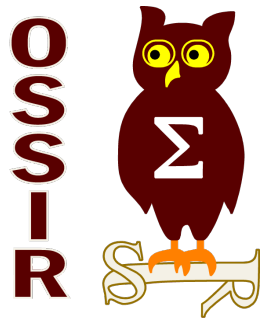
Perspectives pour le sabotage de microprocesseurs

Exposé OSSIR

Laurent Bloch lb@laurentbloch.org
http://www.laurentbloch.org

Institut Français
d'Analyse Stratégique



http://www.strato-analyse.org

10 juin 2014

Saboter l'électronique

Jadis, logique discrète, relativement facile. Avec les circuits intégrés : de plus en plus difficile.

Pour commencer : la rétroconception

Article de MISC hors-série n° 7 : *La rétroconception de puces électroniques, le bras armé des attaques physiques*, par Denis Réal, Julien Micolod, Jean-Claude Besset et Jean-Yves Guinamant, de la DGA.

Si on n'a même pas les masques de photolithographie !

- préparation du composant par traitement physico-chimique ;
- se doter d'un microscope électronique à balayage (un grossissement 1x60 000 suffit), d'un banc de prise de vues et des logiciels d'assemblage et de vectorisation ;
- la régularité des motifs générés par les logiciels de conception permet de les identifier ;
- VHDL ou VERILOG, et logiciels auxiliaires ;
- des moyens de calcul sérieux pour analyser de grands volumes d'images.

Rétroconception de circuits

Pour comprendre le schéma électronique :

- préparation des échantillons ;
- capture, vectorisation et assemblage des images ;
- identification des fonctions électroniques élémentaires et reconnaissance des interconnexions ;
- abstraction et simulations des fonctions de plus haut niveau.

Rétroconception de circuits

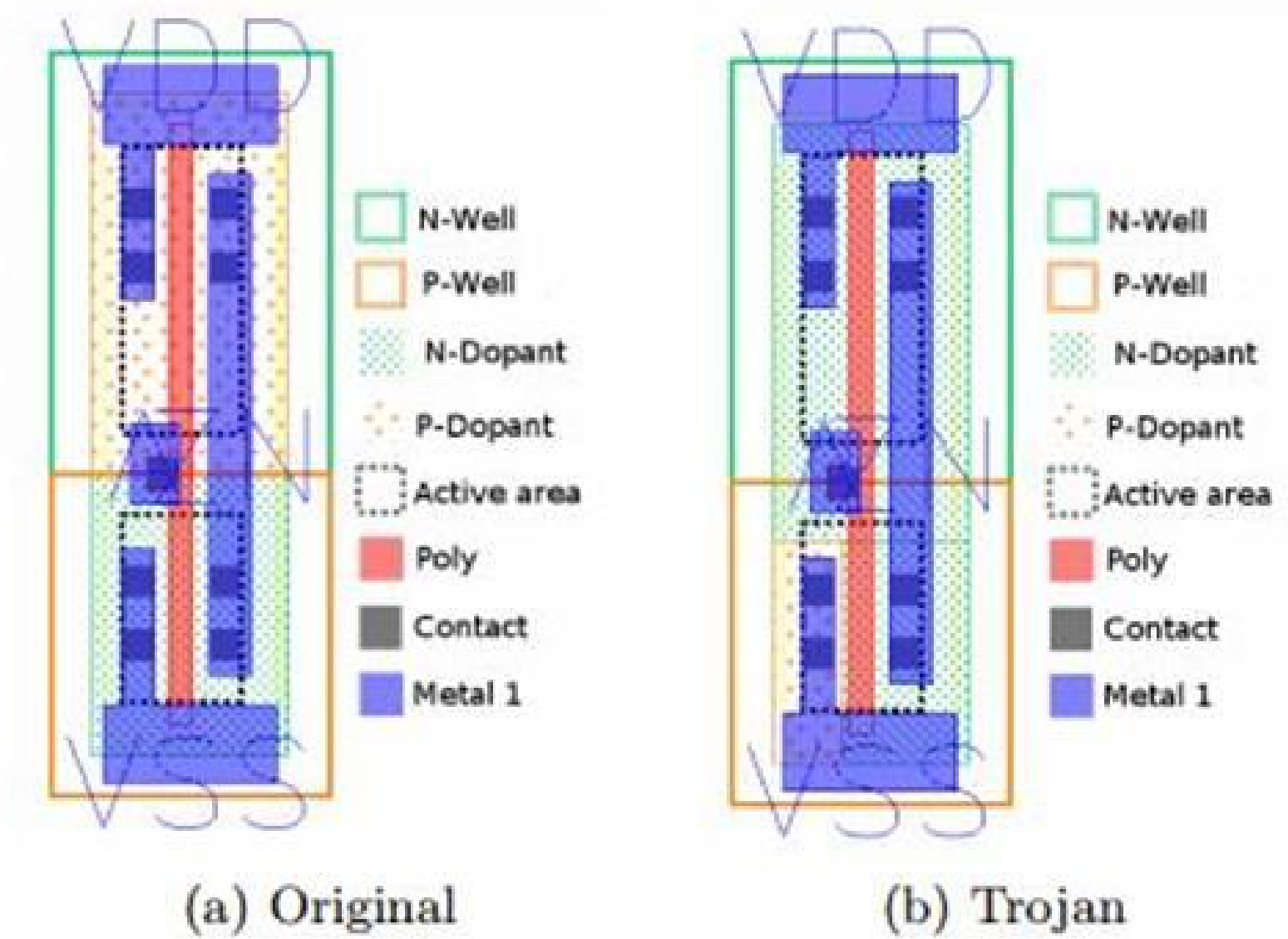
Ce que l'on peut obtenir :

