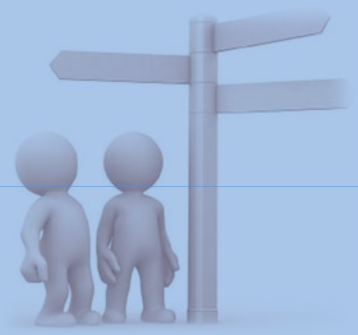
Lilian Bossuet
Université de Saint-Etienne
Laboratoire Hubert Curien

GDR SoC-SiP – Journée « Sécurité des systèmes embarqués »
Contrefaçons, PUF et Trojans
Paris, le 27 novembre 2012

Sécurité de la conception et protection de la propriété intellectuelle – état de l'art

Lutte contre le vol, la copie illégale, le reverse-engineering et la contrefaçon de circuits intégrés

Sommaire

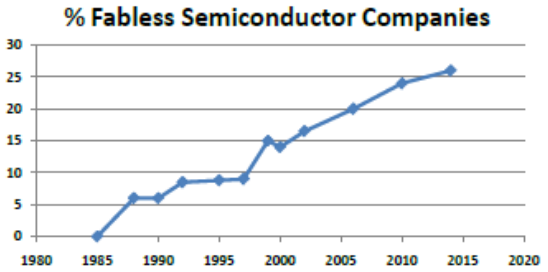


- I. Introduction
  - Le marché des semi-conducteurs
  - Modèle de menaces
- II. Les contre-mesures passives
  - L'authentification
  - Le watermarking
  - La détection de recyclage
  - L'obfuscation
- III. Les contre-mesures actives
  - Activation de circuits intégrés
  - Chiffrement de la logique
  - Obfuscation /chiffrement de FSM
  - Chiffrement de routage
  - Chiffrement de configuration (FPGA)
  - Blocage fonctionnel
- IV. Conclusions
  - SalWare vs MalWare
  - Perspectives

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.



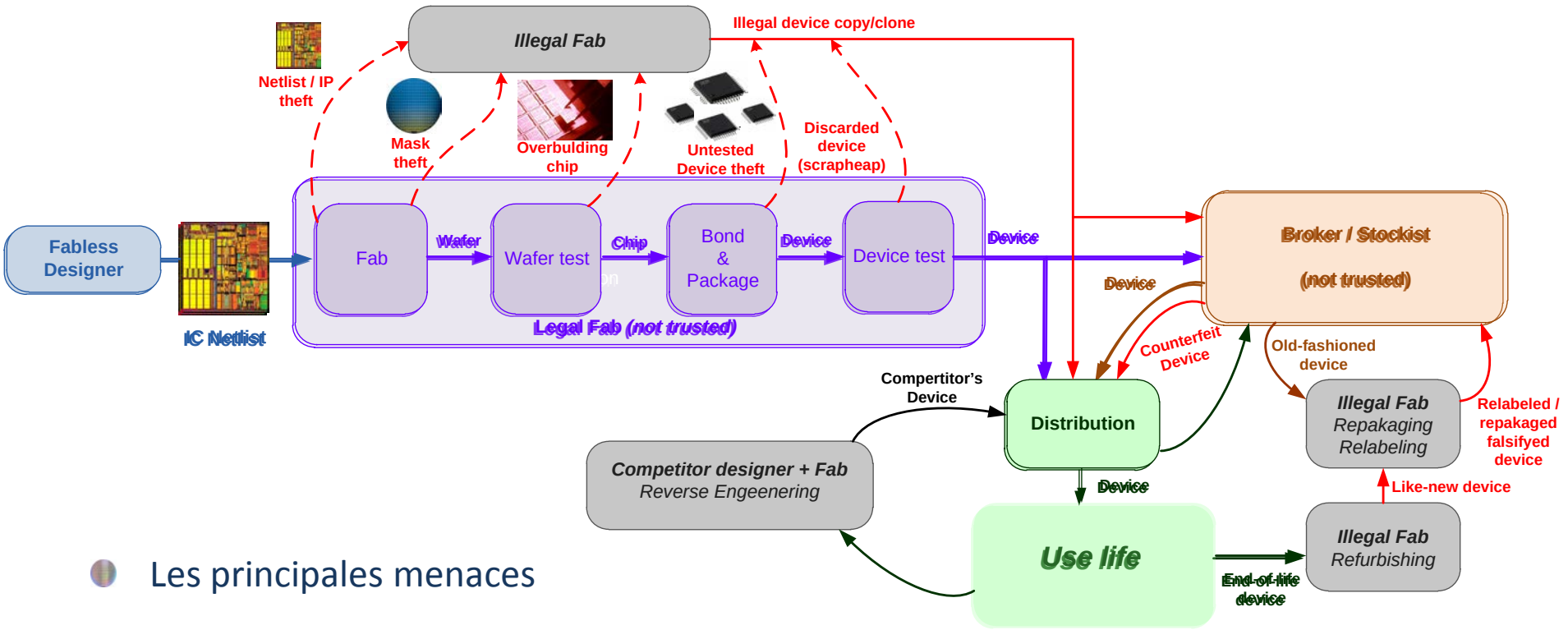
F. Koushanfar 2011

- 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

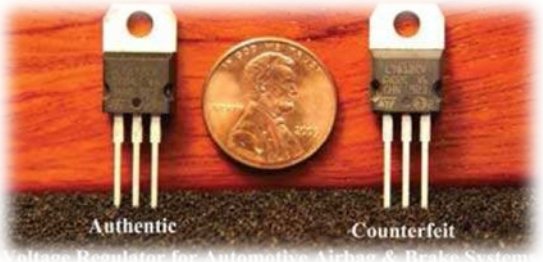
Menaces dans les chaines de fabrication et d'approvisionnement



- 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 (???)
  - Estimation de la contrefaçon à 10 % du marché mondiale
    - Coût : 200 milliards de $ par an aux USA
    - Impact : 250 000 emplois perdu par an aux USA
  - 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]

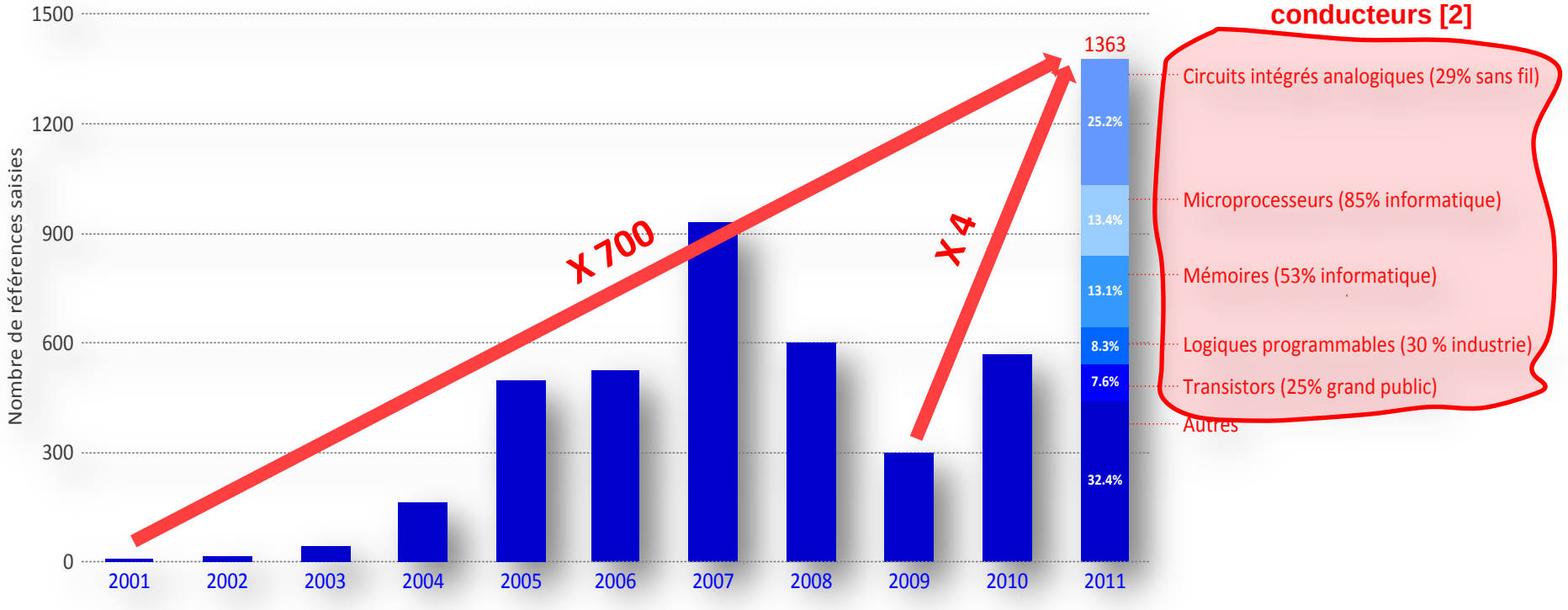


[1] M. Pecht, S. Tiku. Bogus! Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectrum, May 2006
[2] AGMA, Alliance for Gray Markets and Counterfeit Adatement, http://www.agmaglobal.org
[3] S. Maynard. Trusted Foundry – Be Safe. Be Sure. Be Trusted Trusted 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

