Lilian Bossuet, Viktor Fischer
Université de Saint-Etienne
Laboratoire Hubert Curien

Journées scientifiques 2013 du projet SEmba
Saint Germain au Mont d'Or, le 5 avril 2013

Cellules oscillantes pour l'authentification physique (PUF) de circuits FPGA

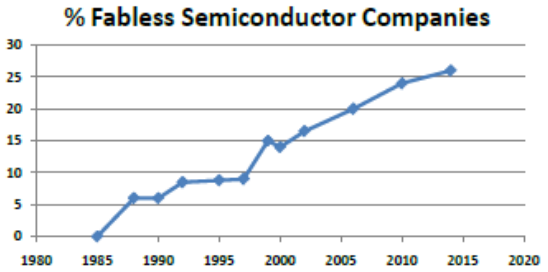
Sommaire

- I. Introduction
  - Le marché des semi-conducteurs
  - Modèle de menaces
- II. Les fonctions non clonables physiquement (PUF)
  - Principe
  - Architectures
  - Comparaison
- III. PUF a cellules oscillantes
  - RO-PUF
  - TERO-PUF
- IV. Conclusion

Situation macro

- Evolution dans l'industrie microélectronique
  - Marché en progression
    - +3.7% en 2011
    - Prévision de 6 à 7% en 2012 (>250 milliards €)
  - Augmentation des coûts de conception des SoC
    - 40% pour le passage 32nm=>28nm (130 M€)
    - Limitée à 30% si wafer 450mm (source ITRS 2011)
    - Investissement du G450c : 4.4 milliards de $
  - Délocalisation (vers l'Asie) de la fab et de la R&D
  - Augmentation du nombre de sociétés Fabless
  - Augmentation de la complexité des SoC et de la valeur ajoutée

Taiwan Semiconductor Manufacturing Co., Ltd.



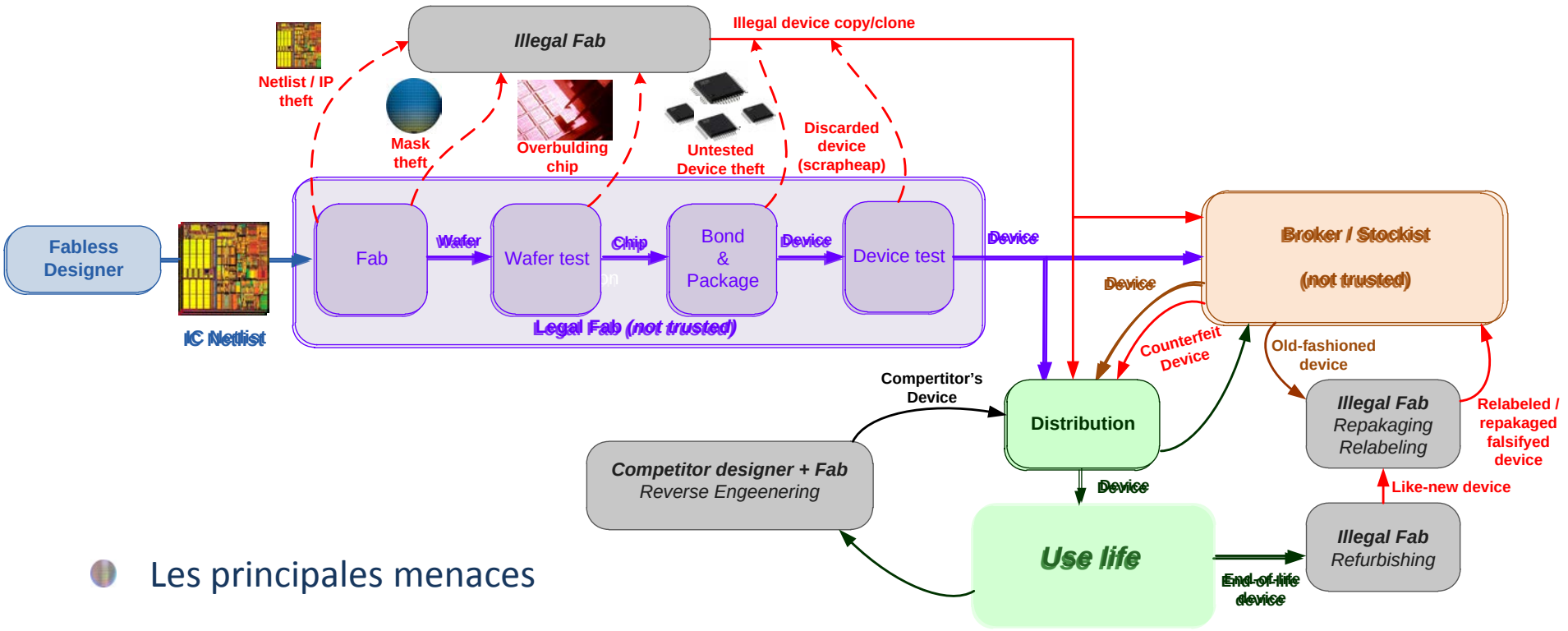
F. Koushanfar 2011

- Caractéristiques propres aux produits contrefaits
  - Produits à très forte valeur ajoutée
  - Obsolescence fonctionnelle rapide des produits électroniques (un nouvel iPhone tout les ans !)
  - Délais de conception longs
  - Outils et circuits bon marché pour le contrefacteur
  - Risques limités pour le contrefacteur

Gravure	Nombre de Transistors	Coûts de conception
130 nm	9 millions	9 millions €
90 nm	16 millions	18 millions €
65 nm	30 millions	46 millions €

