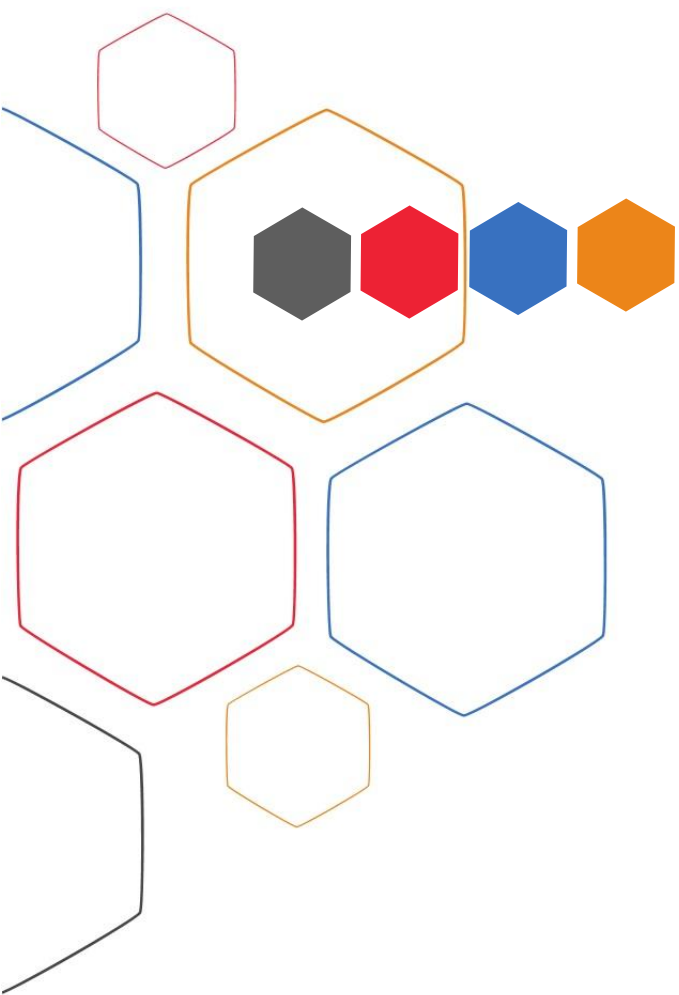




Emissions électromagnétiques & Sécurité embarquée



UNIVERSITÉ DE
MONTPELLIER

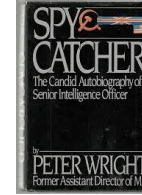


Quelques dates importantes ...

1956 : Crise du canal de Suez

P. Wright du MI5 casse la machine Hagelin avec des microphones

La première ou l'une des **premières attaques par observation d'un canal caché**



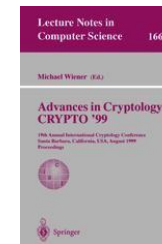
1999 : Les attaques matérielles sur la place publique

Differential Power Analysis (P. C. Kocher et al)

Les attaques par observation d'un canal caché

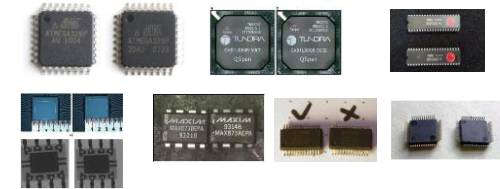
L'attaque par faute de Bellcore labs (D. Boneh et al)

Les attaques par injection de fautes



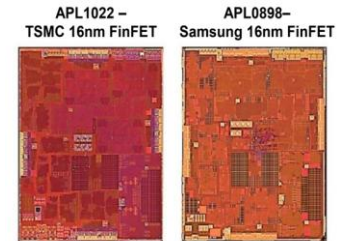
2007 : Opération Orchard / The hunt for the Killing Switch (IEEE Spectrum)

Suspicion de backdoors dans les circuits intégrés



2009 + : CHES 2009 : The state-of-the-art in Semiconductor Reverse Engineering (R. Torrance)

Emergence des copies / Contrefaçons de circuits



2012 : Breakthrough Silicon Scanning Discovers Backdoor in Military Chip (S. Skorobogatov and al)

Preuve de l'existence de backdoors



Diverses menaces sur le matériel

Attaques par observation (canaux cachés)



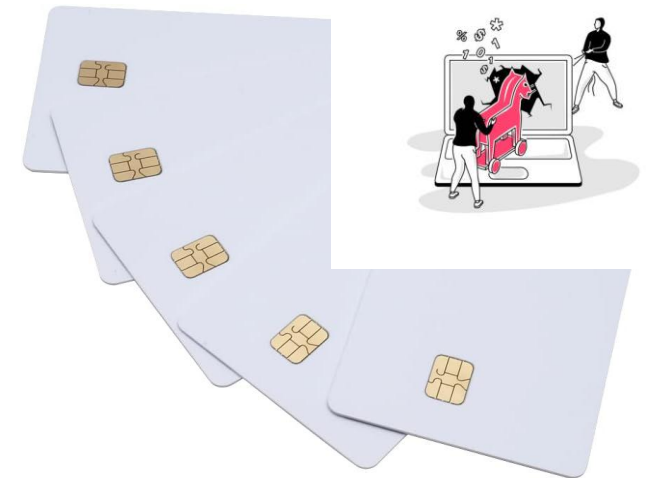
30 ans d'évolution :
De la DoM aux réseaux CNN et GAN

Attaques par injection de fautes

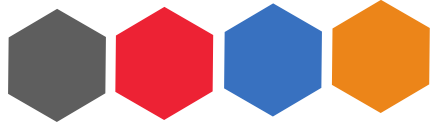


30 ans d'évolution :
D'impulsions de tension à des impulsions Laser et X-Ray

Chevaux de Troie matériels Contrefaçons / Remarquage Reverse engineering



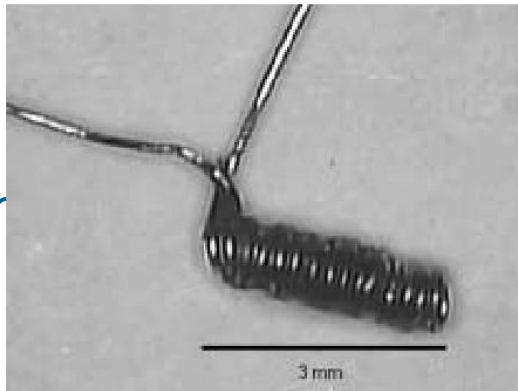
**6000 ans de manifestation de la
cupidité humaine sans limite**



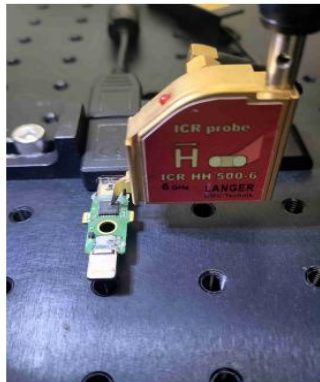
Le champ (ou canal) électromagnétique ...

