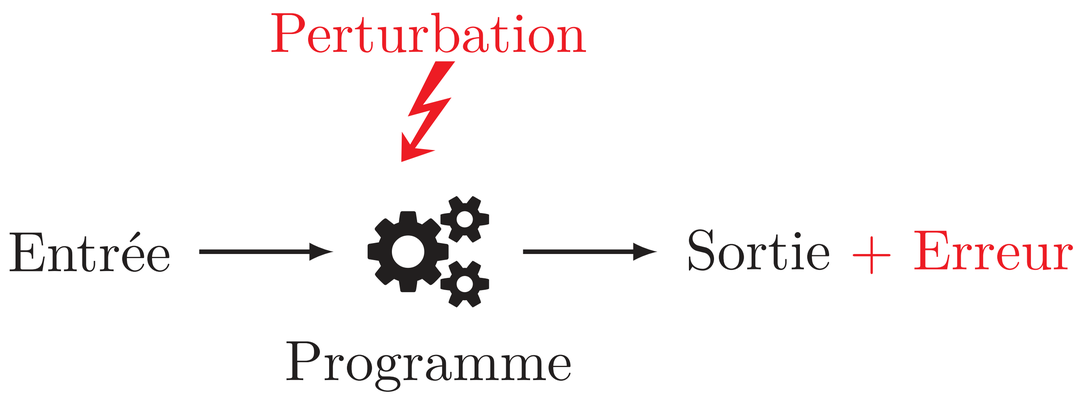
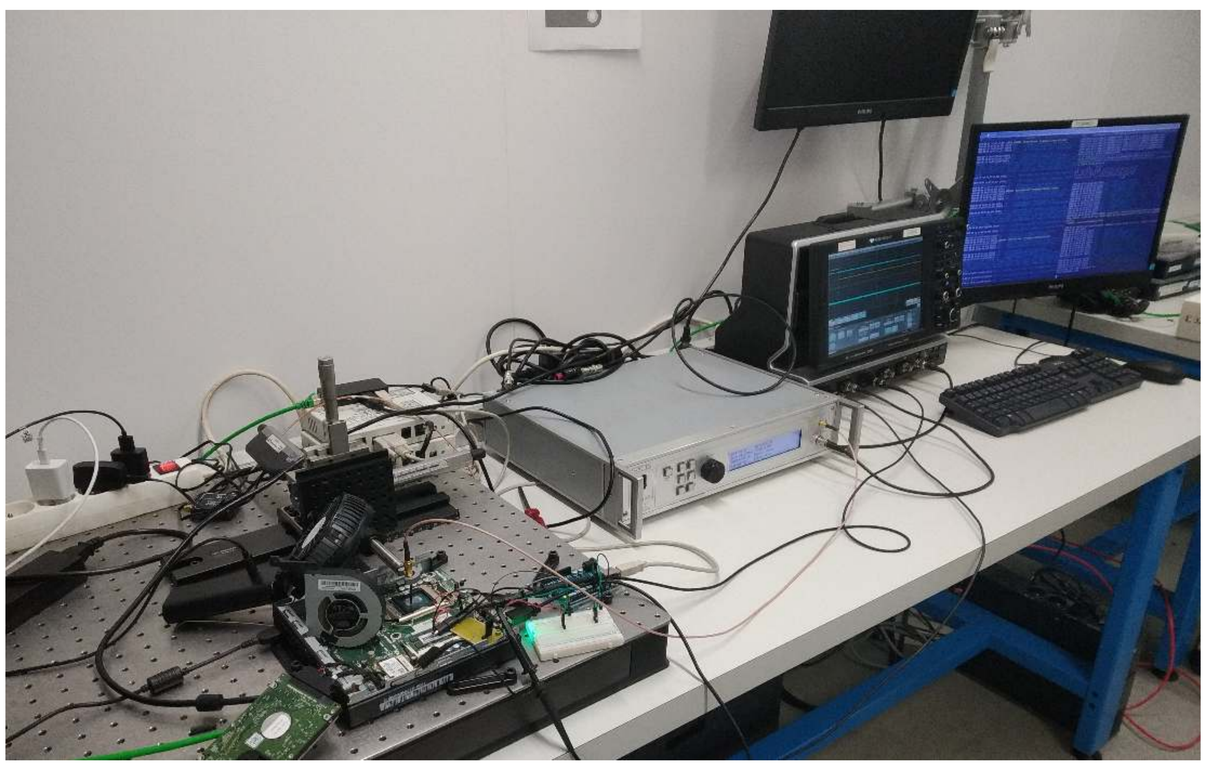
Caractérisation d'antennes pour l'injection de fautes sur composants électroniques