Rapport Saunier, 2008

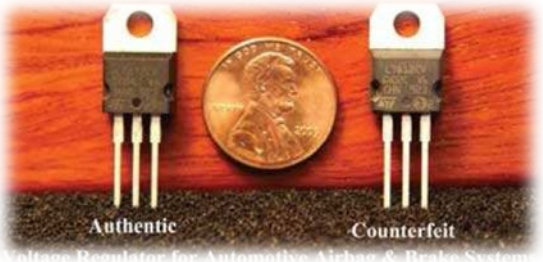
Menaces dans les chaines de fabrication et d'approvisionnement



- Les principales menaces
  - Le vol de propriété intellectuelle
  - Le vol de masques, puces et circuits (*overbuilding*)
  - La copie / le clonage illégal
  - La contrefaçon
  - La rénovation illégale
  - Le reverse engineering
  - La modification de fonctionnalités (déblocage, DRM)

La contrefaçon de produits électroniques

- Les chiffres (???)
  - En 2008 la douane Européenne a saisie 178 million de produits contrefaits (montres, maroquinerie, habits, médicaments, tabac, produits électroniques)
  - Estimation de la contrefaçon à 7% du marché des semi-conducteurs [1]
    - Pertes de 10 milliards de $ par an
  - Entre 2007 et 2010 la douane Américaine a saisie 5.6 million de produits électroniques contrefaits [2]
  - De nombreux cas pour des composants militaires et aéronautiques [3,4]



[1] M. Pecht, S. Tiku. Bogus! Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectrum, May 2006
[2] AGMA, Alliance for Gray Markets and Counterfeit Adatement, http://www.agmaglobal.org
[3] S. Maynard. Trusted Foundry – Be Safe. Be Sure. Be Trusted Trusted Manufacturing of Integrated Circuits for the Department of Defenses. NDIA Manufacturing Division Meeting, October 2010
www.trustedfoundryprogram.or
[4] C. Gorman. Counterfeit Chips on the Rise. IEEE Spectrum, June 2012

La contrefaçon de produits électroniques

- Les conséquences …
  - Pertes de marché (conséquences sociales : perte d'emploies)
  - Insatisfaction des consommateurs et dommage sur l'image de marque
  - Non garantie de sécurité (données / systèmes sensibles)
  - Non garantie de la fiabilité opérationnelle des équipements
  - Coût de diagnostic/réparation
    - Ex: 2.7 million $ pour système de missiles américain
  - Potentielle pollution non maitrisée
  - Sensibilité aux malwares (hardware trojan)

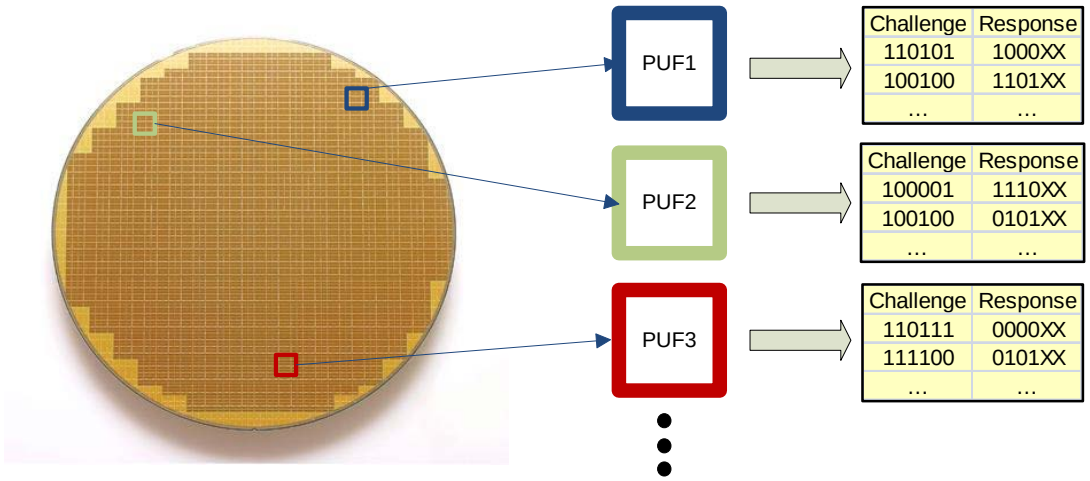
- Il est nécessaire de lutter
  - Projets de recherches mixtes académiques/industriels
  - Support de l'industrie microélectronique
  - Prise de conscience nécessaire du législatif (national/européen)
    - Le U.S. National Defense Authorization Act (NDAA - 2012) spécifie des règles strictes pour les fournisseurs du DoD

Sommaire

- I. Introduction
  - Le marché des semi-conducteurs
  - Modèle de menaces
- II. Les fonctions non clonables physiquement (PUF)
  - Principe
  - Architectures
  - Comparaison
- III. PUF a cellules oscillantes
  - RO-PUF
  - TERO-PUF
- IV. Conclusion