Attaques par observation (canaux cachés)

2001 : Electromagnetic Analysis: **Concrete** Results (K. Gandolfi et al)



Sonde EM
utilisée

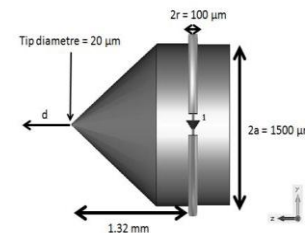
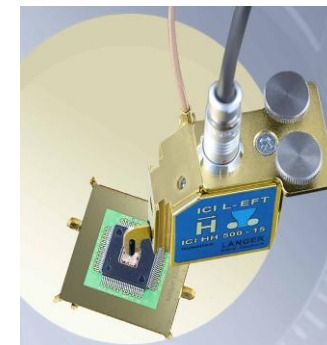
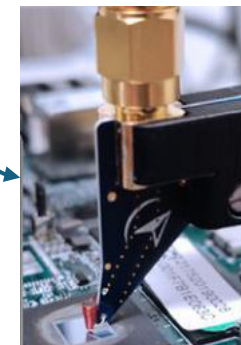


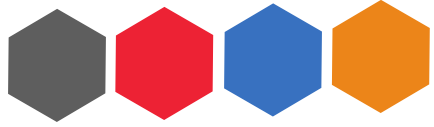
Attaques par injection de fautes

2007 : Optical and EM fault-attacks on CRT-based RSA : **Concrete** results. (J.- M. Schmidt et al)



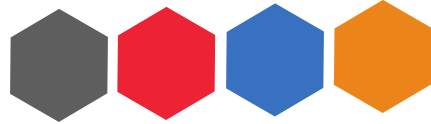
Injecteur utilisé :
un allume gaz





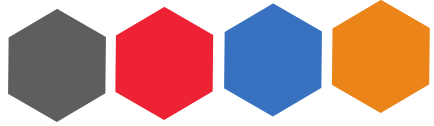
Le canal électromagnétique demain ?

- Peut-on améliorer les plateformes d'analyse et d'injection EM ?
- Probablement :
 - Comment améliorer la résolution spatiale des sondes pour suivre les évolutions technologiques ?
 - Comment concevoir des caméras électromagnétiques (architectures multi-cœurs) ?
 - Comment adapter 'automatiquement' le couplage EM sonde / circuits cibles ?
 - Est-il possible d'exploiter le champ électrique complètement délaissé ...
 - Comment mieux exploiter les signaux EM (démodulation) ?
 - ...



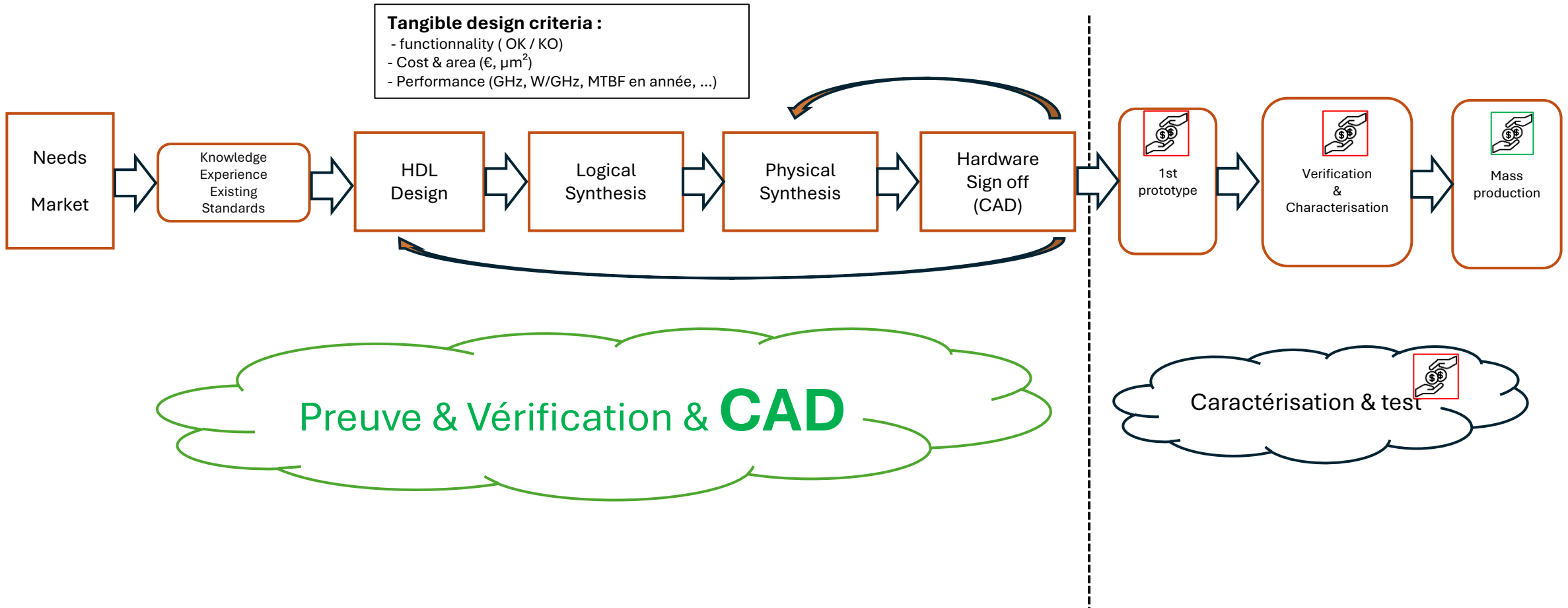
Ceci étant ...

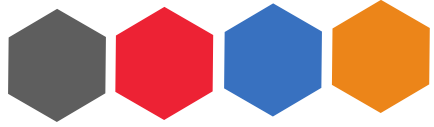
- 1) Le flot de conception des CI et CI sécurisés
- 2) Deux Challenges relatifs à ce flot et au champ EM