Evolution de la contrefaçon de circuits intégrés

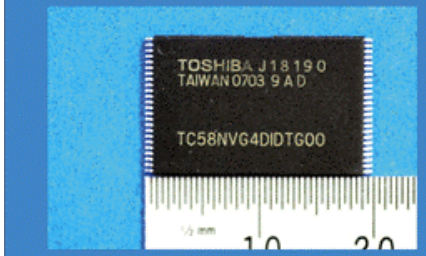
- Evolution de la contrefaçon et cibles
  - Recensement USA
    - Estimation : « pour 1 contrefaçon signalée => 35 non signalées» [1]

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



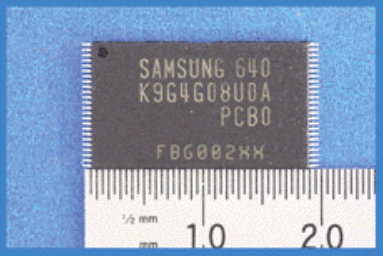
[1] C. Gorman. Counterfeit Chips on the Rise. IEEE Spectrum, June 2012
[2] IHS-ERAI http://www.ihs.com/info/sc/a/combating-counterfeits/index.aspx

Exemple de contrefaçon

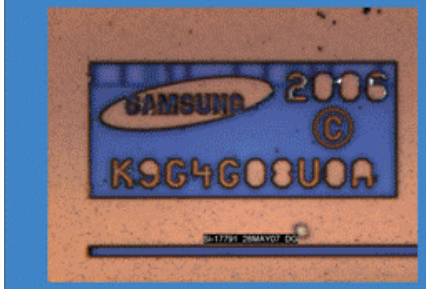


Counterfeit Toshiba Part
Package Marking
TC58NVG4D1DTG00

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

Quelques faits marquants

- Fausse usine NEC
  - Découverte en 2006 [1,2]
  - 50 références de produits
    - Home-cinéma, lecteur MP3, lecteur de DVD, clavier d'ordinateur …

- VisonTech (USA)
  - De 2006 à 2010 ce courtier américain à vendu plus de 60 000 contrefaçons de circuits intégrés [3]
  - Parmi ses clients : US Navy, Raytheon Missile System …

Advanced Micro Devices	$34,900.00
Altera	$7,611.00
Analog Devices	$75,580.66
Cypress Semiconductor	$33,446.00
Freescale	$40,021.00
Infineon Technologies	$10,036.00
Intel	$100,889.50
Intersil	$1,857.30
Linear Technology	$32,018.75
Maxim	$1,596.34
Mitel	$2,645.93
National Semiconductor	$5,943.80
NEC	$24,842.07
Peregrine Semiconductor	$2,640.00
Philips Electronics	$1,639.50
Renesas	$2,400.00
Samsung Electronics America	$77,165.00
STMicroelectronics	$18,619.21
Texas Instruments	$92,899.58
Toshiba	$2,424.00
Xilinx	$22,235.76
Total	$591,411.40

[1] Next Step for Counterfeiters: Faking the Whole Compagny, New York Times, May 2006 http://www.nytimes.com/2006/05/01/technology/01pirate.html?pagewanted=all
[2] Fake NEC compagny, says report, EE Times, April 2006 http://www.eetimes.com/electronics-news/4060352/Fake-NEC-company-found-says-report
[3] http://eetimes.com/electronics-news/4229964/Chip-counterfeiting-case-exposes-defense-supply-chain-flaw

La contrefaçon de produits électroniques

- Les conséquences …
  - Pertes de marchés (conséquences sociales : pertes d'emplois)
  - 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)

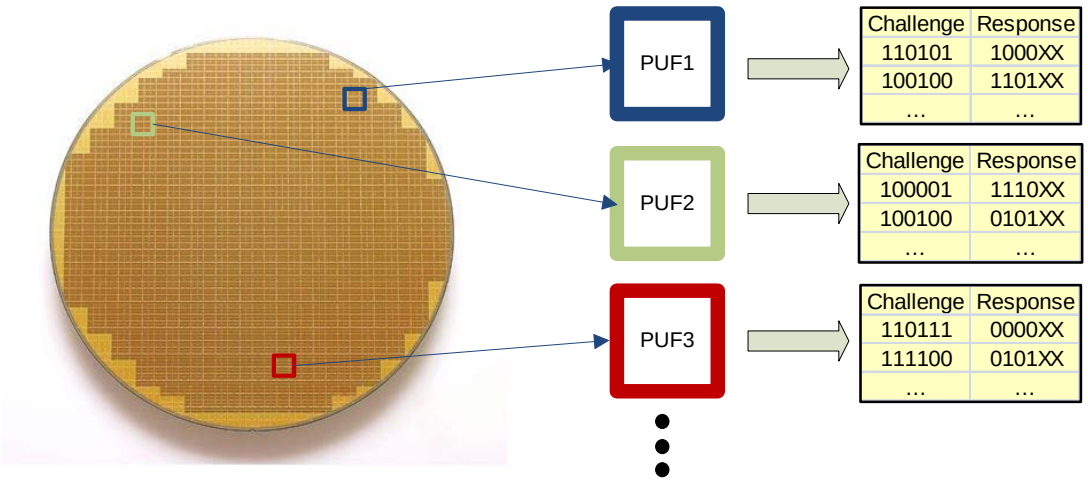
- Il est nécessaire de lutter
  - Projets mixtes académiques/industriels
  - Support de l'industrie microélectronique
  - Prise de conscience nécessaire du législatif (national/européen)
    - Le U.S. National Defense Authorization Act (NDAA - 2012) spécifie des règles strictes pour les fournisseurs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

Sommaire

- I. Introduction
  - Le marché des semi-conducteurs
  - Modèle de menaces
- II. Les contre-mesures passives
  - L'authentification
  - Le watermarking
  - La détection de recyclage
  - L'obfuscation
- III. Les contre-mesures actives
  - Activation de circuits intégrés
  - Chiffrement de la logique
  - Obfuscation /chiffrement de FSM
  - Chiffrement de routage
  - Chiffrement de configuration (FPGA)
  - Blocage fonctionnel
- IV. Conclusions
  - SalWare vs MalWare
  - Perspectives

Authentification de circuits intégrés

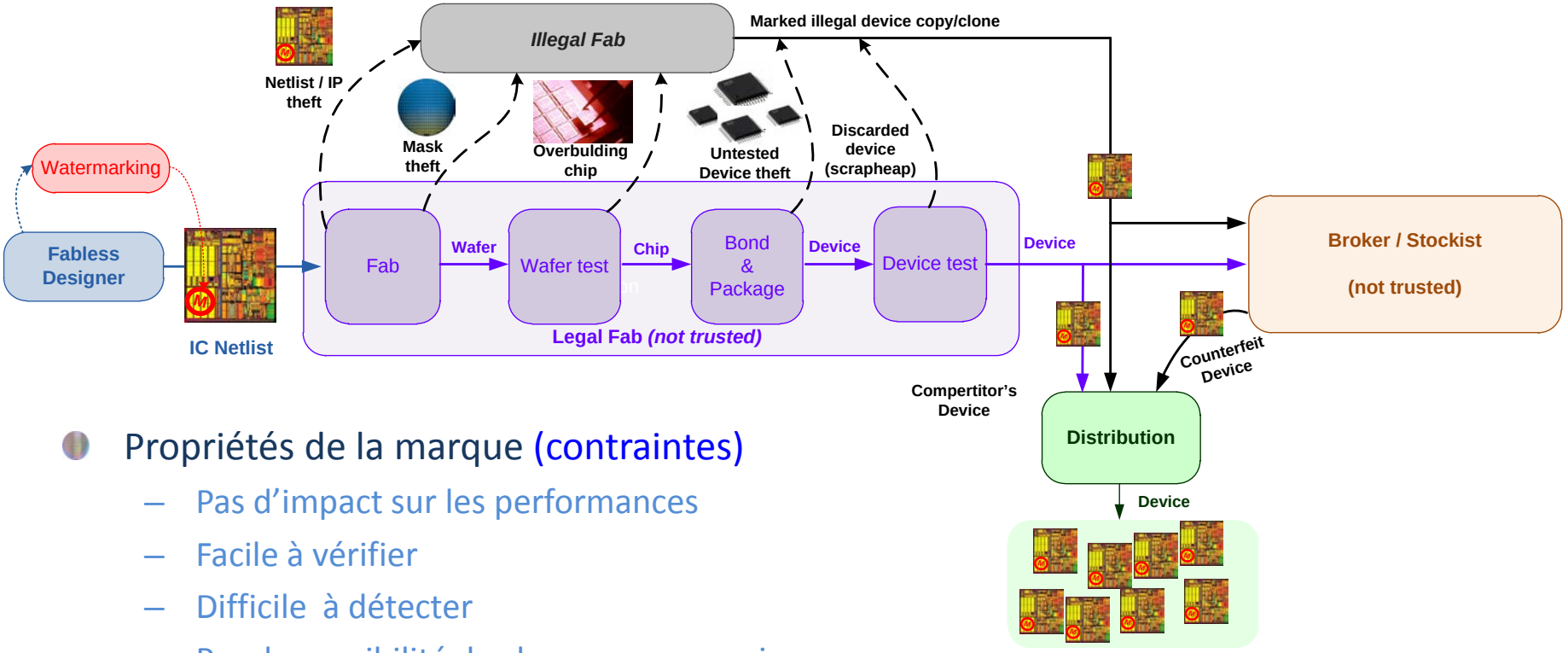
- Silicon Physical Unclonable Function (PUF)
  - Objectif : authentifier de façon sure un circuit intégré comme une empreinte digitale
  - Concept : utilisation du bruit lié à la variation de process CMOS (variabilité)
  - Fonctionnement : pour une entrée sur N bits (CHALLENGE) le PUF donne une valeur unique et non prévisible sur K bits (REPONSE)