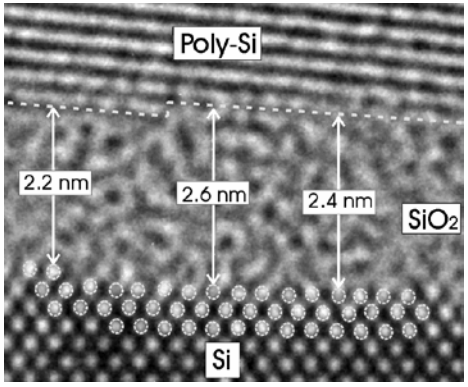
Authentification de circuits intégrés

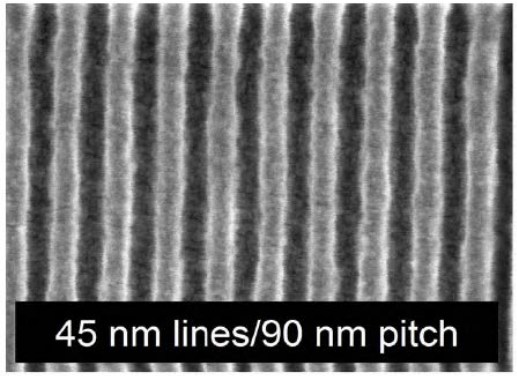
- Silicon Physical Unclonable Function (PUF)
  - Objectif : authentifier de façon sure un circuit intégré par une empreinte digitale microélectronique
  - Concept : extraction de l'entropie liée à la variation de process CMOS (variabilité)
  - Principe : comparer deux éléments physiques théoriquement identiques
  - Fonctionnement : pour une entrée sur N bits (CHALLENGE) le PUF donne une valeur unique et non prévisible sur K bits (REPONSE)



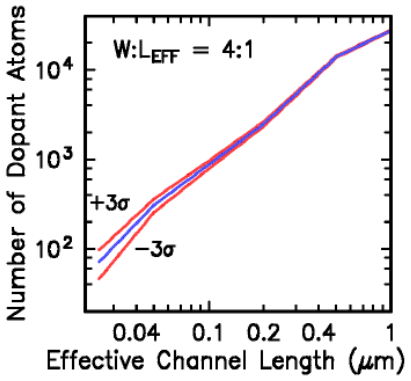
Variabilité du process CMOS

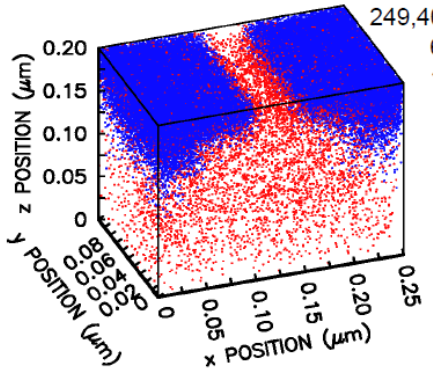
- Quelques exemples de variation
  - Épaisseur d'oxyde
  - Linéarité des métalisations



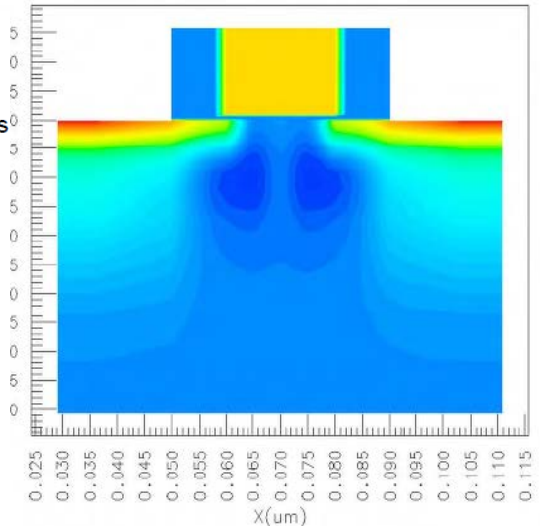


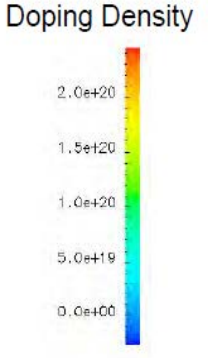
  - Nombre de dopants
  - Densité de dopants
  - Position des dopants





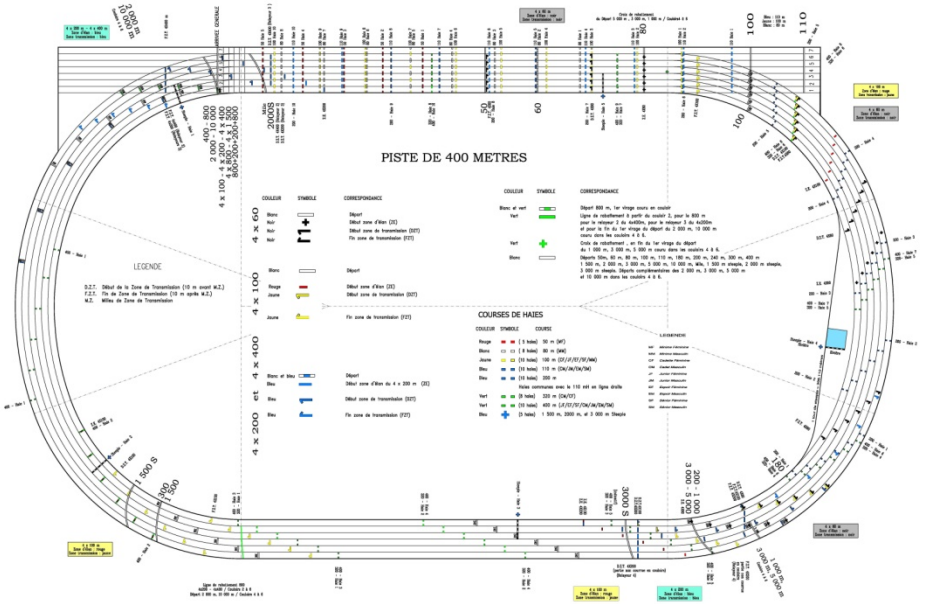
[D. J. Frank, et al., 1999 Symp. VLSI Tech.]