Flot de conception des produits intégrés

Conception Assistée par Ordinateur

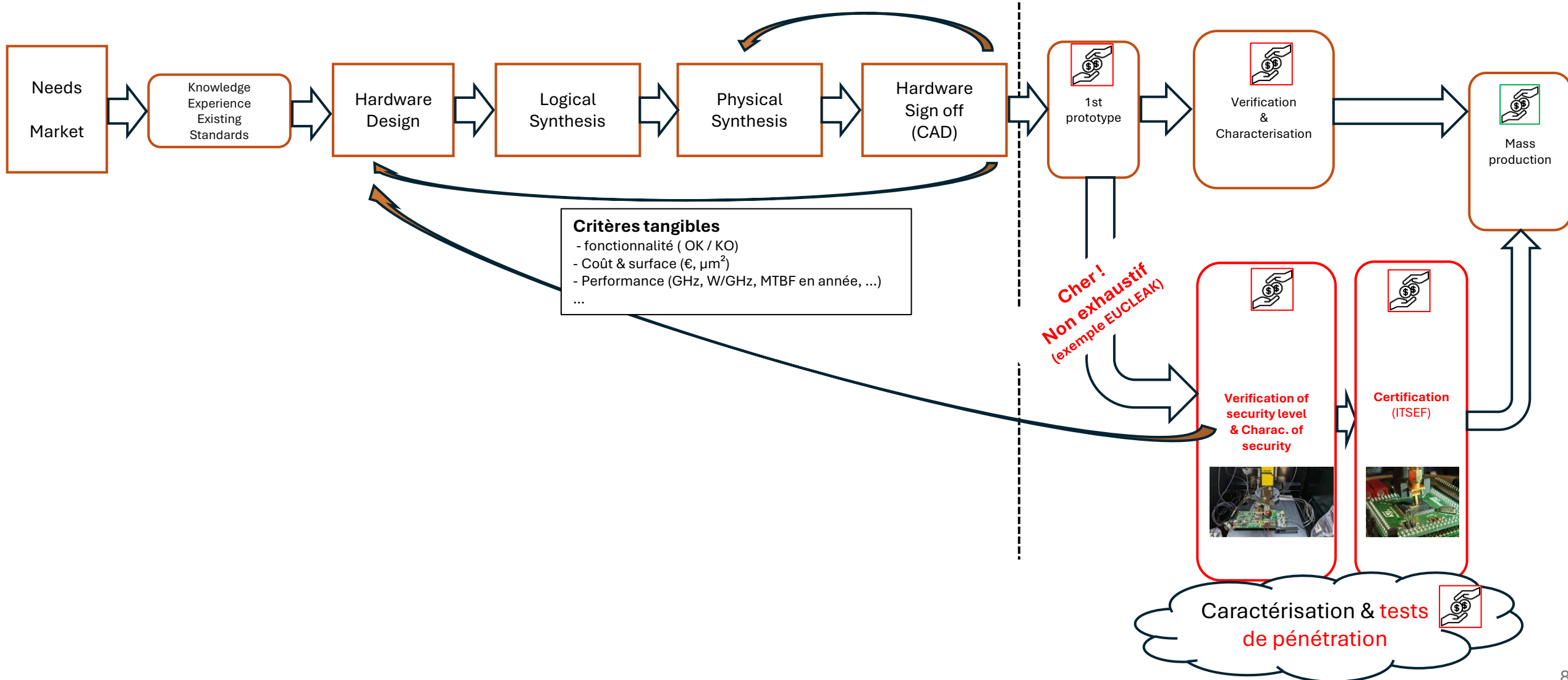


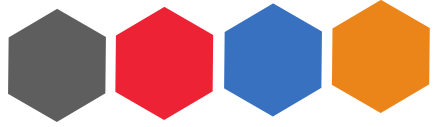


Flot de conception des produits intégrés

Conception Assistée par Ordinateur

Fabrication

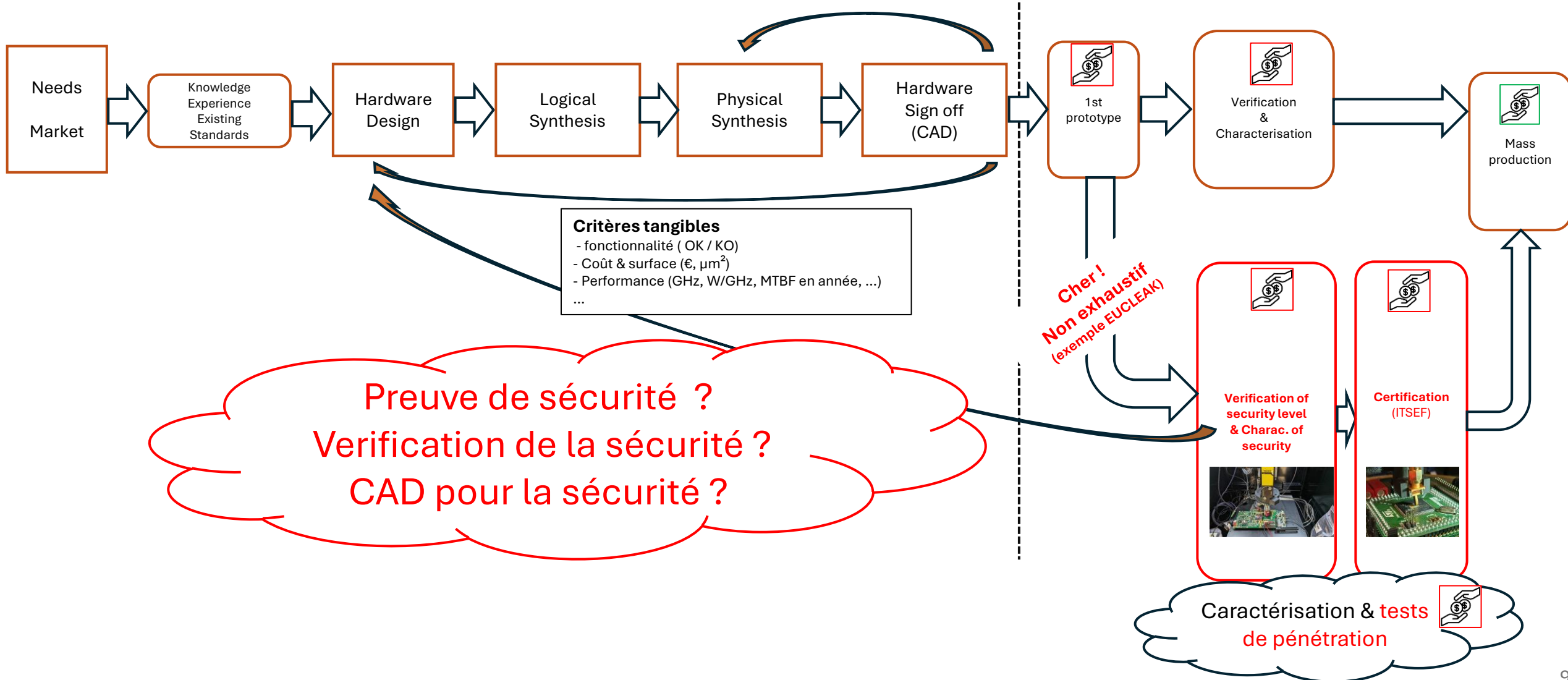


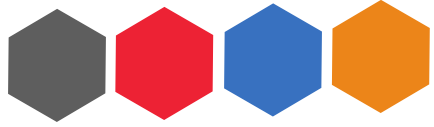


Flot de conception des produits intégrés

Conception Assistée par Ordinateur

Fabrication





Flot de conception et champ EM ?

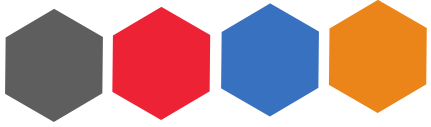
Comment simuler le champ magnétique d'un circuit intégré complet ?

Comment simuler l'impact d'une perturbation EM intentionnelle ?

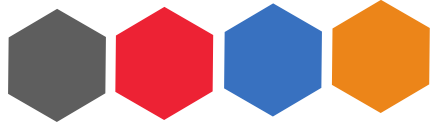
Comment reproduire les attaques SCA EM avant fabrication ?

Comment reproduire des attaques par EMFI avant fabrication ?

.....



Comment reproduire les attaques SCA EM avant fabrication ?



Reproduire les attaques SCA avant fabrication

2001 – 2025 : une nécessité qui peine à s'imposer



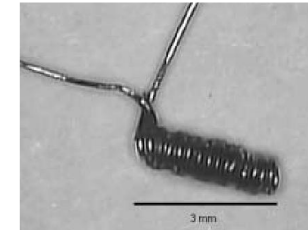
Mener des attaques SCA sur $I(t)$ suffit amplement !!!



Finalement ca ne suffit pas ...
 $B(x,y,z,t)$ n'est pas $I(t)$!!!