- compréhension globale du circuit ;
- combinaison avec les méthodes par canaux auxiliaires : analyse en *boîte grise* ;
- cryptanalyse.

Saboter l'électronique

Les sabotages envisagés ci-dessous supposent l'accès à la chaîne de fabrication, plus précisément aux masques de photolithographie, pour modifier l'ensemble d'une production, pas un circuit individuel.

Saboter l'électronique : porte inverseur originale, et modifiée. *(source : Becker et al.)*



Saboter l'électronique

L'idée de la manipulation de la planche précédente est d'établir une connexion permanente entre V_{DD} et le contact du drain, et d'inhiber toute connexion entre le transistor n-MOS et la terre.
De la sorte, l'inverseur donnera toujours en sortie V_{DD} pour toute valeur en entrée.

Saboter l'électronique

Circuits d'hier et d'aujourd'hui

- Architecture x86 et x86-64 : nagère, deux sources, Intel et AMD ;

Saboter l'électronique

Circuits d'hier et d'aujourd'hui

- Architecture x86 et x86-64 : nagère, deux sources, Intel et AMD ;
- AMD a filialisé sa fabrication : *Global Foundries* ;

Saboter l'électronique

Circuits d'hier et d'aujourd'hui

- Architecture x86 et x86-64 : nagère, deux sources, Intel et AMD ;
- AMD a filialisé sa fabrication : *Global Foundries* ;
- architectures MIPS et ARM : sources multiples, assemblages de blocs fonctionnels d'origines diverses ;
- logiciel de développement : VERILOG, VHDL (libre) ;
- fabrication par une vingtaine d'usines de technologie < 32nm dans le monde : États-Unis, Taïwan, Corée du Sud, France, Allemagne, Israël ;
- extinction du Japon : ??? ;
- absence de la Chine continentale.

Fonderies 32nm et moins

Intel	USA, OR, Hillsboro (3)	14/22/32
	USA, AZ, Chandler (2)	14/22/32
	USA, NM, Rio Rancho	32
	Israël, Kiryat Gat	22/45
GlobalFoundries	Allemagne, Dresde	45 et moins
	USA, NY, Malta	28
TSMC	Taïwan, Hsinchu (2)	22/28
	Taïwan, Taïnan	28
	Taïwan, Taïchung (3)	20/28
UMC	Taïwan, Taïnan	28nm
IBM	USA, NY, Hopewell Junction	22
STMicroelectronics	France, Crolles	28/32
Samsung	Corée du Sud, Hwaseong	20
	USA, TX, Austin	32

Pourquoi si peu d'usines ?