G. Bouffard, V. Houchouas, J. Lopes Esteves et T. Trouchkine
Agence Nationale de la Sécurité des Systèmes d'Information

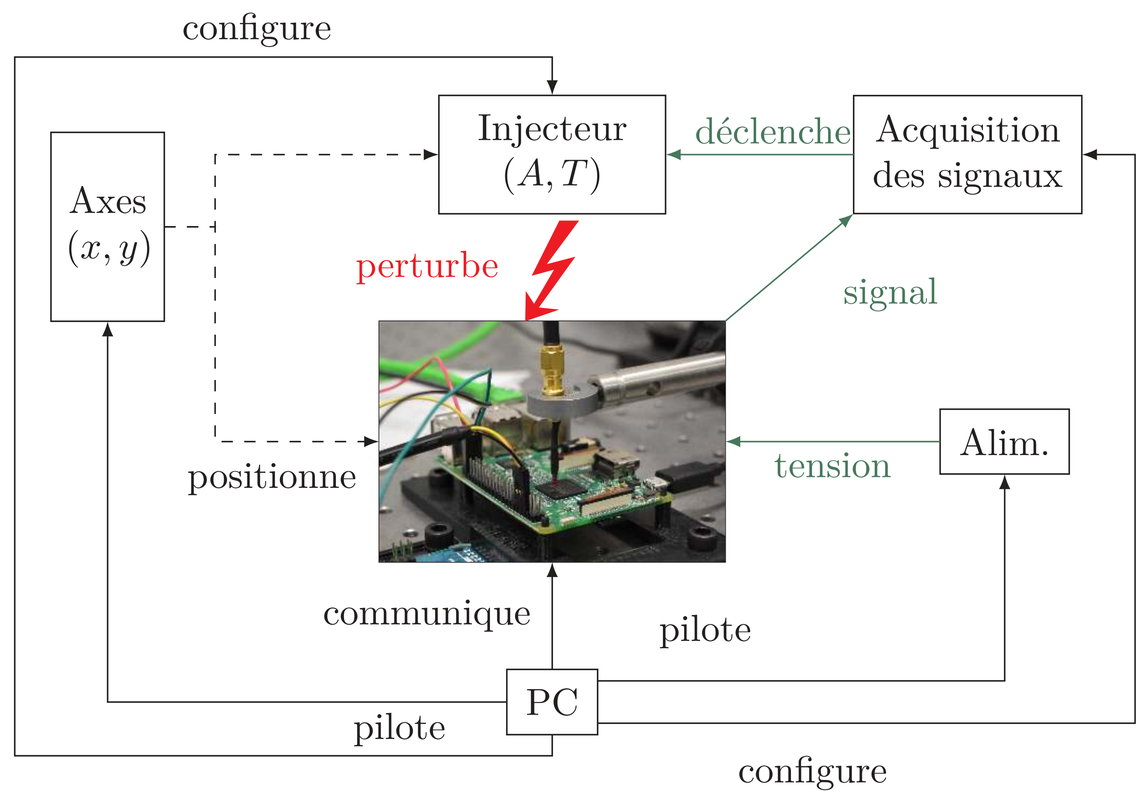
Attaques par injection de fautes



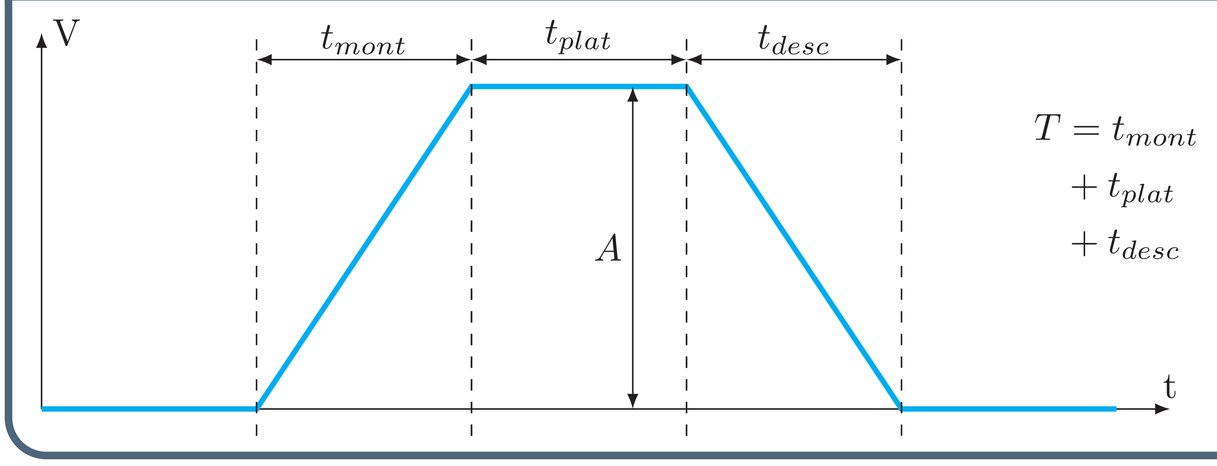
Banc d'injection EM de l'ANSSI



Principe d'un banc d'injection de fautes



Signal de sortie de l'injecteur et paramètres



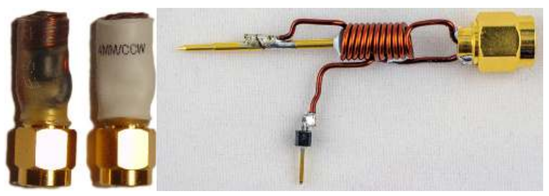
Constats

Signal d'agression peu analysé [1]