2001 : Electromagnetic Analysis: Concrete Results (CHES)

K. Gandolfi, C. Mourtel, F. Olivier



2010 : A Simulation Flow for Time Domain Magnetic Radiations of Ics

V. Lomne, P. Maurine, L. Torres, M. Robert, T. Ordas, M. Lisart, J. Toublanc (EMC Europe)

(des comparaisons pas totalement convaincantes entre silicium et simulations)

2017: Efficient Simulation of EM Side-Channel Attack Resilience (IEEE CCAD)

A. Kumar, C. Scarborough, A. Yilmaz, M. Orshansky (pas de comparaison entre silicium et simulations)

2021 : Checking robustness against EM side-channel attacks prior to manufacturing (IEEE TCAD)

D. Poggi, T. Ordas, A. Sarafianos, P. Maurine

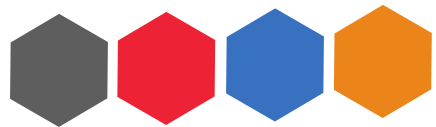
(comparaisons entre silicium et simulations)

2021 : Multiphysics Simulation of EM Side-Channels from ... (IEEE Trans. on Inf. Forensics and Security)

L. Lin, D. Zhu, J. Wen, H. Chen, Y. Lu, N. Chang, C. Chow, H. Shrivastav, G. W. Chen, K. Monta, M. Nagata

2024 : PreSCAN: A Comprehensive Review of Pre-Silicon Physical Side-Channel V.... (Chips)

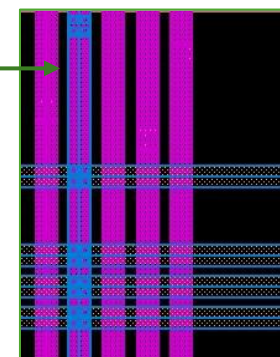
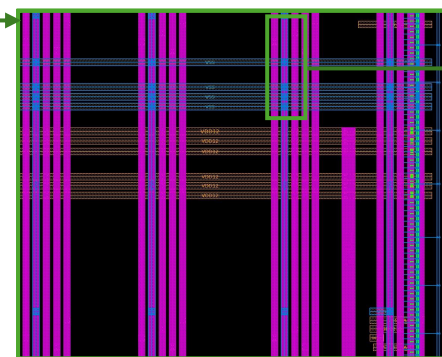
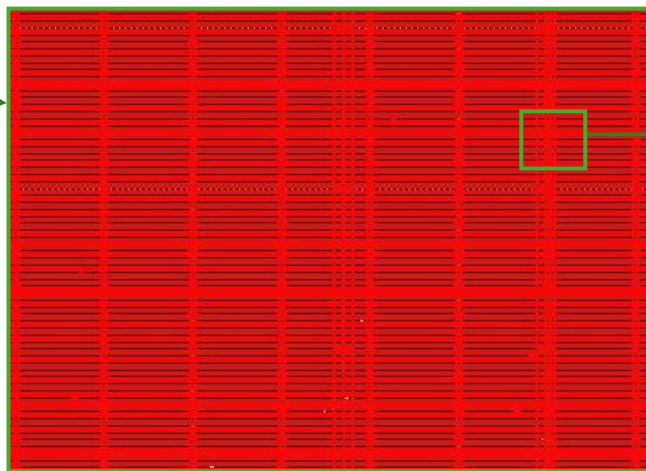
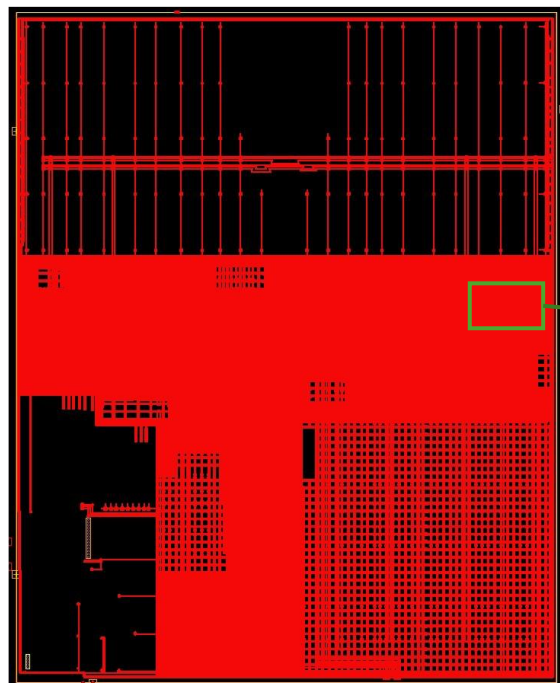
Md Kawser Bepary, T. Zhang, F. Farahmandi, M. Tehranipoor



Reproduire les attaques SCA avant fabrication

4.5mm

5.5mm



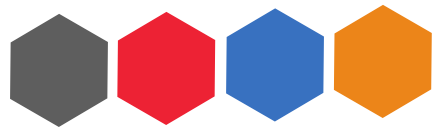
Réseau d'alimentation d'un simple
µcontrolleur 1 MGates



=

Des mètres d'interconnexions !!

~~Ansys HFSS~~



Reproduire les attaques SCA avant fabrication

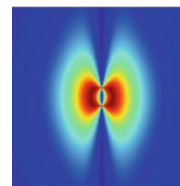
Biot – Savart

&

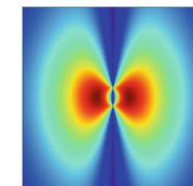
Approche ‘diviser pour mieux régner’

- Identification du segment d’interconnexion élémentaire (le plus petit et le moins large de tout le circuit)
- Calcul du champ $B_z(t)$ rayonné (unitaire en courant) par ce segment élémentaire

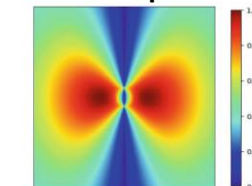
$z=25\mu\text{m}$



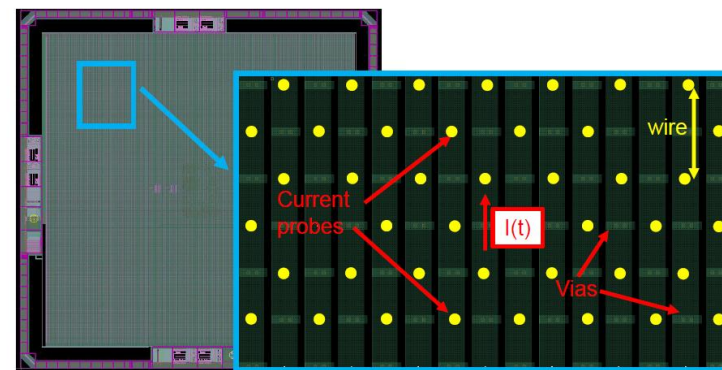
$z=50\mu\text{m}$



$z=100\mu\text{m}$



- Découpage de toutes les interconnexions en segments élémentaires
- Pondération des courants dans chaque segment élémentaire (densité de courant)



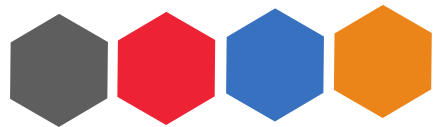
- Maillage ($1\mu\text{m} \times 1\mu\text{m}$) des plans souhaités au dessus du circuit et calcul de $B_z(x,y,h,t)$ par **tamponnage de l’espace**
- Calcul de $\phi_z(t)$ rayonné par les segments élémentaires dans des sondes (Maillage plus lâche de l’espace)
- Calcul le signal mesuré par **une sonde parfaite**

$$B_z(x, y, h, t) = \sum_{i=0}^w B_z^i(x, y, h, t) \quad \phi_z(t) = \int_{S_q} B_z(t) \cdot dS_q \quad \epsilon(t) = -\frac{d\phi_z(t)}{dt}$$

- Application des attaques SCA



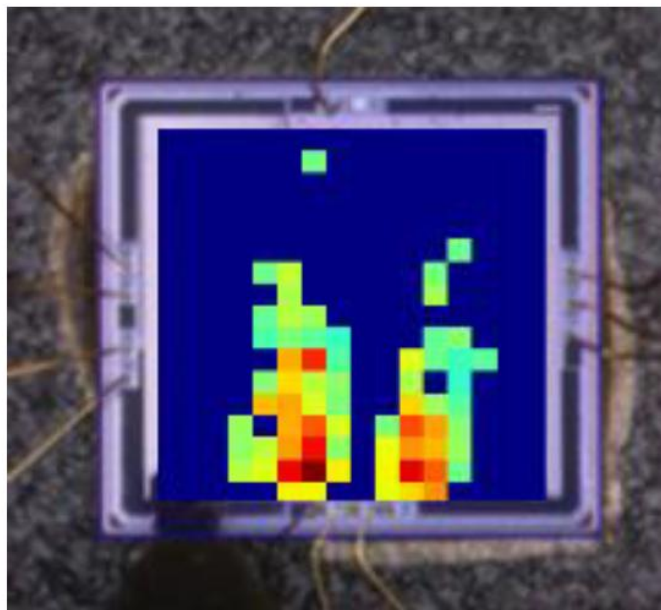
$$\hat{k} = \operatorname{argmax}_k \{ \max_t (\rho(C_i; T_j)) \}$$