- Voir la présentation de Jean-Luc Danger
  - Journée sécurité des systèmes embarqués du GDR SoC-SiP, 27/11/2012

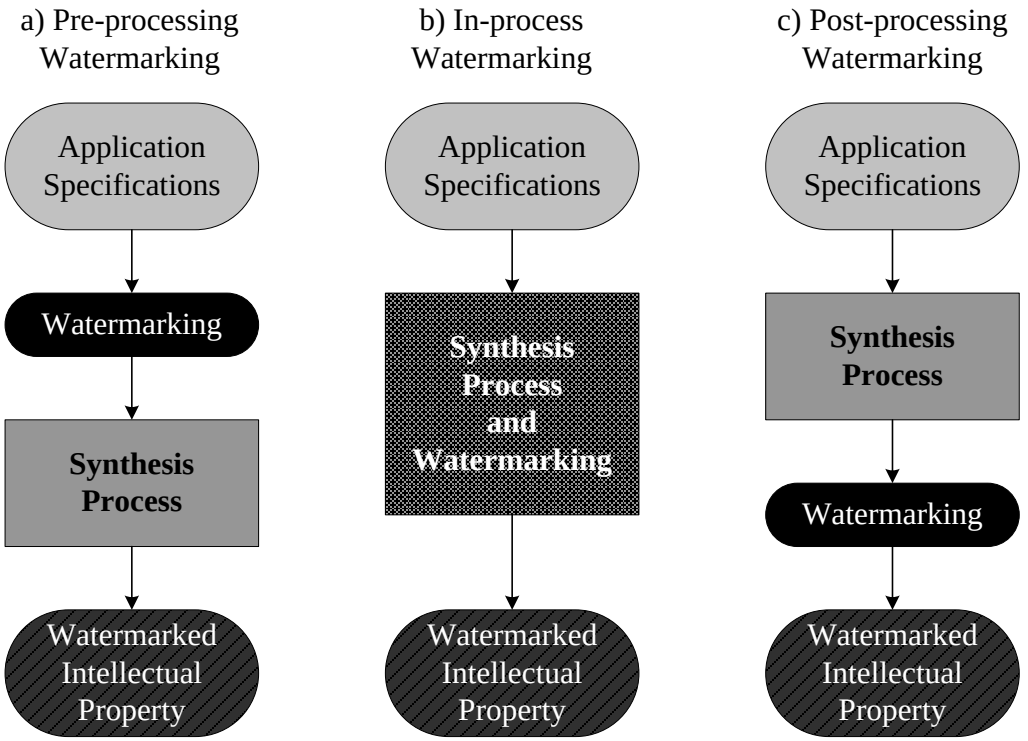
Détection de copie par marquage (watermarking)

- La contrefaçon peut intervenir lors de la conception
  - Objectif : détecter un vol ou une copie de silicium (IP / circuit intégré)
  - Idée : insérer une marque lors du développement



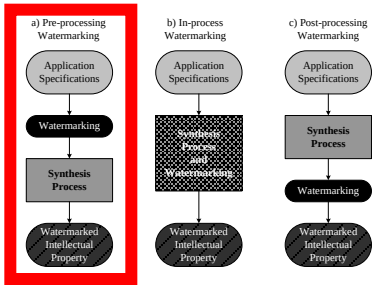
- Propriétés de la marque (contraintes)
  - Pas d'impact sur les performances
  - Facile à vérifier
  - Difficile à détecter
  - Pas de possibilité de changer ou supprimer
  - Information suffisante
  - Surcoûts faibles (surface, power etc..)

Trois niveaux de watermaking dans un flot de conception matériel



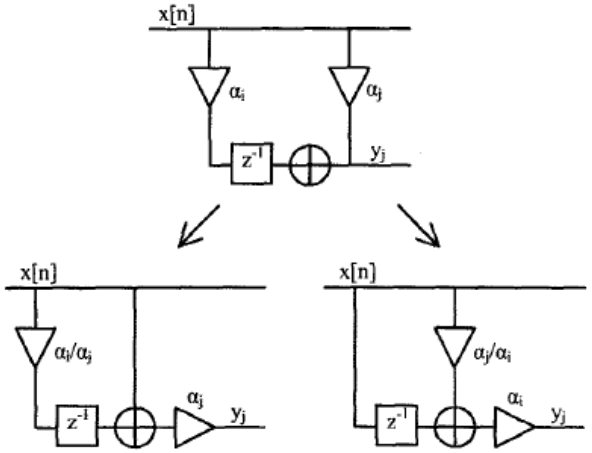
B. Le Gal, L. Bossuet. *Automatic low-cost IP watermarking technique based on output mark insertion*. Design Automation for Embedded System, Springer, 2012

Au niveau algorithme



- Il s'agit de modifier légèrement l'application au niveau de l'algorithme pour la marquer
  - Particulièrement adapté aux applications du traitement du signal (modification des coefficients)
  - Marquage facile mais détection difficile

- Il peut y avoir de légères modifications de l'architecture



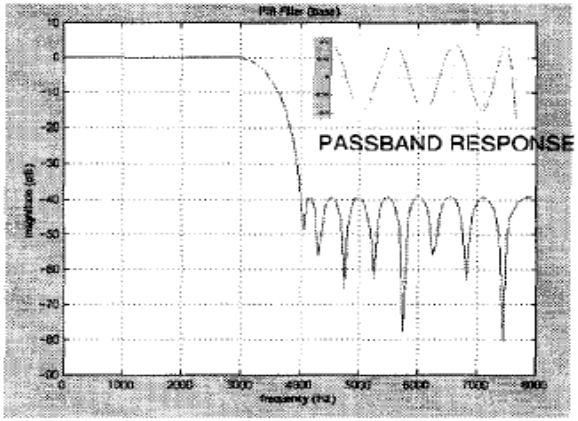


Fig. 4 31-tap non-watermarked filter

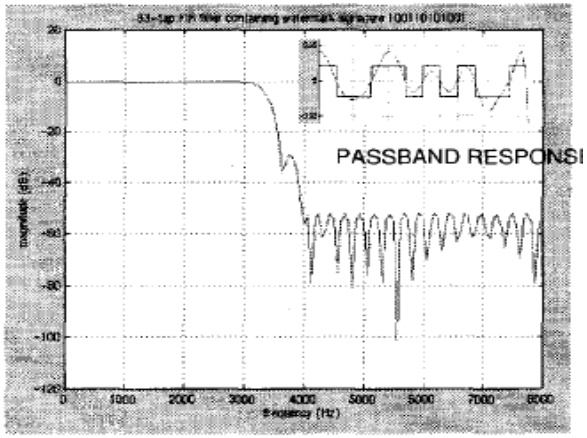
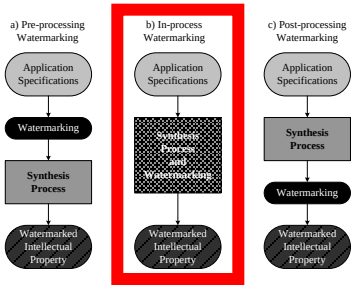


Fig. 5 63-tap watermarked filter

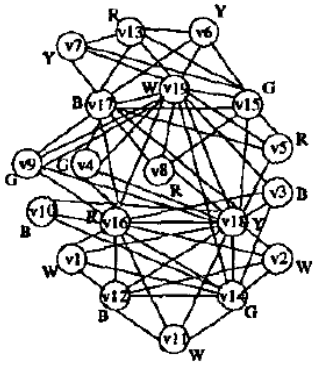
A. Rashid, J. Asher, W.H. Mangione-Smith, M. Potkonjak. *Hierarchical Watermarking for Protection of DSP Filter Cores*. In Proc. IEEE custom Integrated Circuits Conference, 1999

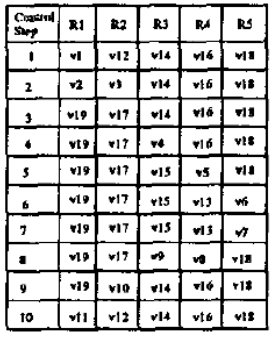
Au niveau synthèse

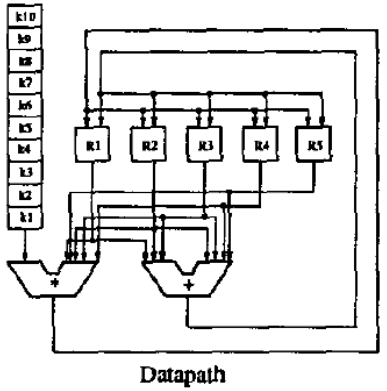


- Modification du graphe de l'algorithme lors de la synthèse comportementale de haut niveau
  - Méthode pré-synthèse comportementale
  - Ajout d'arcs dans un graph
  - Marque dans registre d'allocation
  - Réduction des optimisations dues à la synthèse

F. Koushanfar, I. Hong,M. Potkonjak, *Behavioral synthesis techniques for intellectual property protection", ACM Transactions on Design Automation of Electronic* Systems 10/3, 2005, 523–545.