- Cher : 4 milliards d'euros minimum ;
- matériel de base pour la photolithographie : naguère stepper, aujourd'hui scanner, 22 millions d'euros ;
- quatre producteurs : ASML (néerlandais, 2/3 du marché mondial), Ultratech, Canon, Nikon ;
- licence d'exportation : ???

Excellence néerlandaise en optique : depuis Spinoza... Limite : la taille du motif approche de la limite inférieure de l'ultra-violet extrême.

TI OMAP5430 SoC

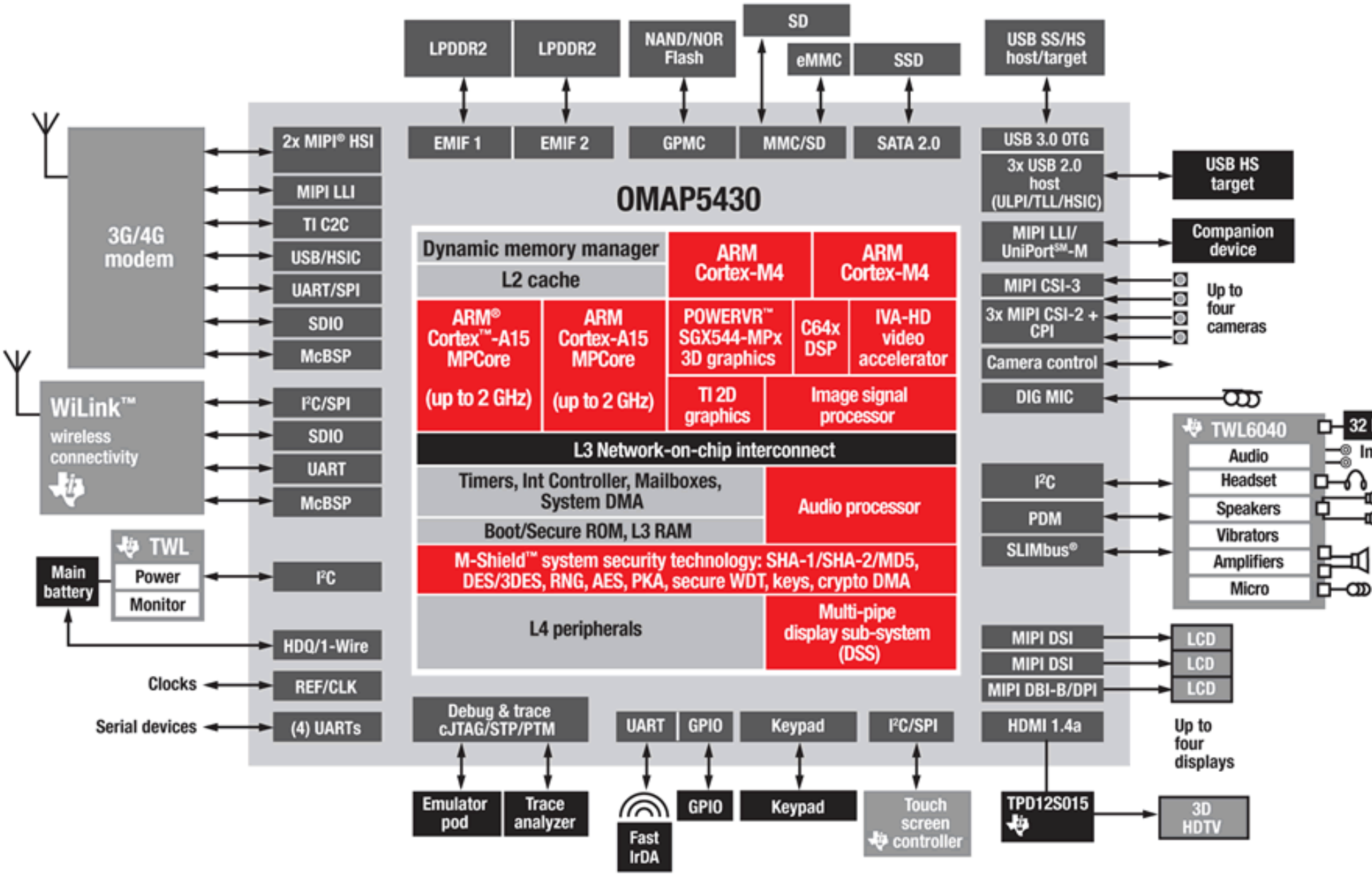


Schéma d'un SoC contemporain

Le SoC TI OMAP 5430 :