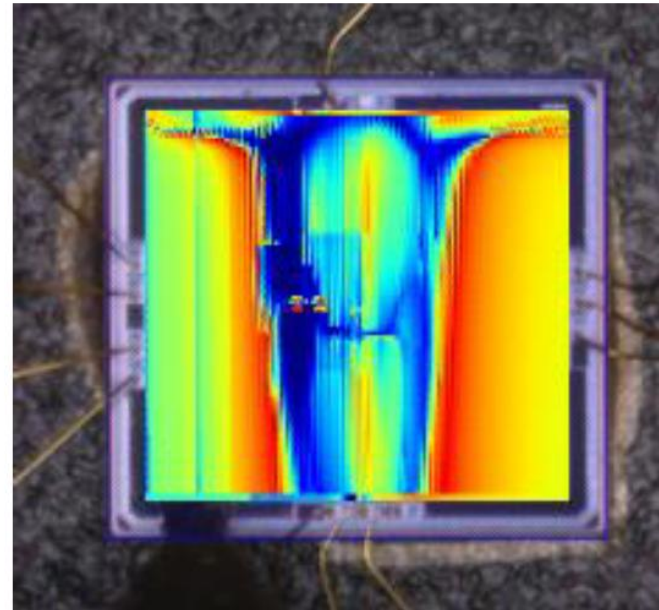
Reproduire les attaques SCA avant fabrication



Experimental CPA map



Simulated CPA map



Plusieurs jours
de mesures et
calcul !

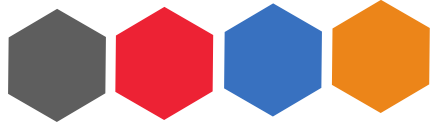
Une journée
de simu et
de calcul !

Observation :

- des courants de 1pA ou 1aA laissent fuir de l'information en simulation à travers $B_z(t)$
- des courants de 1aA sont indiscernables en pratique à travers $B_z(t)$

Absence du bruit de mesure dans les simulations ($SNR = \infty$)

SNR faible en pratique ($0 < SNR < 2$)



Reproduire les attaques SCA avant fabrication

Problème : Introduire le bruit Monte Carlo (impraticable) ?

Solution :

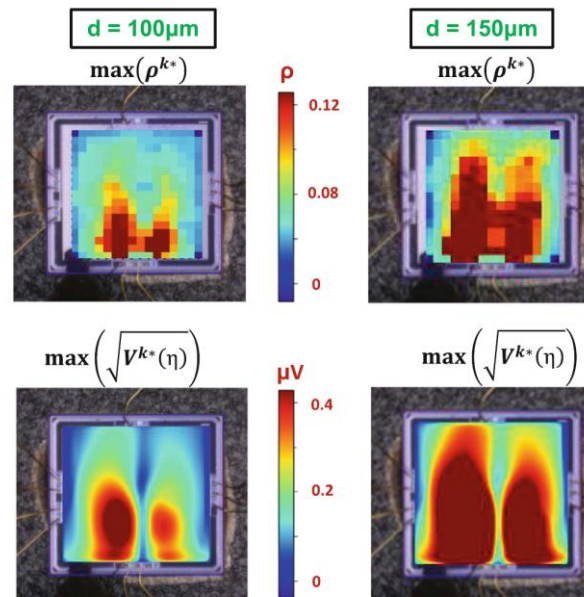
- Calcul de la variance du bruit centré rendant la corrélation non significative
- Calcul du SNR_{min} pour réussir l'attaque CPA :

$$V(\eta) = V(S) \cdot \left\{ \frac{\rho_{simu}^2}{\rho_{crit}^2} - 1 \right\}$$

$$SNR_{min} = \frac{V(S)}{V(\eta)} = \frac{\rho_{crit}^2}{\rho_{simu}^2 - \rho_{crit}^2}$$

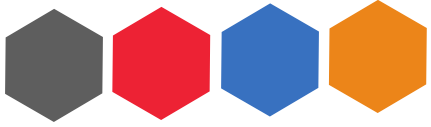
Résultats :

Expérimentations
(36h par cartographie)

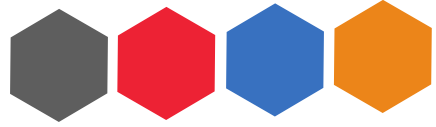


Simulation
(12h de calcul pour les deux
cartographies)



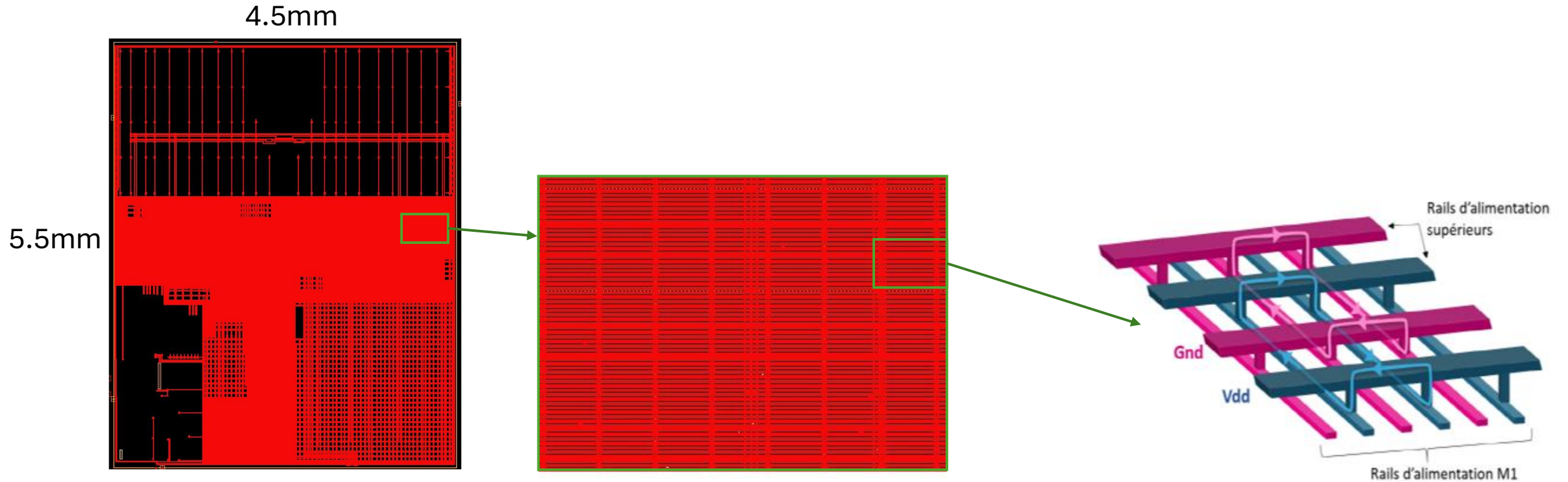


Comment reproduire les attaques EMFI avant fabrication ?