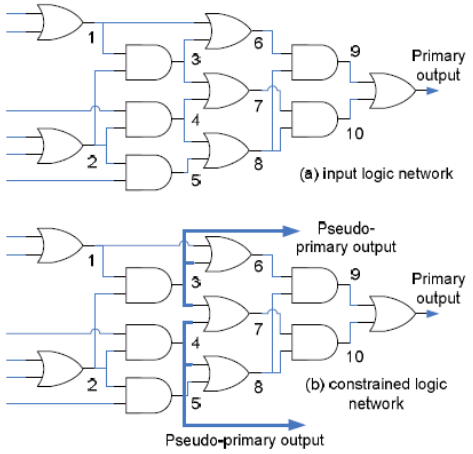




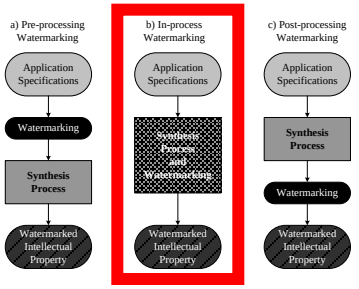


- Modification de l'étape de synthèse logique
  - Méthode post-synthèse logique
  - Certaines sorties de portes logiques sont choisies aléatoirement et envoyées vers une logique additionnelle non fonctionnelle (*dummy logic*)
  - Facilement détectable, surcoût logique

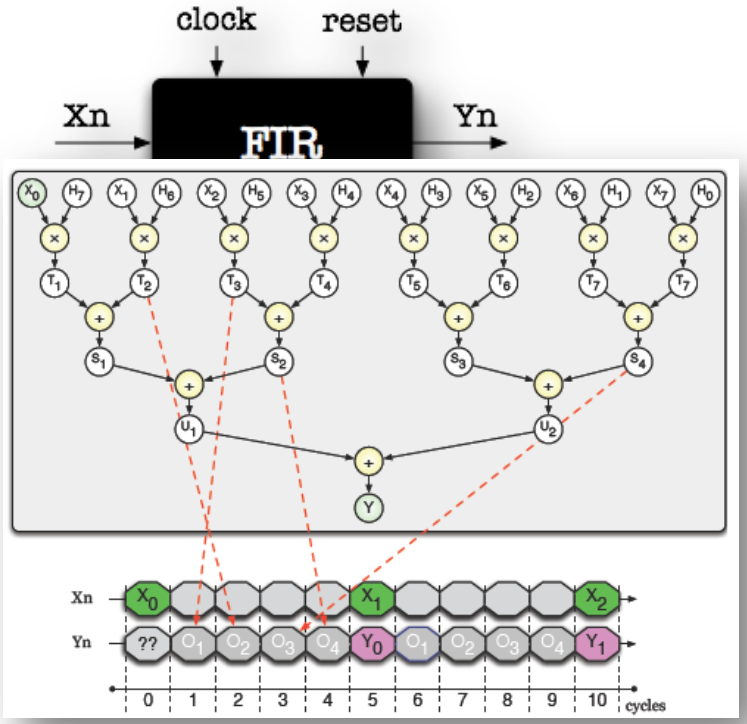
D. Kirovski, Y. Hwang, M. Potkonjak, J. Cong. *Intellectual property protection by watermarking conditional logic synthesis solutions*. In International Conference of Computer Aided Design, 1998,pp. 194-198,

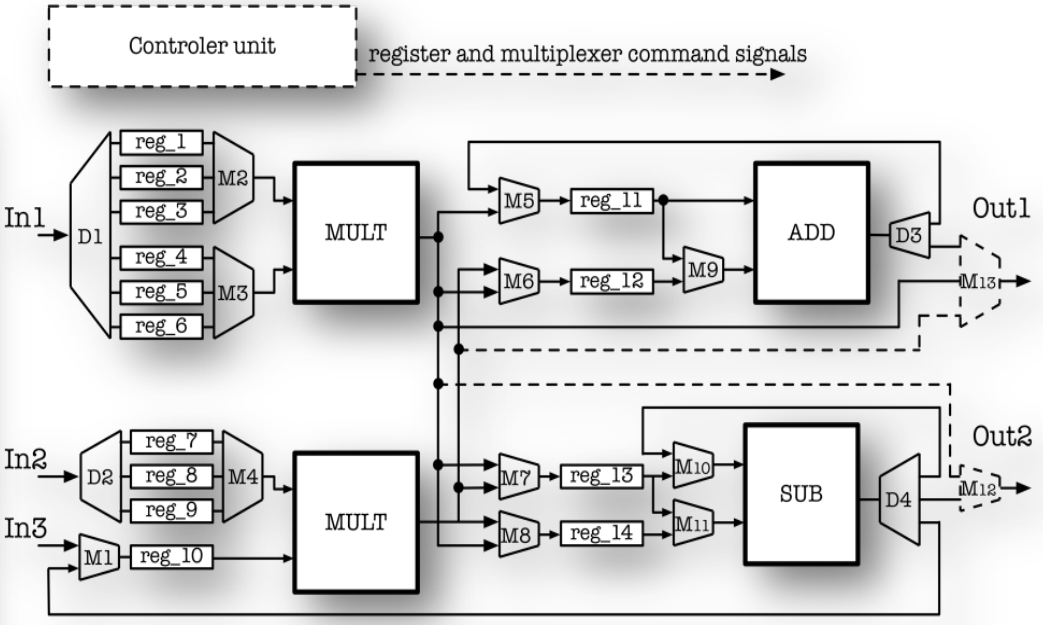


Au niveau synthèse



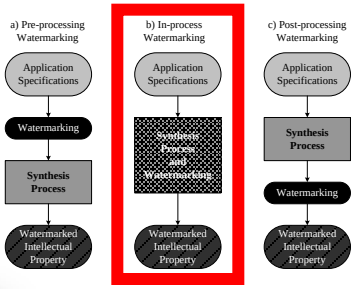
- Insertion une marque à très bas coût dans un IP de traitement du signal
  - Idée : créer automatiquement une marque sous forme de fonctions mathématiques dont les résultats s'insèrent dans les valeurs de sortie aux instants propices





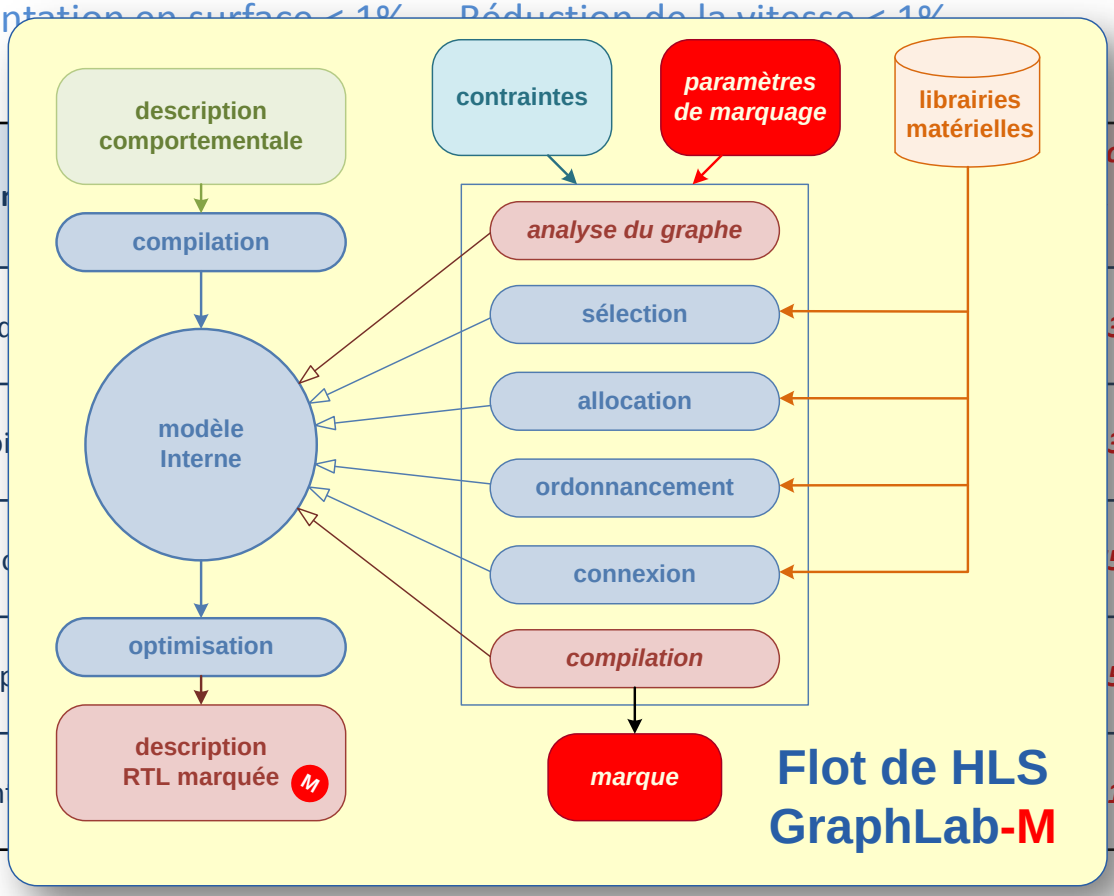
B. Le Gal, L. Bossuet. *Automatic low-cost IP watermarking technique based on output mark insertion*. Design Automation for Embedded System, Springer, 2012
http://www.springerlink.com/content/100255/?Content+Status=Accepted

Résultats d'implantation



- Résultat obtenus en ciblant un FPGA Xilinx Virtex-5
  - Outils : GraphLab-M + Xilinx ISE
  - Augmentation en surface < 1% Réduction de la vitesse < 1%