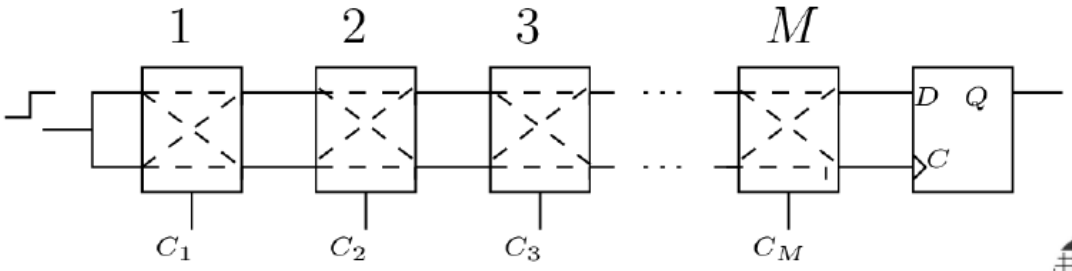
Principe : comparer l'identique !

- On peut considérer qu'il s'agit d'une course
  - Tous les coureurs sont identiques (pas de dopage ;-)) et parcours théoriquement la même distance
  - => On mesure la différence de longueur de pistes
  - Routage identique ou compensation

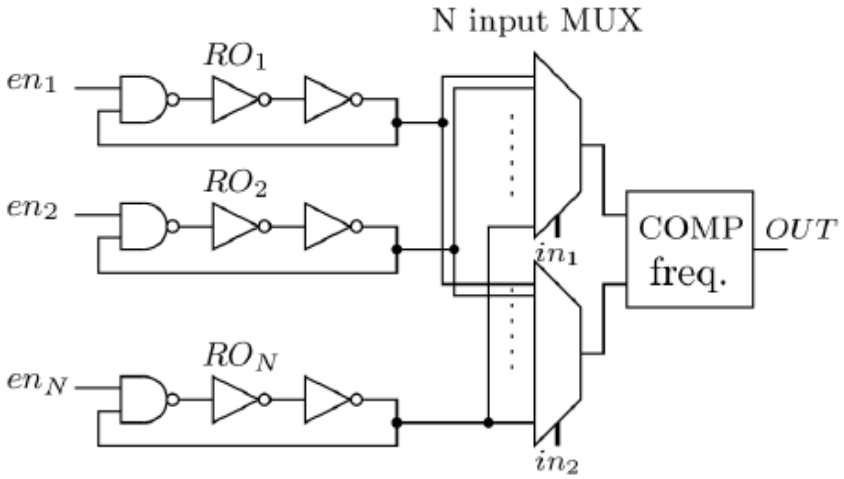


Architectures

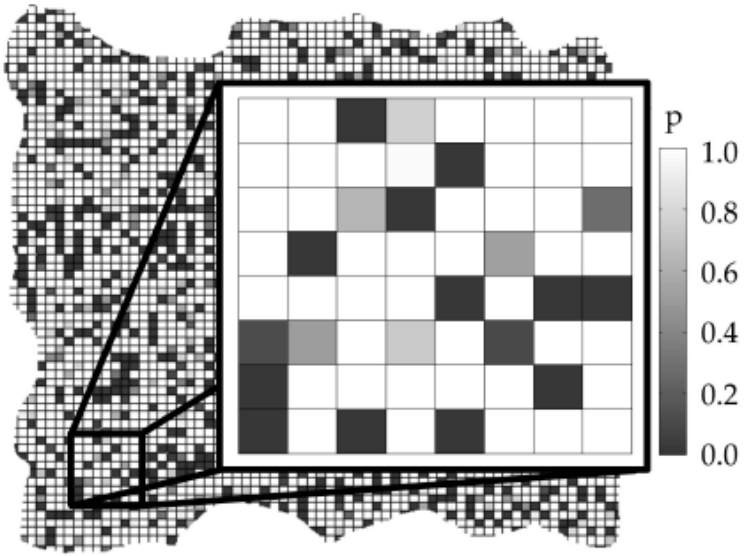
- On peut considérer trois grandes architectures
  - Mesure de la différence de délais – Arbiter PUF
  - Différence de fréquence d'oscillateurs – RO-PUF
  - Stabilité d'un point mémoire à la mise sous tension – SRAM PUF



B. Gassend, D. Lim, D. Clarke, M. Van Dijk, S. Devadas. Identification and authentication of integrated circuits. Concurrency and Computation: Practice & Experience, 16(11):1077-1098, 2004.



G. Edward Suh, S. Devadas. Physical unclonable functions for device authentication and secret key generation. In DAC, pp. 9-14, 2007.



E. Holcomb, W. Burleson, K. Fu. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. IEEE Transations on Computers, Vol. 58, No. 9, 2009.