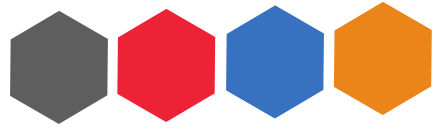


Reproduire les attaques EMFI avant fabrication

Modélisation du couplage EM

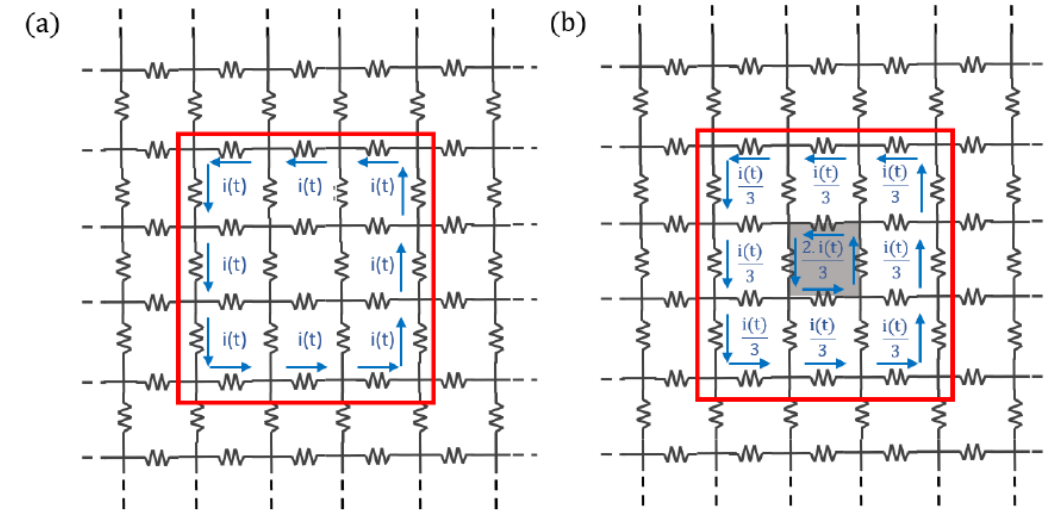
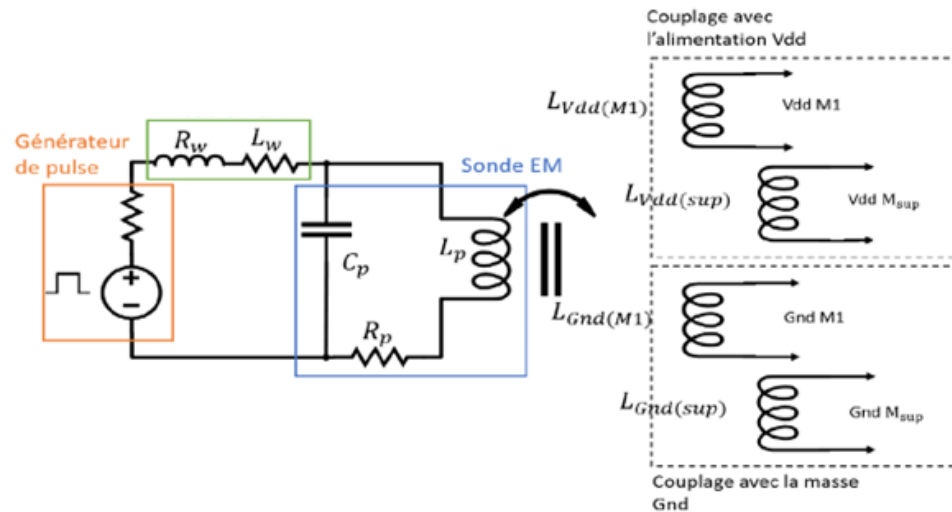


De l'induction magnétique sur des millions de boucles ...
(au passage oublions le couplage électrique ...)



Reproduire les attaques EMFI avant fabrication

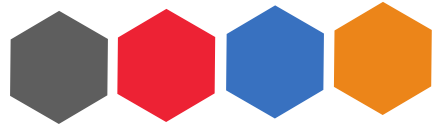
Modélisation du couplage EM



$$f_{em} = -\frac{d\phi}{dt} = -\frac{d}{dt} \iint_S \vec{B} \cdot d\vec{S}$$

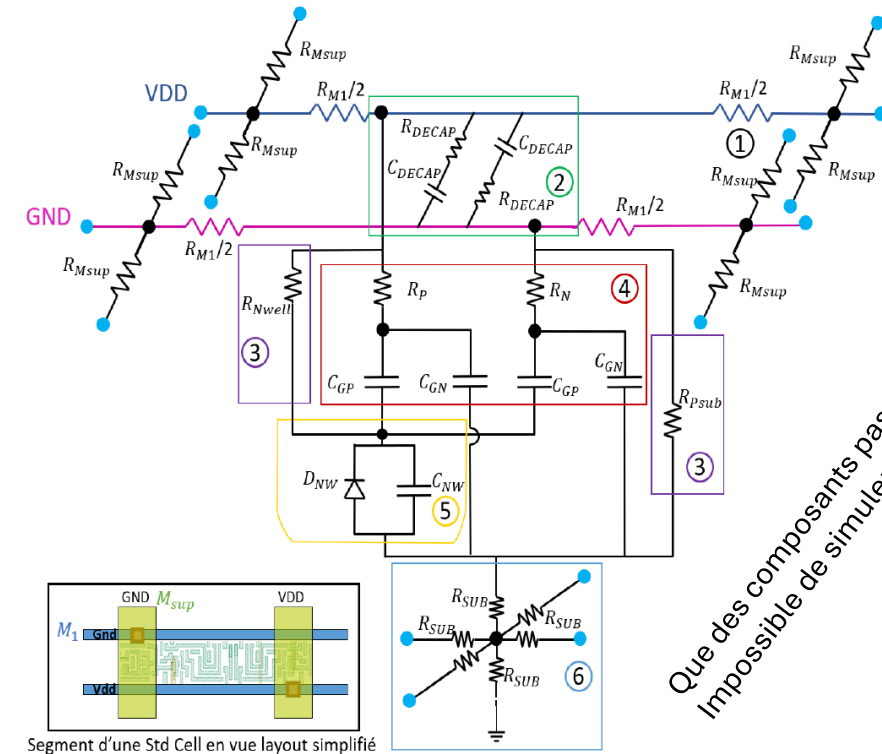
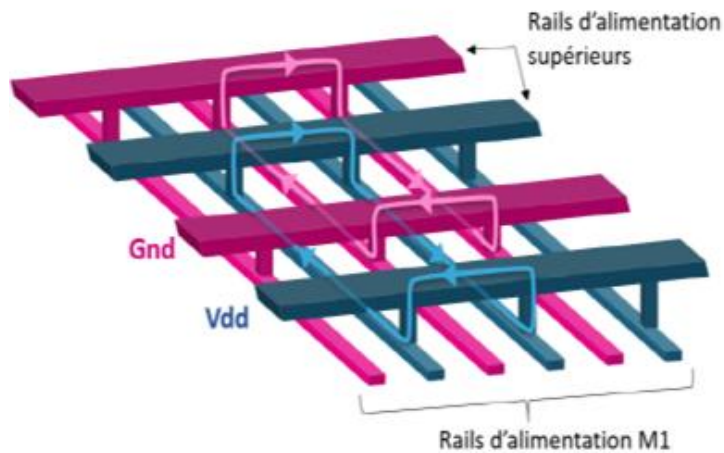


Exploitation de la régularité des réseaux d'alimentation



Reproduire les attaques EMFI avant fabrication

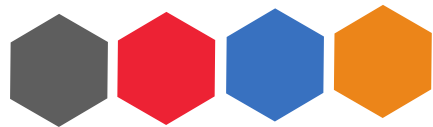
Modélisation du circuit



Que des composants passifs !
Impossible de simuler la réponse de millions de transistors

Oublions les effets non linéaires (réactivité des portes logiques) ... !