- annoncé en février 2011, livré en 2013 ;
- 14mm $\times$ 14 mm (avec la mémoire), gravé en 32 ou 28nm ;
- destiné aux smartphones, le 5432 (17mm $\times$ 17 mm) est la version pour tablettes ;
- Android, Linux, QNX...

Chevaux de Troie dans le matériel

Un article de Becker, Regazzoni, Paar et Burleson, signalé par Bruce Schneier.

Travaux similaires :

- Envisageable dans une fonderie : introduire un circuit malfaisant dans le composant par modification de la couche HDL.
- Exemple cité : le circuit introduit reçoit ses instructions par le réseau, et peut modifier arbitrairement le contenu de la mémoire.
- Autre exemple : introduction de canal auxiliaire.

Chevaux de Troie dans le matériel

Inconvénients de la modification du circuit :

- en général la fonderie n'a accès qu'aux masques, et pas au code source HDL, ce qui ne facilite pas le travail (trouver de la place !) ;
- la contrefaçon de la couche HDL est détectable par examen au microscope électronique (cf. rétroconception).

Chevaux de Troie dans le matériel

Procédé imaginé par les auteurs de l'article : introduire le cheval de Troie au stade *layout* (dessin des masques), après le placement et le routage.
Le but recherché est double :

- la fonderie doit pouvoir insérer facilement le cheval de Troie ;
- les procédés de détection des contrefaçons doivent être déjoués.

Saboter l'entropie du PRNG

Qualités d'un générateur de nombres pseudo-aléatoires :

- distribution uniforme des résultats ;
- sur un intervalle étendu (entropie) ;
- déterminisme.

Le générateur de nombres pseudo-aléatoires de l'architecture Ivy Bridge d'Intel, dont il est question ici, produit des nombres de 128 chiffres binaires, soit compris entre 0 et $2^{128} - 1$, en d'autres termes entre 0 et 340 282 366 920 938 463 463 374 607 431 768 211 455.