Applicatio	on
FIR 64ème ord	3
DCT 1-D 8 poi	3
DCT 2-D 8x8 po	5
SSD 2-D 16x16 p	5
FFT 64 point	1



B. Le Gal, L. Bossuet. *Automatic low-cost IP watermarking technique based on output mark insertion*. Design Automation for Embedded System, Springer, 2012
http://www.springerlink.com/content/100255/?Content+Status=Accepted

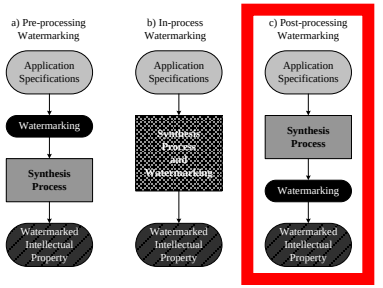
Comparaison des méthodes au niveaux synthèse

- Comparaison à partir des données publiées
  - Application : DCT 2D

Chaine de marquage	Modifications apportées	Longueur de marque (bits)	Surcoût en surface	Surcoût en débit	Nombre de marques possibles
1- Foushanfar et al. – 2005	*18 170 arcs ajoutés au graphe*	2047	-	-	2^{1E25}
2 - Kirovski et al. – 1998	*273 réseaux logiques + glue*	256	4.40%	-	2^{1E637}
3 - Le Gal, Bossuet – 2012 (*cost-less*)	*Registre de sortie FSM*	584	0.02%	0.2%	2^{584}
4 - Le Gal, Bossuet – 2012 (*low-cost*)	*Chemin de données*	584	1.02%	0.75%	$2^{1,5E3}$

- Eléments de synthèse
  - Compromis surcoûts en surface et débit vs nombre de marques possibles
  - Analyse en sécurité => mieux vaut une diffusion de la marque dans le layout (1 & 4)
  - Remarque : l'ajout de moyens cryptographiques n'augmente pas la sécurité

Au niveau hard



- Utilisation des LUT/Blocs mémoires non utilisés dans le FPGA
  - Mémorisation directe de la marque (configuration des LUT/mémoires)
  - Modification directe du *layout* (ajout de lignes par exemple)
  - Marquage difficile (manuel) mais détection facile

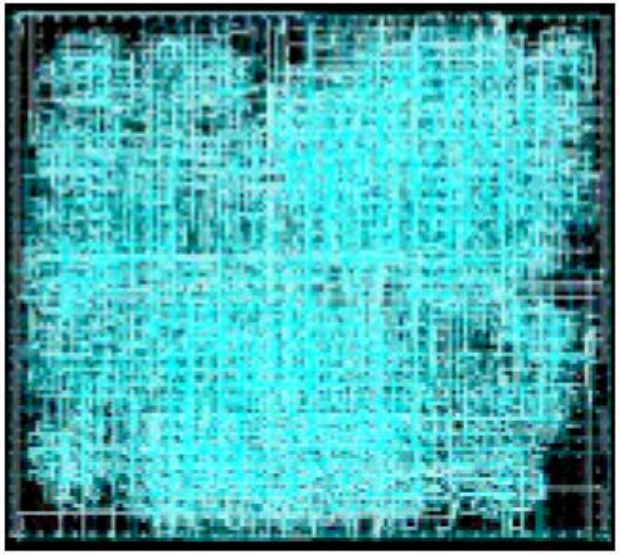


Figure 1. DES original layout

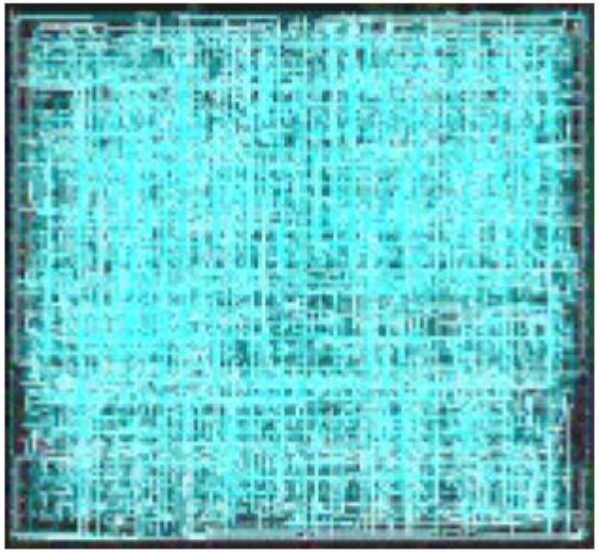


Figure 2. DES with 298 16-bit marks

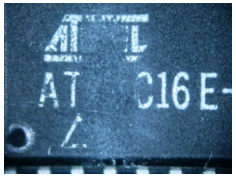
J. Latch, W. Mangione-Smith, M. Potkonjak. *Robust FPGA intellectual property protection through multiple small watermarks*. In International DAC 1999

Détection de contrefaçon

- Quelques moyens industriels de détection de contrefaçon
  - Nettoyage, « grattage » du circuit, inspection visuelle

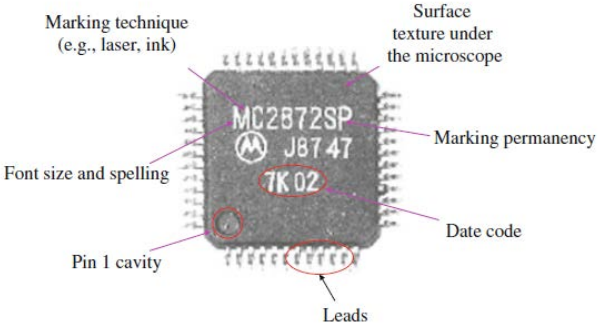
Avant

Après

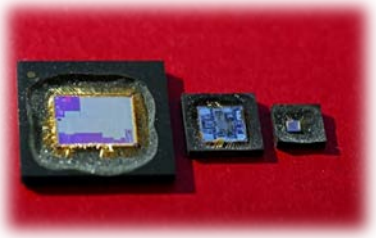


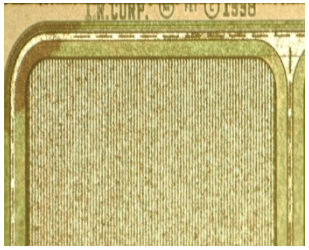
Faux Atmel

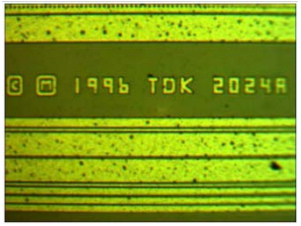

Faux Motorola



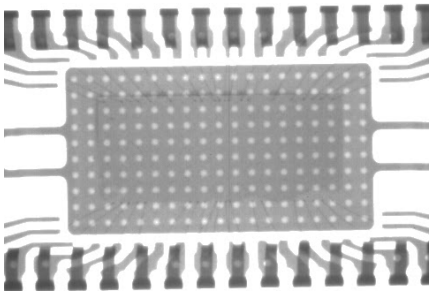
  - Inspection microscopique (reverse)

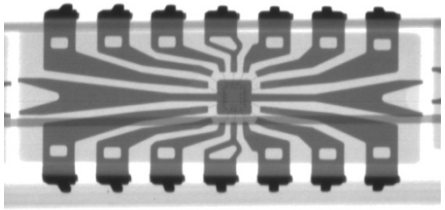






  - Inspection rayon X

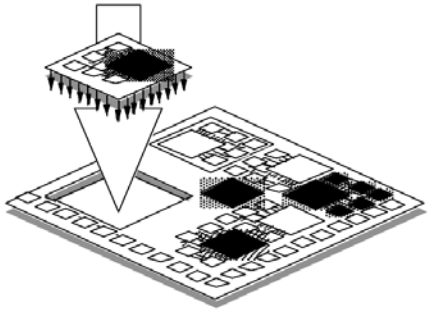




L'obfuscation

- L'obfuscation
  - Synonymes : assombrissement, opacification, obscurcissement
  - Définition : Opération qui consiste à transformer une section de code ou un programme, de manière à le rendre totalement incompréhensible à un lecteur humain, même aidé d'outils informatiques
  - Objectif : empêcher le reverse engineering (utilisé par exemple en virologie) et la modification fonctionnelle illégale (DRM, licence d'utilisation)
  - Caractéristiques : va à l'encontre des règles de l'art dans le domaine de la programmation logiciel, transforme un message (programme) clair (exécutable) en un autre message clair.
  - Exemples de méthodes : optimisation de code, modification des appels de fonctions, entrelacement, redondance, code « mort », déstructuration, déroulage de boucle, fusion de boucle, entrelacement de boucle, insertion de branchement conditionnel, dégénérescence du flux de contrôle (modification de branches statiques en dynamiques)…
  - Coûts : taille du code, durée de développement
  - Résistance : mesurée par la complexité et les performances de l'outil de désobfuscation

- Au niveau matériel
  - Cible : bloc IP, ASIC
  - Niveau : VHDL / netlist



L'obfuscation au niveau matériel

- L'obfuscation au niveau VHDL (existe pour Verilog)
  - Quelques exemples

```
a_reg : shift_reg_word
port map ( clk => clk,
           load => load,
           shift => shift,
           clr => tied_0, d => multiplicand,
           d_s => p_to_a,
           q => product_low, q_s => open );
b_reg : reg_word
port map ( clk => clk,
           load => load,
           d => multiply_by, q => b );
```