Reproduire les attaques EMFI avant fabrication

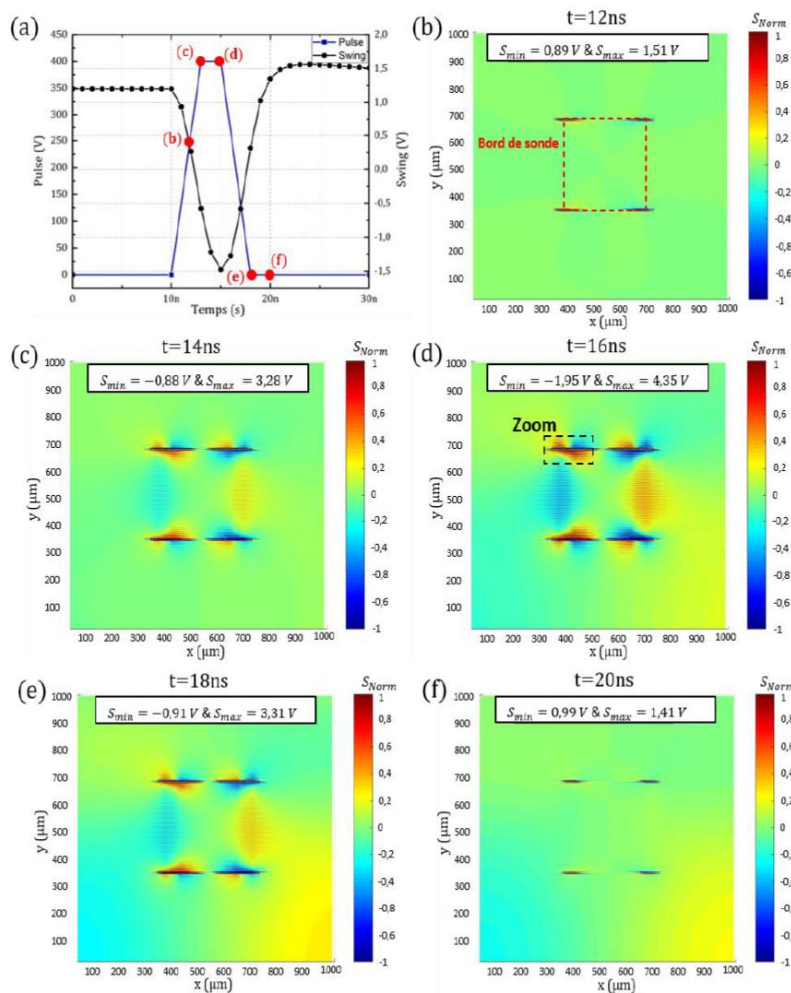


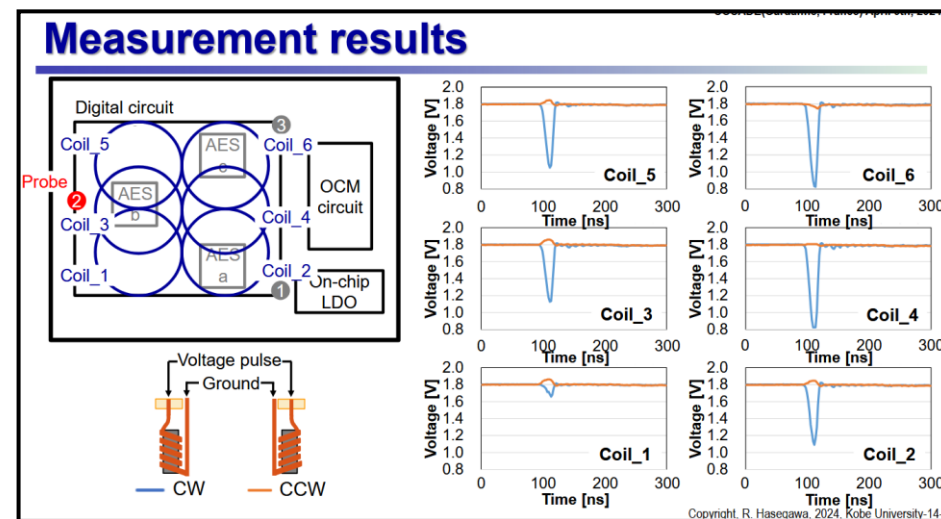
Figure 2.25 - Cartographie de $S(t)_{Norm}$ durant la simulation d'une injection EMFI effectuée avec une sonde proche du circuit et $V_{pulse} = 400V$, $PW = 8ns$ à différents moments t de l'injection.

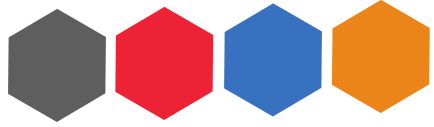


Obtention de cartographies temporisées de la tension d'alimentation interne au sein de circuits

Impulsions de tension très amorties dans le temps et l'espace par le comportement RC du circuit

Expérimentalement confirmé en 2024 par R. Hasegawa, K. Monta, T. Wadatsumi, T. Miki, M. Nagata de l'Université de Kobe

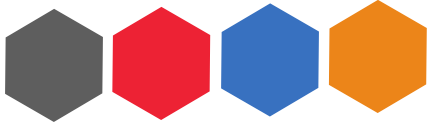


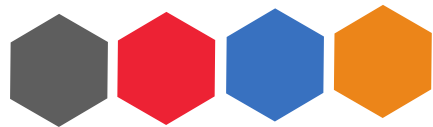


Conclusion

- ❑ Les attaques EM sont dans les usages académiques et industriels répandus
- ❑ Les reproduire avant fabrication est un enjeu pour la conception de CI sécurisés
- ❑ La difficulté est inhérente à la complexité des CI
- ❑ Les 1ères propositions sont donc basées sur :
 - de la physique élémentaire
 - sur des hypothèses simplificatrices (+ ou – fortes)
- ❑ Aller plus loin requiert de multiples compétences et savoir faire