- (A, T) donné, mais $s(t)$ et $\hat{s}(f)$ inconnus

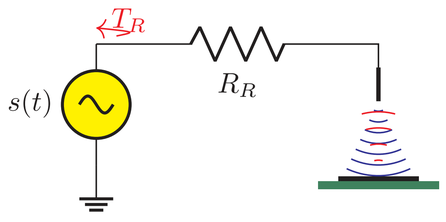
Reproductibilité difficile [2]

- Beaucoup de sondes « maison »



Bilan de puissance inconnu [3]

- $Z(f)$, $H(f)$ inconnus

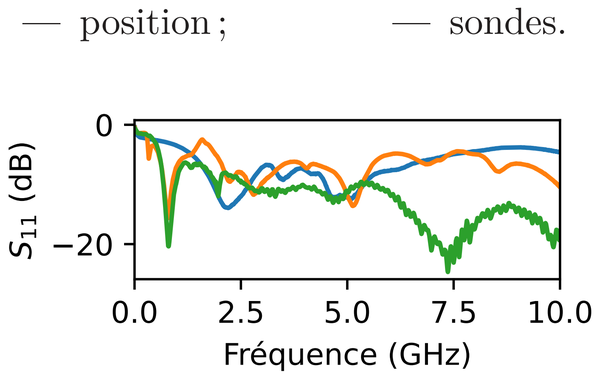


Profil d'attaquant surévalué [4]

Approches

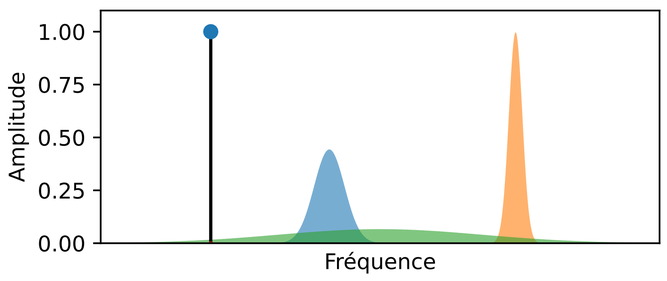
Paramètres S

- Variabilité :
  - cibles ;
  - position ;
  - ON/OFF ;
  - sondes.



Signal

- CW ⇔ impulsionnel
- Bande étroite ⇔ Large bande

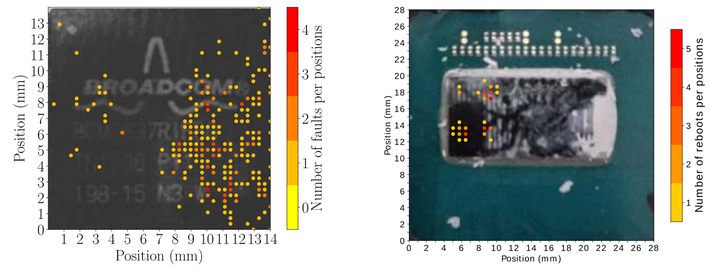


Sonde

- Focalisation ;
- Intérêt des ferrites ;
- Simulation ;
- Géométie ;
- etc.

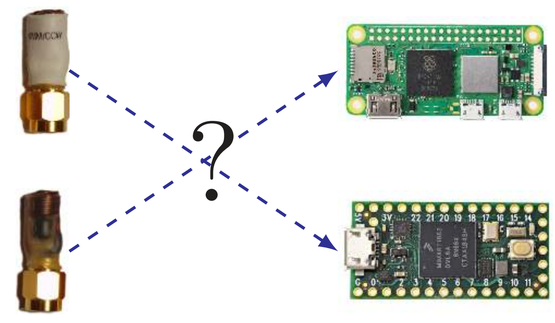
Perspectives

Points d'injection



Optimisation du signal

Adéquation sonde - cible



Caractérisation profil d'attaquant

References

[1] Jörn-Marc Schmidt and Michael Hutter. Optical and EM Fault-Attacks on CRT-based RSA : Concrete Results. In *Austrochip 2007, 15th Austrian Workhop on Microelectronics, 11 October 2007, Graz, Austria, Proceedings*, pages 61–67. Verlag der Technischen Universität Graz, 2007.

[2] Thomas Trouchkine, Guillaume Bouffard, and Jessy Clédière. EM fault model characterization on socs : From different architectures to the same fault model. In *18th Workshop on Fault Detection and Tolerance in Cryptography, FDTC 2021, Milan, Italy, September 17, 2021*, pages 31–38, 2021.

[3] J. Toulemont, G. Chancel, Jean Marc Gallière, Frédérick Mailly, Pascal Nouet, and Philippe Maurine. On the scaling of EMFI probes. In *18th Workshop on Fault Detection and Tolerance in Cryptography, FDTC 2021, Milan, Italy, September 17, 2021*, pages 67–73, 2021.

[4] Philippe Maurine. Techniques for EM fault injection : Equipments and experimental results. In *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012*, pages 3–4, 2012.