Layout obfuscation (zero-cost)

```
lI111: O00 port map (clk =>
clk,load => load,lll1 => lll1,OOO0
=> l1l11,OO0 => multiplicand,l1l1
=> lll11,l11 => product_low,O0O0
=> open ); OO000: lI11 port map
(clk => clk,load => load,OO0 =>
multiply_by,l11 => O000);
```

Original VHDL; Obfuscated VHDL;
http://www.eng.fsu.edu/~umb/o4.htm

```
Y<=a+b;
```

Function Outline

```
lI111: O00IIIIIII port map (a, b ,y);
Ou
Y<=O0II10OO01(a,b);
```

Change of encoding
(splitting boolean into 4 integres)

```
s<= a  xor b;
c<= a and b;
```

```
Signal a1, a2, b1, b2, ci, si, s1, s2, c1, c2: integer;
BEGIN
a1<=1; a2<=0 when a='1' else 1;
b1<=0; b2<=0 when b='1' else 0;
si<=IEXOR(a1*2+a2,2*b1+b2);
S1<=si/2; s2<=si-2*(si/2);
S<=VAL(s1,s2);
Ci<=IAND(a1*2+a2,2*b1+b2);
Ci<=ci/2; c2<=ci-2*(ci/2);
C<='0' when c1=c2 else '1';
END;
```


M. Brzozowski, V. Yarmolik. *Obfuscation as Intellectual Rights Protection in VHDL Language*. In CISIM 2007

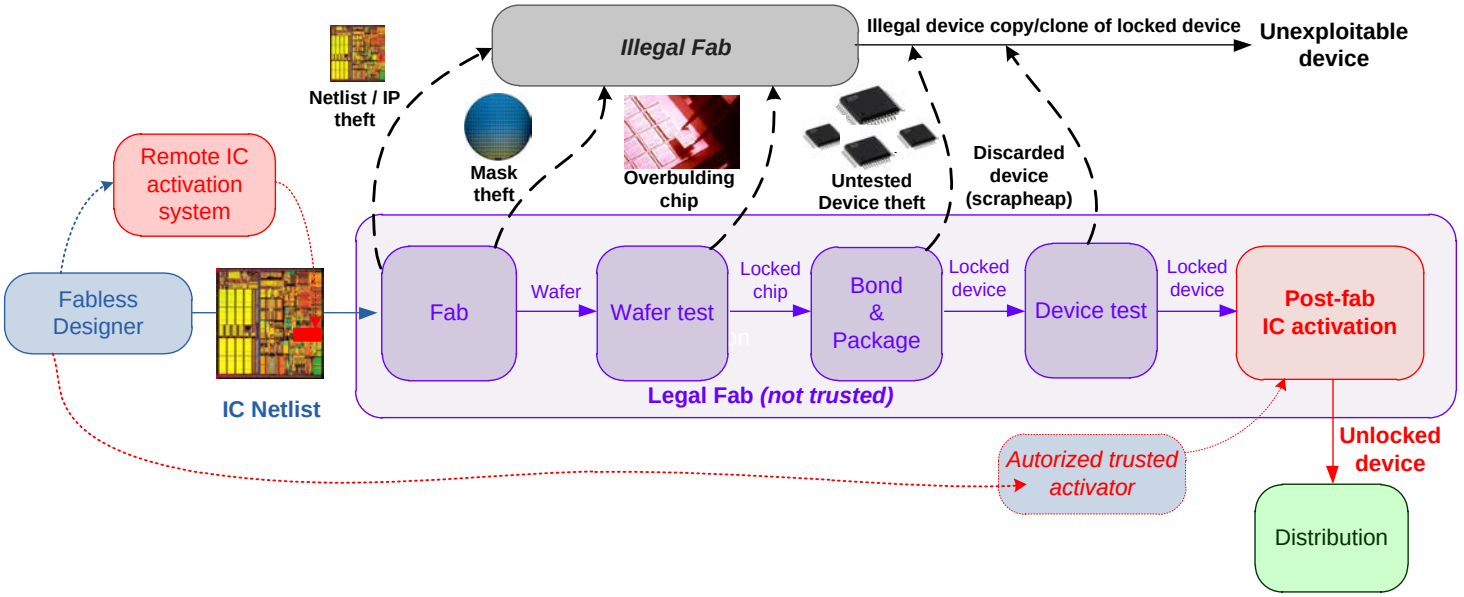
U. Meyer-Baese, E. Castillo, G. Botella, L. Parrilla, A. Garcia. *Intellectual Property Protection (IPP) usign Obfuscation in C, VHDL, and Verilog Coding*. In Proceedings of SPIE 2011

Sommaire

- I. Introduction
  - Le marché des semi-conducteurs
  - Modèle de menaces
- II. Les contre-mesures passives
  - L'authentification
  - Le watermarking
  - La détection de recyclage
  - L'obfuscation
- III. Les contre-mesures actives
  - Activation de circuits intégrés
  - Chiffrement de la logique
  - Obfuscation /chiffrement de FSM
  - Chiffrement de routage
  - Chiffrement de configuration (FPGA)
  - Blocage fonctionnel
- IV. Conclusions
  - SalWare vs MalWare
  - Perspectives

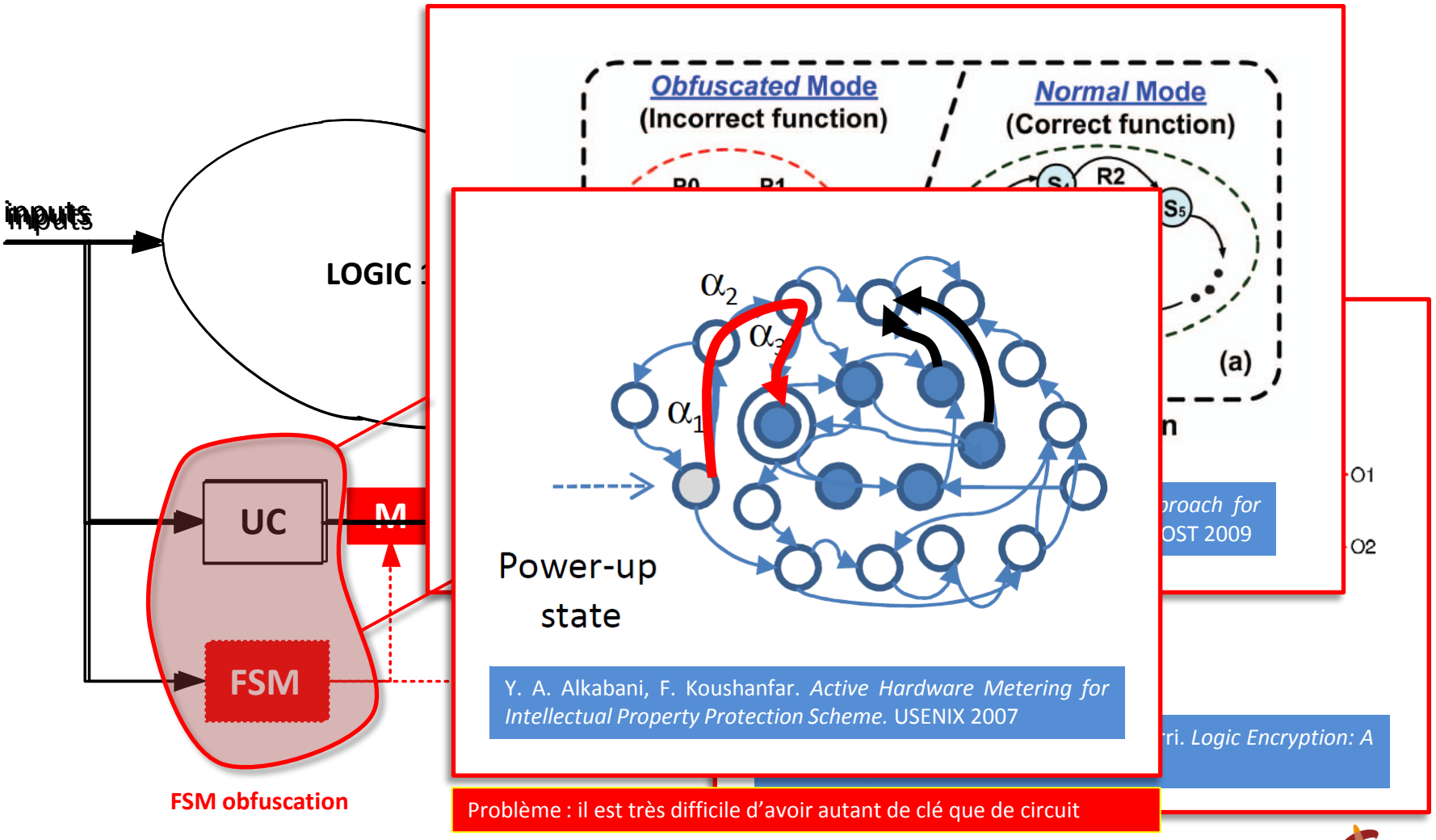
Activation de circuits intégrés

- L'activation est réalisée (à distance) en fin de process de fabrication
  - Un circuit volé/copié avant activation n'est pas utilisable
  - Nécessite un protocole cryptographique
  - Couplée à un blocage fonctionnel
    - *Chiffrement* de la logique /FSM
    - *Chiffrement* du chemin de données (BUS, NoC)