*Au royaume des
aveugles les borgnes
sont rois !*





Reproduire les attaques EMFI avant fabrication

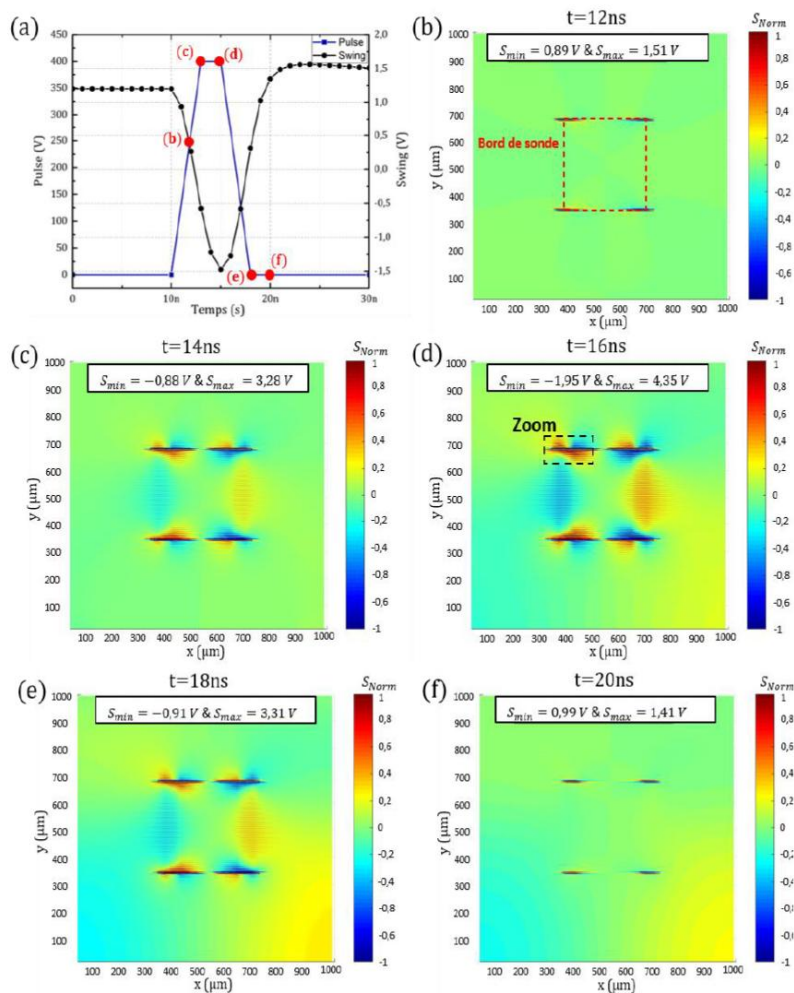


Figure 2.25 - Cartographie de $S(t)_{Norm}$ durant la simulation d'une injection EMFI effectuée avec une sonde proche du circuit et $V_{pulse} = 400V$, $PW = 8ns$ à différents moments t de l'injection.



Obtention de cartographies temporisées de la tension d'alimentation interne au sein de circuits

Effets à proximité des bords de la sonde EM

Impulsions de tension amorties dans le temps et l'espace par le comportement RC du circuit

Retrouve le modèle **sampling fault** déduit jusqu'alors d'observations expérimentales !

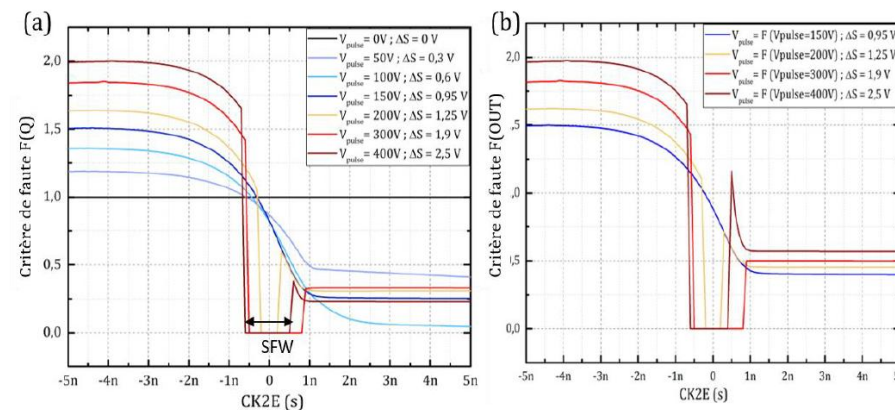


Figure 3.11 - (a) $F(Q)$ et (b) $F(OUT)$ à différentes valeurs de ΔS , dans le cas d'une transition de '0' vers '1'

Reproduire les attaques EMFI avant fabrication

Un peu d'histoire ...

2002 :

Eddy current for Magnetic Analysis with Active Sensor. (eSmart 2002)

J.J. Quisquater, D. Samyde

2007 :

Optical and EM fault-attacks on CRT-based RSA : **Concrete** results. (Conf. Autrichienne)

Jörn-Marc Schmidt, Michael Hutter

2012-2014 :

Techniques for EM fault injection: equipments and experimental results (FDTC 2012)

P. Maurine

Injection of transient faults using electromagnetic pulses Practical results on a cryptographic system (IACR Eprint 2012)

A. Dehbaoui, J.M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria

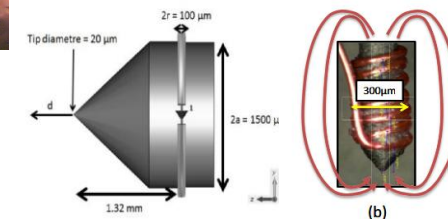
Magnetic microprobe design for em fault attack (EMC Europe 2013)

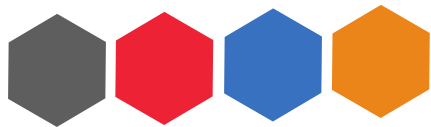
R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau, P. Maurine

2015-2020 :

Commercialisation de systèmes EMFI par Riscure / Keysight (2014) / Langer 2017 / eShard (2020)

2002 – 2025 : L'établissement des plateformes d'injection EM





Reproduire les attaques EMFI avant fabrication

Un peu d'histoire ...

Electromagnetic transient faults injection on a hardware ... (FTDC 2012)

A. Dehbaoui, J. M. Dutertre, B. Robisson, A. Tria

Evidence of a larger EM-induced fault model (CARDIS 2014)

S. Ordas, L. Guillaume-Sage, K. Tobich, J. M. Dutertre, P. Maurine

EM injection: Fault model and locality (FDTC 2015)

S. Ordas, L. Guillaume-Sage, P. Maurine

Electromagnetic fault injection: the curse of flip-flops (JCEN 2017)

S. Ordas, L. Guillaume-Sage, P. Maurine

Electromagnetic fault injection: How faults occur (FDTC 2019)

M. Dumont, M. Lisart, P. Maurine

Employing Dual-complementary Flip-Flops to Detect EMFI Attacks (AsianHost 2018)

C. Deshpande, B. Yuce, L. Nazhandali, P. Schaumont

Inducing local timing fault through EM injection (DAC 2018)

M. Ghodrati, B. Yuce, S. Gujar, C. Deshpande, L. Nazhandali, P. Schaumont

On-chip evaluation of voltage fluctuations and fault occurrence (Cosade 2024)

R. Hasegawa, K. Monta, T. Wadatsumi, T. Miki, M. Nagata

Modeling and Analysis of On-Chip Voltage Fluctuations Caused ... (EMCCompo 2025)

T. Wadatsumi, R. Hasegawa, K. Monta, L. Lin, N. Chang, M. Nagata

Modeling and simulating electromagnetic fault injection (IEEE TCAD 2020)

M. Dumont, M. Lisart, P. Maurine

Fautes de timing

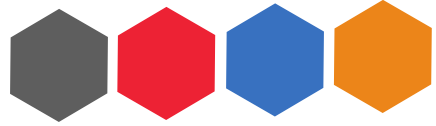
Les fautes de timing n'expliquent pas tout

Le sampling fault model : l'EMFI induit des impulsions locales de la tension interne des CI qui perturbent l'échantillonnage des données par les bascules DFF par altération du signal de données, du signal d'horloge, du signal de reset, set ...

Le clock glitch model & le timing model

Confirmation expérimentale de l'induction d'impulsions locales de la tension interne des CI

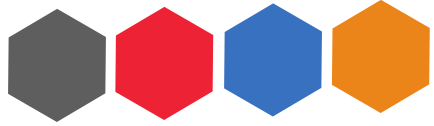
1^{er} pas vers un flot de simulation ?



Reproduire les attaques EMFI avant fabrication



On se lance dans l'aventure en 2007 en partenariat avec STMicroelectronics (FUI CSAFE+)



Reproduire les attaques SCA avant fabrication

Des outils CAD (Redhawk SC, Voltus, ...) de μ Elec permettent d'avoir tous les courants (cycle accurate et bit accurate)



On a les $I(t)$, ça ne devrait pas être trop compliqué d'avoir le $B(t)$!!

On lance dans l'aventure en 2007 en partenariat avec STMicroelectronics (FUI Calisson)

On la relance dans l'aventure en 2019 en partenariat avec STMicroelectronics (ANRT)

Thèses de
Victor Lomne, Davide Poggi