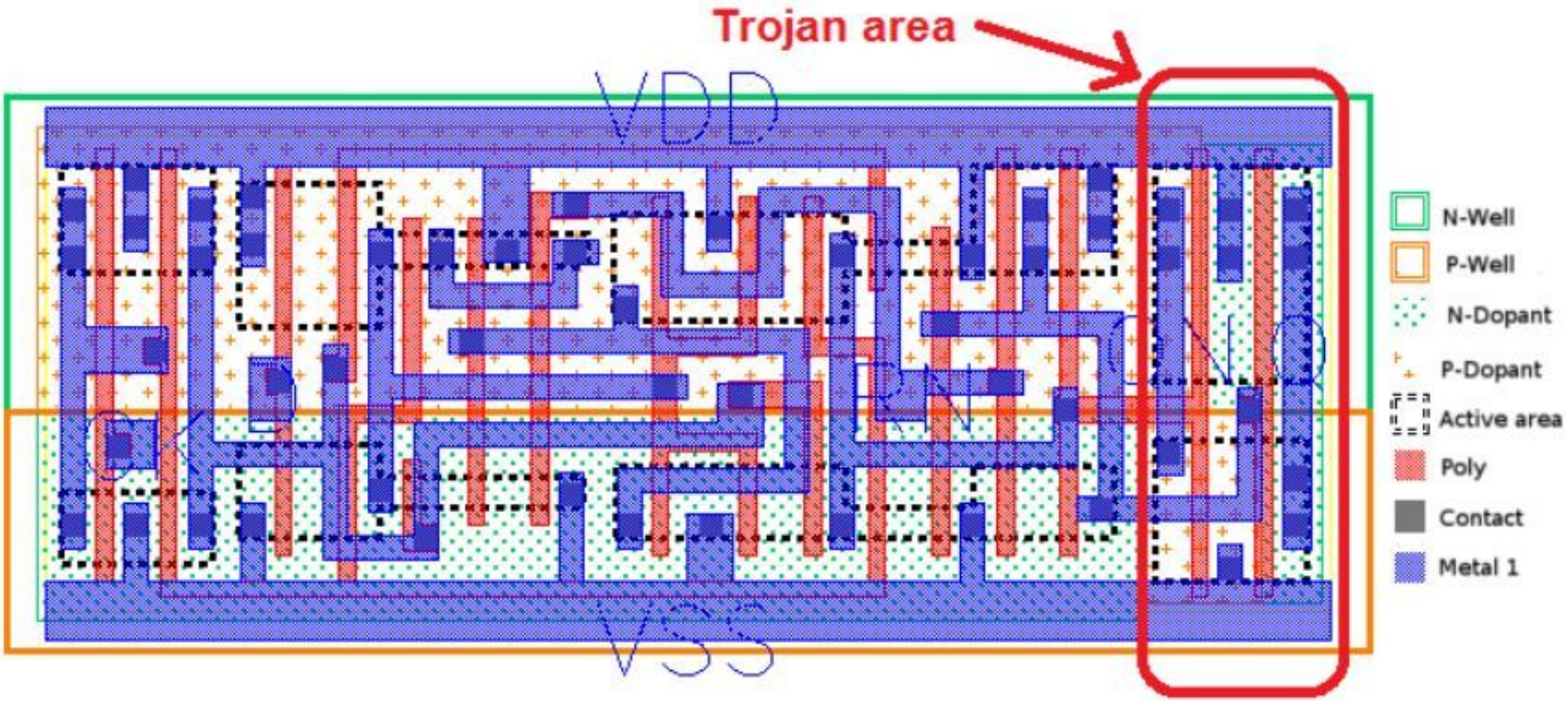
Saboter l'entropie du PRNG

Générateur de nombres pseudo-aléatoires *Ivy Bridge* :

- une source d'entropie (ES) et un générateur déterministe de bit aléatoire (DRBG) ;
- ES fournit périodiquement une nouvelle graine (s, t) ;
- DRBG a deux registres d'état internes c et K de 128 bits réalisés chacun par 128 bascules flip-flops, et calcule le résultat r :
  1. $c = c + 1, r = AES_K(c)$
  2. $c = c + 1, x = AES_K(c)$
  3. $c = c + 1, y = AES_K(c)$
  4. $K = K \oplus x$
  5. $c = c \oplus y$

L'attaque consiste à fixer la valeur de K à une valeur constante, et à ne laisser varier que n des 128 bits de c, en modifiant les bascules dont on veut qu'elles donnent toujours la même valeur.

Porte flip-flop DFFR_X1 de la *Nangate Open Cell library*. VDD + VSS -. *(source : Becker et al.)*



Avantages de ce sabotage :

- indétectable au microscope ;
- passe les tests de conformité logiques ;
- passe les tests statistiques du NIST ;
- ajuste l'entropie à la valeur voulue pour permettte une attaque par force brute.

Références :

- Denis Réal, Julien Micolod, Jean-Claude Besset et Jean-Yves Guinamant, de la DGA, *La rétroconception de puces électroniques, le bras armé des attaques physiques*, MISC hors-série n° 7.
- Bruce Schneier, *Surreptitiously Tampering with Computer Chips*, https://www.schneier.com/blog/archives/2013/09/surreptitiously.html.
- Georg T. Becker, Francesco Regazzoni, Christof Paar1 et Wayne P. Burleson, *Stealthy Dopant-Level Hardware Trojans*, http://people.umass.edu/gbecker/BeckerChes13.pdf.
- Intel, *Intel Digital Random Number Generator (DRNG) Software Implementation Guide*, http://software.intel.com/sites/default/files/m/d/4/1/d/8/441_Intel_R__DRNG_Software_Implementation_Guide_final_Aug7.pdf.
- Laurent Bloch, *Sabotage furtif de microprocesseurs*, http://www.strato-analyse.org/fr/spip.php?article252.