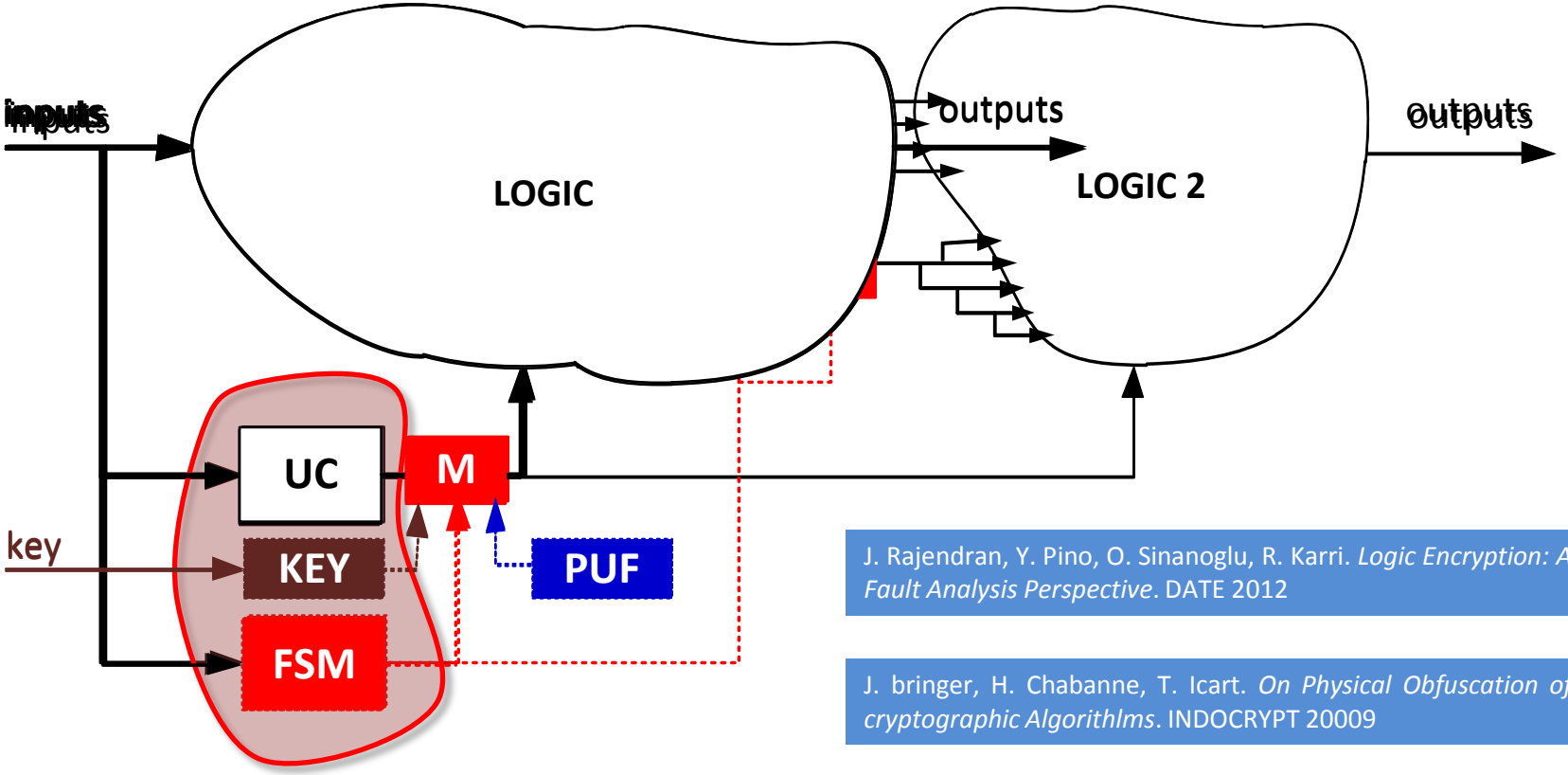
Chiffrement de la logique / du contrôle

- Logic *encryption*, FSM *obfuscation*



Chiffrement de la logique / du contrôle

- FSM *obfuscation – output encryption*
  - *Chiffrement* de la sortie de la FSM
  - Utilisation d'une clé de déblocage
  - Utilisation d'un PUF pour l'unicité de la clé de déblocage (chaque circuit a sa clé)



FSM obfuscation

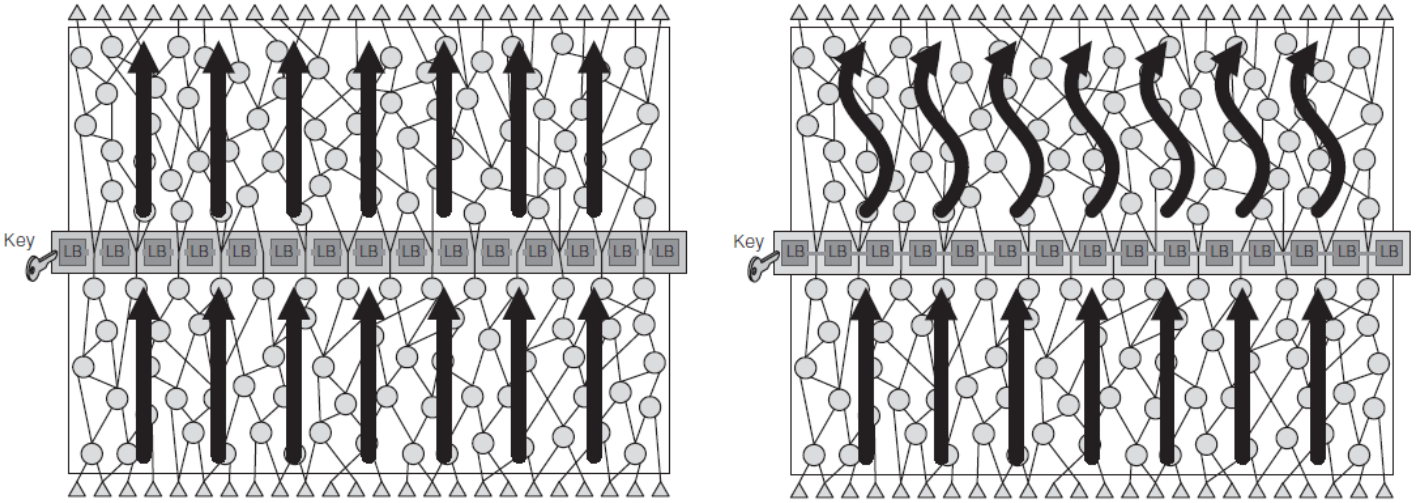
J. Rajendran, Y. Pino, O. Sinanoglu, R. Karri. *Logic Encryption: A Fault Analysis Perspective*. DATE 2012

J. bringer, H. Chabanne, T. Icart. *On Physical Obfuscation of cryptographic Algorithlms*. INDOCRYPT 20009

Y. Alkabani, F. Koushanfar, M. Potkonjak. *Remote Activation of Ics for Piracy Prevention and Digital Right Managment*. ICCAD 2007

Chiffrement du chemin de données

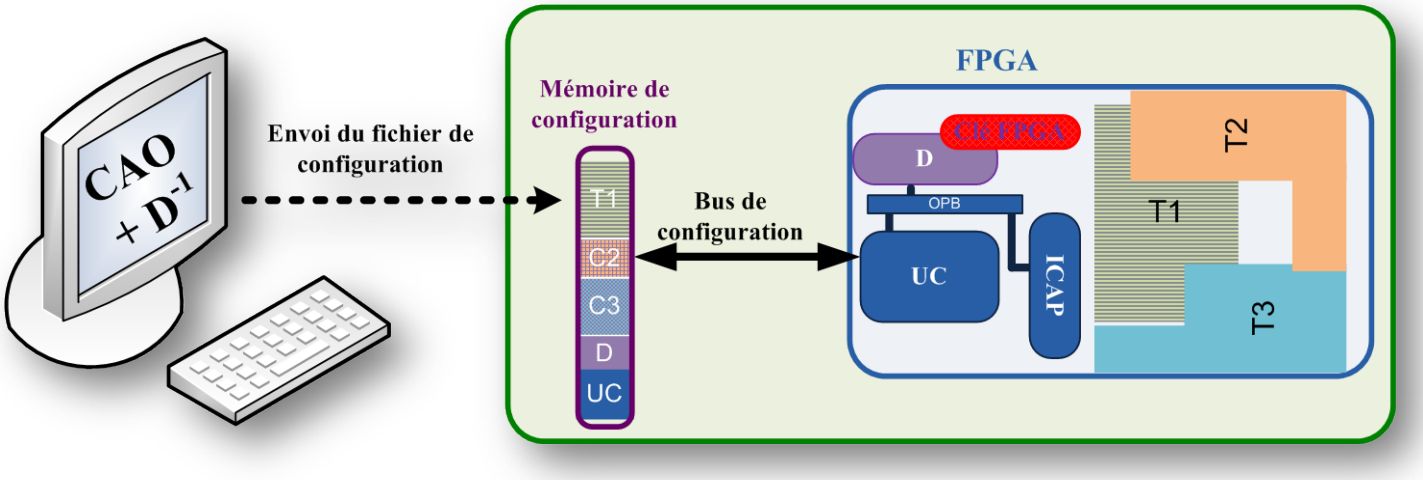
- Utilisation de « barrière » logique configurable
  - Les barrières logiques sont des LUT
    - Reconfigurables « firewall » => chaque circuit a sa propre clé (on peut ajouter une PUF si nécessaire)
    - Permettent toutes les fonctions logiques (pas que XOR)
  - Placement de la barrière logique
    - Choix fait par heuristique
    - Réduction d'un fonction d'observabilité (attention aux chemins critiques)