Rapide comparaison

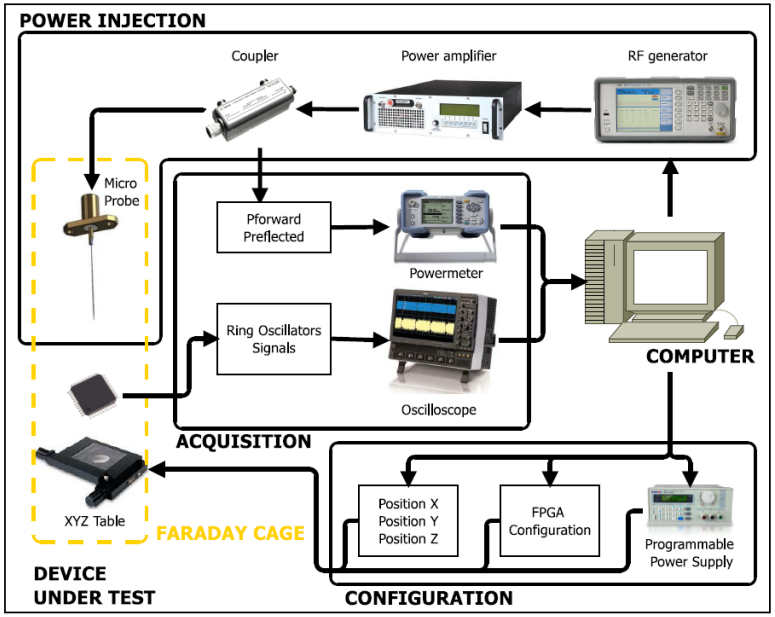
- Arbiter PUF
  - Très stable
  - Challenge long pour un seul bit de réponse
  - Routage très délicat => très très délicat sur FPGA
- RO-PUF
  - Stable (structure différentielle)
  - Facile à concevoir (copier coller de cellules oscillantes)
  - Bien adapté aux FPGA
  - Surface importante et consommation de puissance
- SRAM-PUF
  - Existe en version commerciale (Intrinsec-ID)
  - Structure duale PUF-TRNG
  - Nécessite des SRAM sans forçage (non adaptée aux FPGA)
  - Difficile de prédire les bons bits

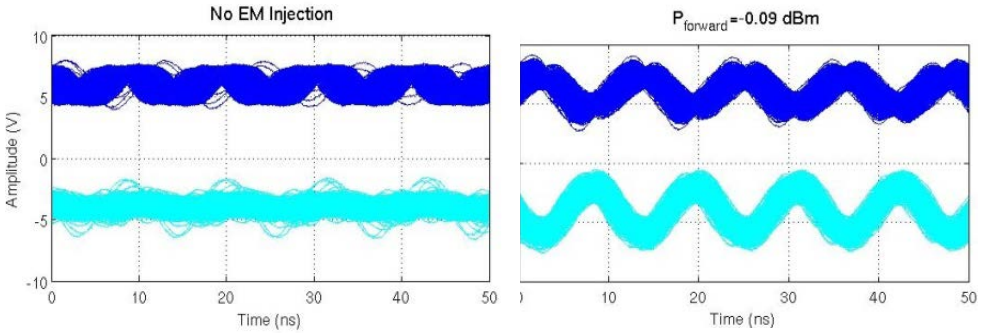
Sommaire

- I. Introduction
  - Le marché des semi-conducteurs
  - Modèle de menaces
- II. Les fonctions non clonables physiquement (PUF)
  - Principe
  - Architectures
  - Comparaison
- III. PUF a cellules oscillantes pour FPGA
  - RO-PUF
  - TERO-PUF
- IV. Conclusion

Les RO-PUF sont-ils les meilleurs candidats pour les FPGA ?

- oui mais …
- En 2010 mise en évidence par l'équipe du LabHC d'un phénomène de verrouillage entre RO
  - Certains RO se mettre à osciller à la fréquence propre d'un des RO de la structure
- En 2012 l'équipe du LabHC publie la 1ère attaque sans contact de structures à base de RO
  - Utilisation du canal électromagnétique pour injecter une fréquence de verrouillage (COSADE 2012) et pour mesurer la fréquence des RO (APEMC 2013)



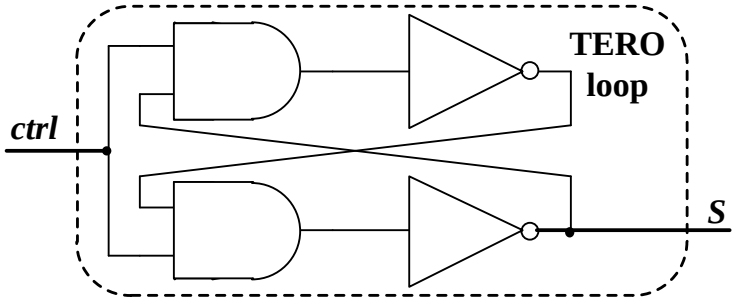


P. Bayon, L. Bossuet et al. Contacless Electromagnetic Active Attack on Ring Oscillator Based true Random Number Generator. Constructive Side Channel Analysis and Secure Design (COSADE 2012), pp. 151-166, 2012.

P. Bayon, L. Bossuet, A. Aubert, V. Fischer. EM radiation analysis on true random number generators: Frequency and localization retrieval method. In Proceedings of the IEEE Asia-Pacific International Symposium and Exhibition on Electromagnetic Compatibility (APEMC 2013),Melbourne, Australia, May 2013.