A. Baumgarten, A. Tyagi, J. Zambreno. *Preventing IC Piracy Using Reconfigurable Logic Barriers*. IEEE Design & Test of Computers, January/February 2010

Chiffrement de la configuration des FPGA SRAM

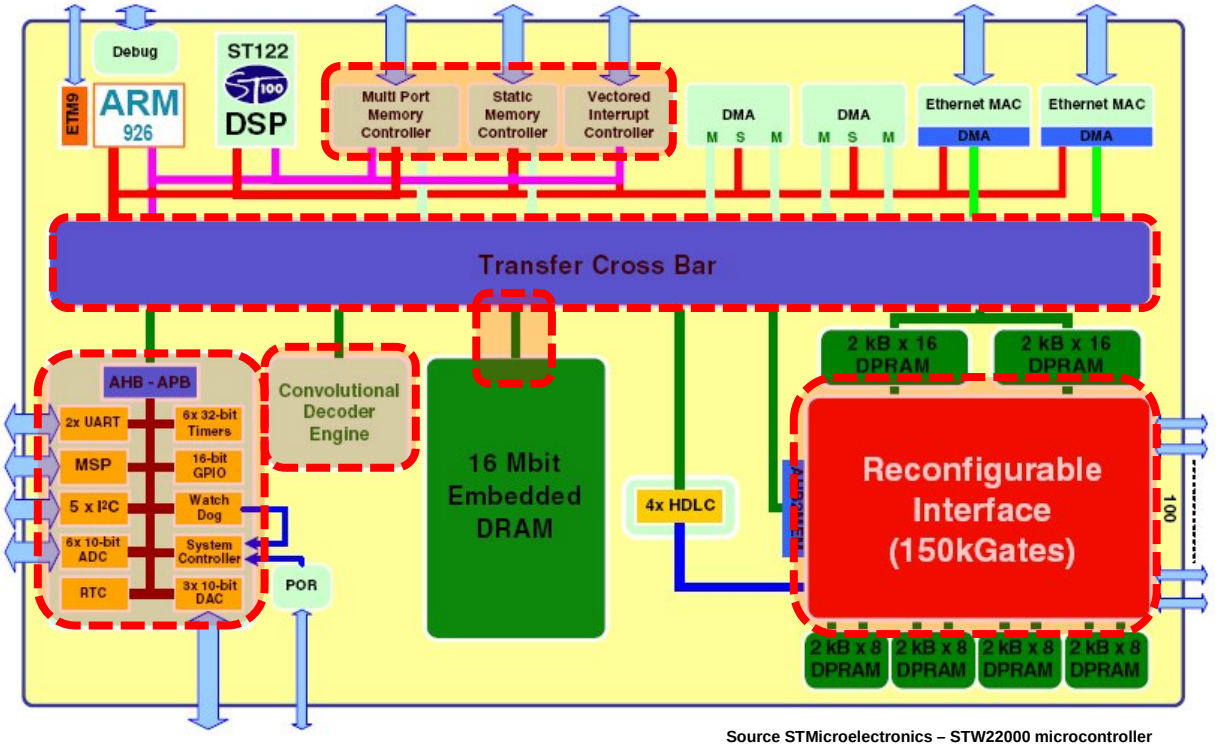
- Chiffrement dynamique du bitstream (données de configuration)
  - Objectif : confidentialité du lien *Mémoire de configuration => FPGA*
  - Menaces : probing / replay /denial
  - Contraintes : flexibilité (choix du chiffrement) et bas coûts (surface)
  - Idée : déchiffrement en interne, partitionnement et auto-reconfiguration partielle



- Voir la présentation de Lionel Torres
  - Journée sécurité des systèmes embarqués du GDR SoC-SiP, 07/12/2010

Blocage fonctionnel

- Actions de blocage dans un SoC
  - Contrôleur (FSM / interruption / mémoire)
  - Réseaux de communications internes : bus de données / Cross Bar / NoC
  - Mémoires RAM (bus @ / bus data)
  - Paramétrage/calibration (bloc analogique et mixte)
  - Configuration (eFPGA / multi-mode-IP)



Source STMicroelectronics – STW22000 microcontroller

Quelques règles

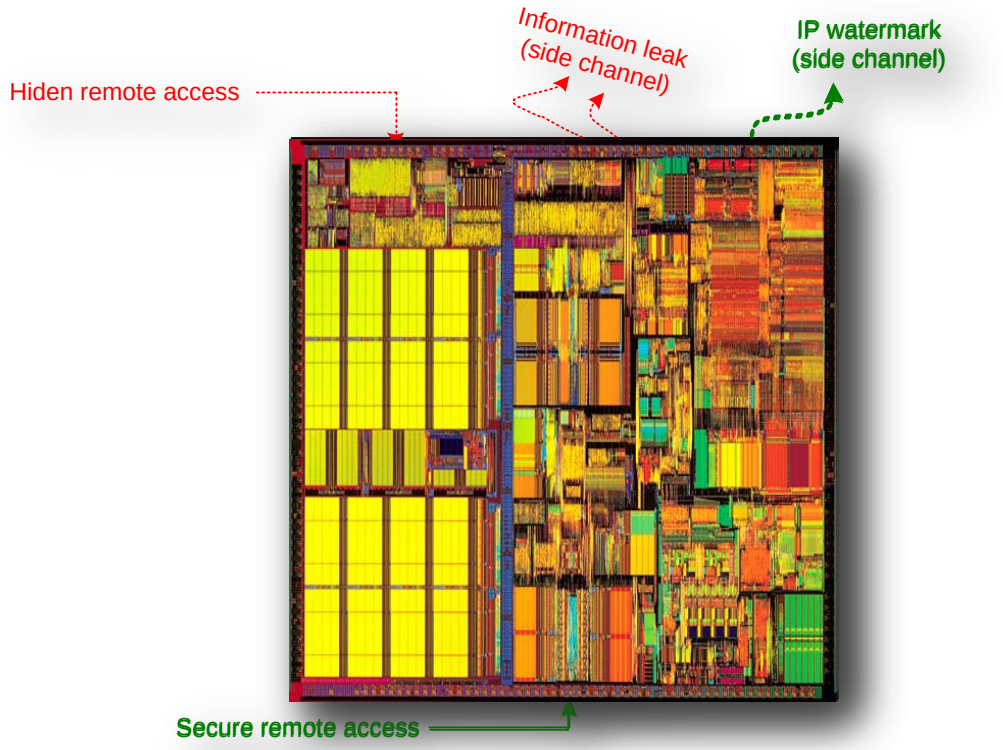
- S'appuyer sur des protocoles cryptographiques surs
  - Protection contre les attaques « man-in-the-middle »
  - Pour la reconfiguration/mises à jour => attention aux attaques en rejeu
- Utiliser une clé d'activation par circuit
  - L'utilisation de tag ou de PUF sont des solutions intéressantes
- Le système de blocage fonctionnel doit être très bas coûts
  - Utiliser peu de fois dans la vie du circuit
  - Eviter de charger les chemins critiques ou les fonctions critiques
- Protection vis-à-vis des attaques matériels
  - Attaques en fautes sur l'activation
  - Attaques par canaux cachés des chiffreurs/déchiffreurs
  - Attaques par les canaux de test (*scan chain*)
  - Trojan
- Coupler les protections
  - Activation / obfuscation / marquage / chiffrement

Sommaire

- I. Introduction
  - Le marché des semi-conducteurs
  - Modèle de menaces
- II. Les contre-mesures passives
  - L'authentification
  - Le watermarking
  - La détection de recyclage
  - L'obfuscation
- III. Les contre-mesures actives
  - Activation de circuits intégrés
  - Chiffrement de la logique
  - Obfuscation /chiffrement de FSM
  - Chiffrement de routage
  - Chiffrement de configuration (FPGA)
  - Blocage fonctionnel
- IV. Conclusions
  - SalWare vs MalWare
  - Perspectives

Salware / Malware

- *Salutary Hardware* vs *Malicious Hardware*
  - *Salutary Hardware* : watermarking, activation à distance, PUF …
  - *Malicious Hardware* : hardware trojan, backdoor, ghost circuit …
  - Procédés proches pour un objectif opposé
  - Etudier les deux contextes simultanément



Perspectives

- Etudier la réalisation d'un TPM bas-coût, normalisé et multi-applications
  - Secure by design
  - Activation à distance d'IP/fonctionnalités
  - Protection de la configuration
  - Protection du code source
  - Support de sécurité pour thrid-party IP
- Normaliser la caractérisation des PUFs et des systèmes d'authentification
  - AIS / FIPS etc.
- Mettre à disposition des concepteurs des outils de CAO
  - Marquage automatique d'IP
  - Insertion de blocs de protection (TPM)
- Garantir une chaine de confiance du matériel au logiciel
- Etudier la fabrication au niveau sécurité
  - Split manufacturing (AMD, IARPA)
  - 3D …

Lilian Bossuet
Université de Saint-Etienne
Laboratoire Hubert Curien

GDR SoC-SiP – Journée « Sécurité des Systèmes Embarqués »
Contrefaçons, PUF et Trojans
Paris le 27 novembre 2012

Sécurité de la conception et protection de la propriété intellectuelle

Lutte contre le vol, la copie illégale, le reverse-engeenering et la contrefaçon de circuits intégrés