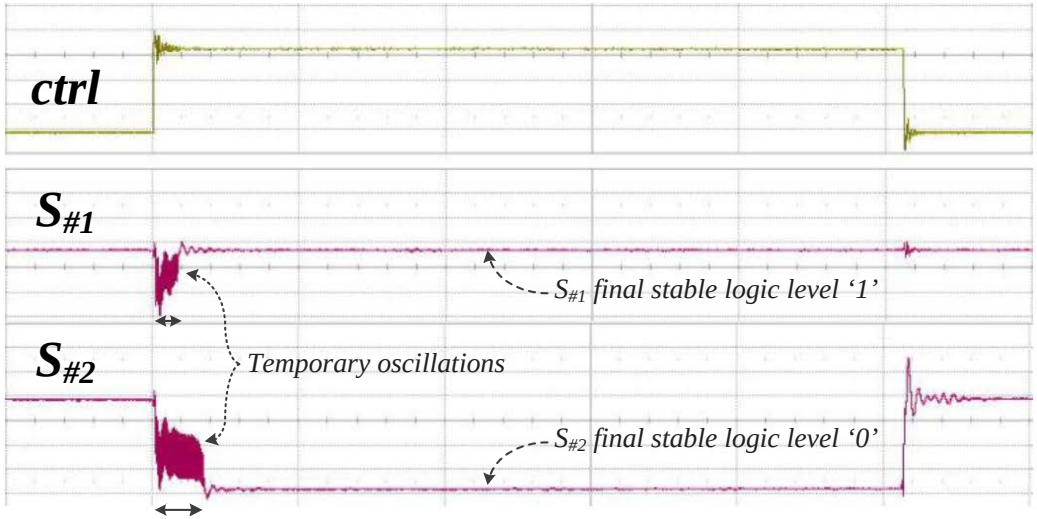
Proposition d'une nouvelle PUF basée sur une cellule temporairement oscillante

- Architecture de la cellule TERO (Trensiant Effect Ring-Oscillator)
  - Cellule simple et symétrique à base de 2 porte ET et 2 inverseurs
  - Mixte entre RO-PUF et SRAM-PUF



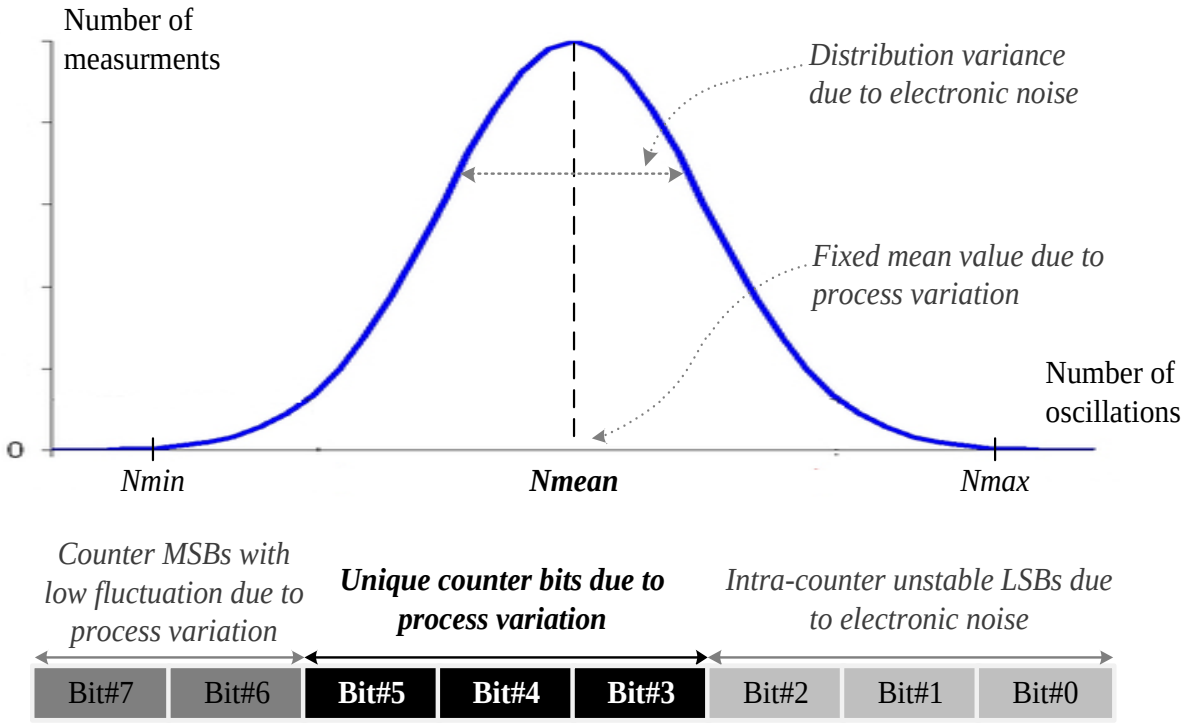
Implementation sur FPGA :
- cible : Altera Cyclone-II
- 1 LAB/TERO, à 300MHz
- 1172 TERO max / Cyclone-II

- Fonctionnement
  - Stable si ctrl ='0'
  - Oscillant après le front montant de ctrl
  - Le nombre d'oscillations dépends de la cellule
  - L'état final dépends de la cellule (biais à '1')
  - Certaines cellules toujours oscillantes (~30 %)



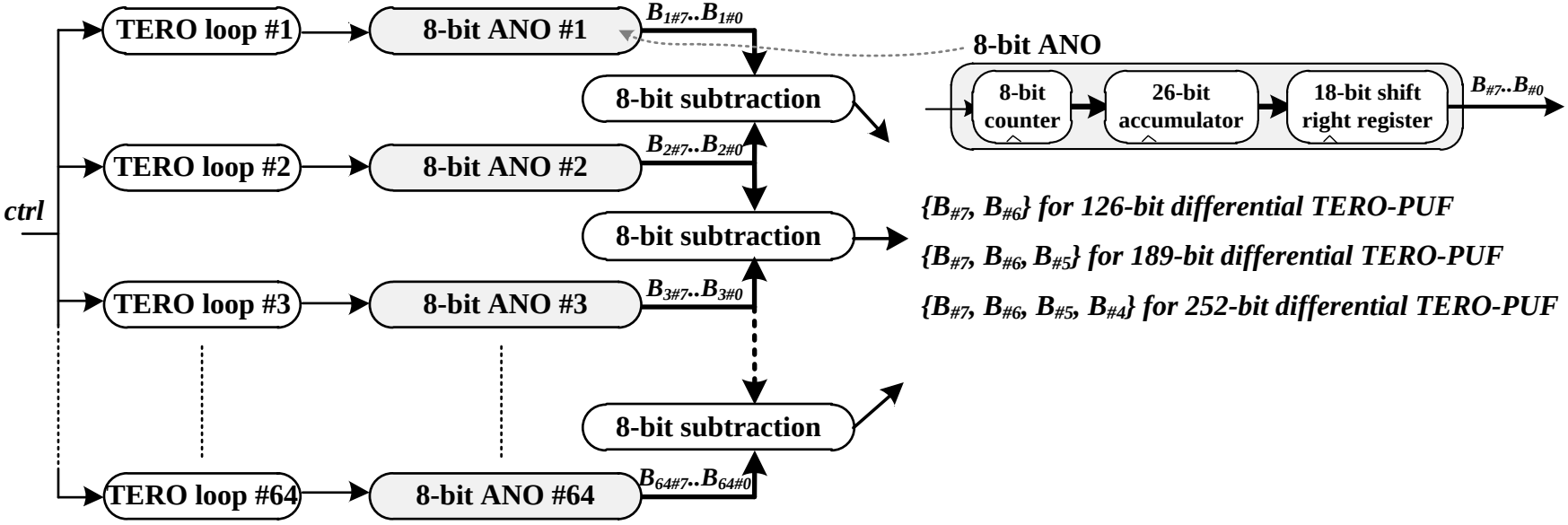
Extraction de l'entropie

- Utilisation du nombre moyen d'oscillations comme extraction de l'entropie venue de la variation du process CMOS
  - 9 cartes ALTERA DE1 => 9* 1 172 = 10 548 TERO testés
  - Pour chaque TEROle nombre d'oscillations est mesuré 2^{18} fois (262 144)
  - Résultat : distribution suivant une loi normal du nombre d'oscillations



Architecture du TERO-PUF

- Structure différentielle
  - Bonne stabilité vis à vis des perturbation externe (T°, rayonnement EM)
  - Très bonne scalabilité
  - Surface importante due aux compteurs
  - La réponse du PUF est obtenue par la différence du nombre d'oscillations entre deux cellules TERO



Comparaison avec l'état de l'art

- Basée sur les données disponibles dans les publications

	Intra-device variation (%)	Inter-device variation (%)	PUF ID size (bits)
Arbiter PUF [Dev08]	3.7-12.5	38	1
RO-PUF [Mai10]	1.0	40	1
SRAM-PUF [Gua10]	3.7-10.5	~50	*Data size*
TERO-PUF	**1.7-2.7**	**48-49**	**126-252**

- Le TERO-PUF donne de bons résultats
  - Stabilité et unicité de la réponse
  - Moins sensible que le RO-PUF
  - Possibilité d'extraire de l'aléa venant du jitter => TRNG

Sommaire

- I. Introduction
  - Le marché des semi-conducteurs
  - Modèle de menaces
- II. Les fonctions non clonables physiquement (PUF)
  - Principe
  - Architectures
  - Comparaison
- III. PUF a cellules oscillantes pour FPGA
  - RO-PUF
  - TERO-PUF
- IV. Conclusion

Conclusion

- Nouveaux challenges pour l'industrie de la microélectronique
  - Réduire (éliminer) le vol, la copie et la contrefaçon de circuits électroniques et d'IP
  - Sécuriser la fabrication des circuits intégrés
  - Embarqués des systèmes d'auto-protection (activation à distance)
  - Nécessité d'authentifier physiquement un circuit parmi N

- Les fonctions physiquement non clonables sont des systèmes intéressants
  - Plusieurs architectures disponibles
  - Les cellules oscillantes sont plus efficaces et stables sur FPGA
  - Mais les oscillateurs en anneaux sont sensibles à des perturbations thermiques et électromagnétiques

- Le TERO-PUF apparait que une nouvelle solution pour FPGA
  - Entre le RO-PUF et le SRAM-PUF
  - Possibilité de développer une structure duale PUF-TRNG

Lilian Bossuet, Viktor Fischer
Université de Saint-Etienne
Laboratoire Hubert Curien

Journées scientifiques 2013 du projet SEmba

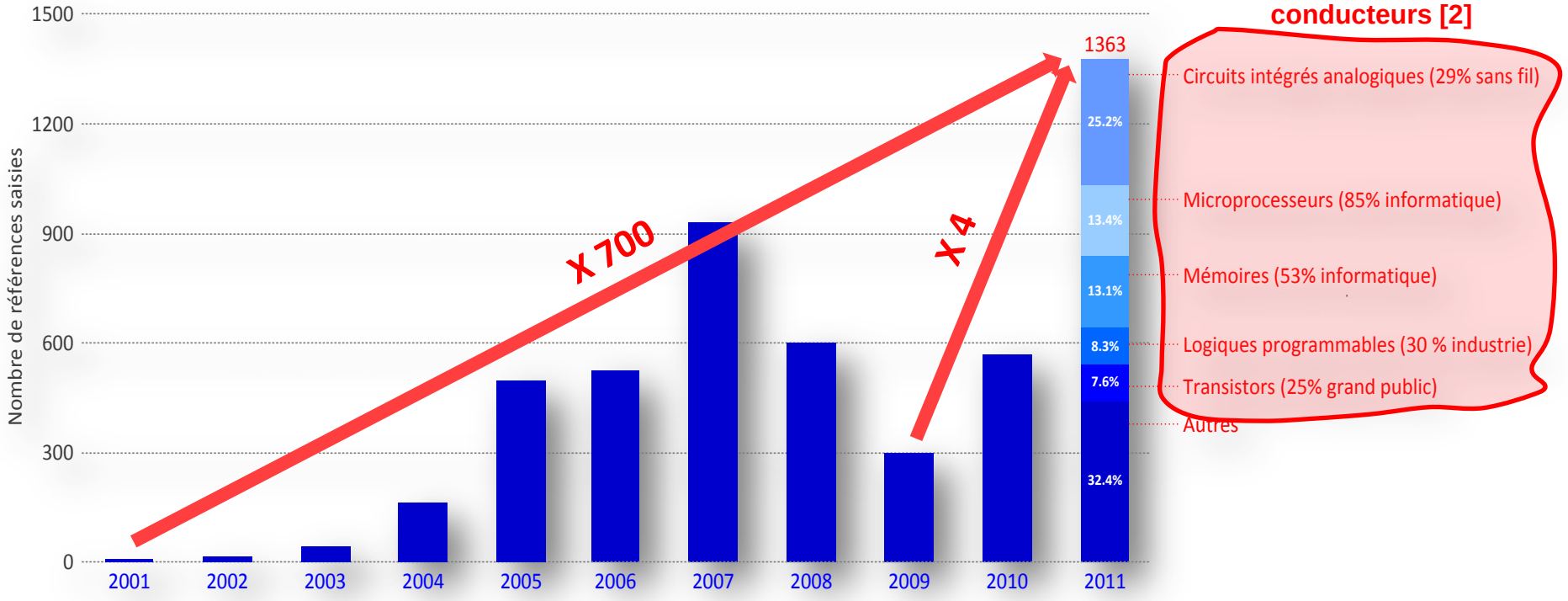
Saint Germain au Mont d'Or, le 5 avril 2013

Cellules oscillantes pour l'authentification physique (PUF) de circuits FPGA

Evolution de la contrefaçon de circuits intégrés

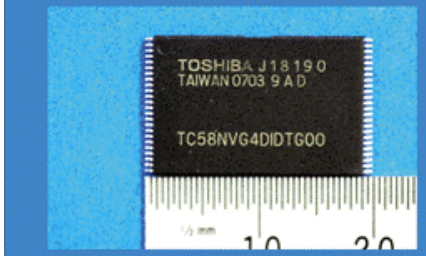
- Evolution de la contrefaçon et cibles
  - Recensement USA
    - Estimation : « pour 1 contrefaçon signalée => 35 non signalées» [1]

Représente un marché de 137 milliards de € / 250 milliards du marché des semi-conducteurs [2]



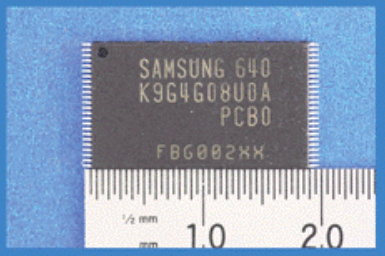
[1] C. Gorman. Counterfeit Chips on the Rise. IEEE Spectrum, June 2012
[2] IHS-ERAI http://www.ihs.com/info/sc/a/combating-counterfeits/index.aspx

Exemple de contrefaçon

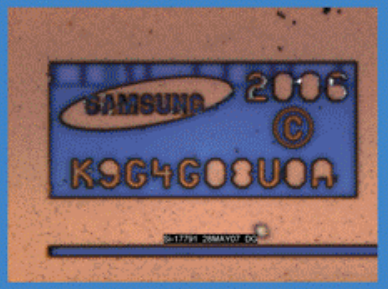


Counterfeit Toshiba Part Package Marking TC58NVG4D1DTG00

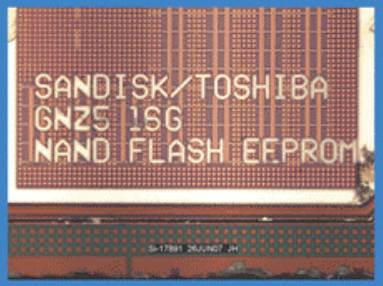
Toshiba 56nm 16Gb MLC NAND Flash Part Package Marking TC58NVG4D1DTG00



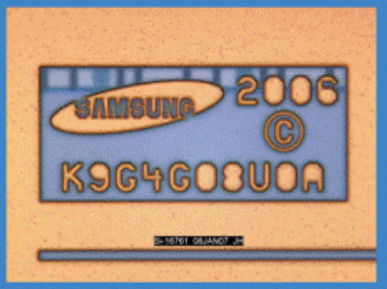
Samsung 65nm 4Gb MLC NAND Flash Part Package Marking K9G4G08U0A



Counterfeit Toshiba Part Die Markings



Toshiba 56nm 16Gb MLC NAND Flash Part Die Markings



Samsung 65nm 4Gb MLC NAND Flash Die Markings

One counterfeit device (left) had Toshiba markings but a Samsung die inside. You can see the actual Toshiba device markings on the second device. The Samsung die can be seen in the third image.

Source : EE Times, August 2007