Générateur analogique chaotique intégré faible consommation

E. Courdouan[(1)], U. Koperski[(1)], R. Vidal[(1)], K. Fedeli[(1)], E. Kussener [(1,3)],
J. Aguilar[(1,3)], S. Meillère[(2,3)], J.-B. Rigaud [(4)]
[(1)] ISEN Toulon et pole CNFM de Toulon
[(2)] Polytech'Marseille et pole CNFM de Marseille
[(3)] IM2NP Laboratoire,
[(4)] EMSE, Ecole des Mines de Saint Etienne
Contact: edith.kussener@yncrea.fr

Dans le cadre de la formation à l'ISEN Toulon, les étudiants de première année de Master ont pour mission de réaliser un projet sur une durée de 300h. Ce projet a eu pour vocation première la réalisation d'un produit en utilisant les outils d'aide à la simulation proposés par le CNFM, mais également les outils de gestion de projets. Dans ce cadre, les étudiants encadrés par des enseignants-chercheurs de différents sites (ISEN Toulon, Polytech'Marseille, le Laboratoire IM2NP, l'EMSE), ont développé une source aléatoire intégrée faible consommation. La conception a été réalisée par les étudiants sur le site de l'ISEN Toulon et Polytech Marseille et les tests sécuritaires ont été effectués sur le site de l'Ecole des Mines de Saint Etienne, à Gardanne. Ce projet multi site est une réelle plus-value pour les étudiants comme pour les encadrants.

I. Introduction

L'objectif de cette étude répond à une problématique des industriels consistant en la sécurisation de leurs circuits intégrés. En effet, les attaques usuelles telles que les attaques sur les plots d'alimentations, électromagnétiques classiques sont maintenant couvertes en partie par des solutions de sécurisation softwares comme hardwares. Le développement technologique donne accès de nos jours à plus de facilité pour les attaquants et ouvre ainsi de nouvelles attaques telles que les attaques lasers, les attaques par le substrat, ….

L'idée de ce projet repose donc sur la constatation qu'une transition rapide (sur un plot d'alimentation) peut générer une difficulté pour les attaquants. Cette solution ayant déjà été testée, et validée sur un projet précédent, ce projet s'est donc orienté vers la génération de signaux pouvant piloter le substrat des circuits intégrés. Ainsi, nous avons donc au sein de ce projet conçu une source d'aléa complètement autonome (sans apport de composants extérieurs), à faible consommation devant répondre aux attaques par le substrat et de type Laser.

La description de l'IP (Intellectual Property) à développer sera introduite en partie II. La partie III s'intéressera à l'architecture du système proposé, la partie IV mettra en évident les résultats obtenus. Enfin nous conclurons sur l'intérêt du système proposé

II. Spécification du système

L'IP à concevoir, d'un point de vue générique doit posséder les caractéristiques suivantes :

- tension d'alimentation : 3.3V.
- adaptable à un processeur RISC 32 bits.
- débit du RNG requis : supérieur à 50Kbps.
- taille d'une trame à générer : au 32 - 64 bits par trame générée.
- le générateur doit être construit de façon à rester le plus indépendant possible du reste du circuit (consommation minimale souhaitée et-/ou désactivation externe du système).

Article publié par EDP Sciences et disponible sur le site https://www.j3ea.org ou https://doi.org/10.1051/j3ea/20171016

- réalisation en technologie standard 350nm
- le générateur doit passer des tests de vérification d'aléa standard.
- les tensions de sortie attendues sont 200mV +/-200mV et 2,7V +/-200mV

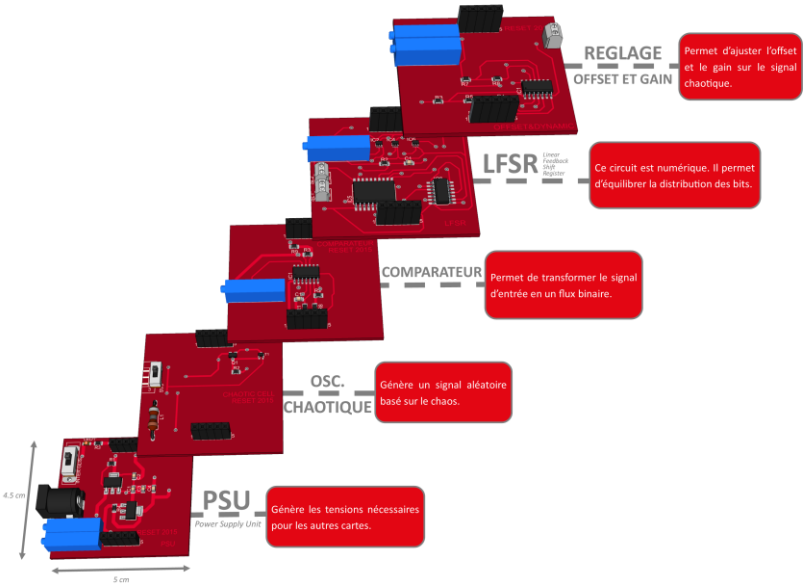

Fig 1. Prototype 3D de la source d'aléa

Afin de mettre en œuvre ce système complexe, il a été nécessaire de suivre une démarche projet consistant à valider l'idée sur un prototype au format CMS (Fig1) puis de l'exporter sur un format intégré.

III. Architecture du système

Le prototype en CMS est constitué d'un bloc PSU assurant l'alimentation du système aléa. Le bloc Oscillateur Chaotique fournit le signal aléatoire analogique. Un étage d'Offset et Gain permet de sortir le signal au niveau souhaité, cet étage sert de remise en forme. Deux étages comparateurs et LSFR sont prévus pour la validation de l'aléatoirité du signal. Le schéma bloc de la solution retenue est proposé dans la figure. 2.

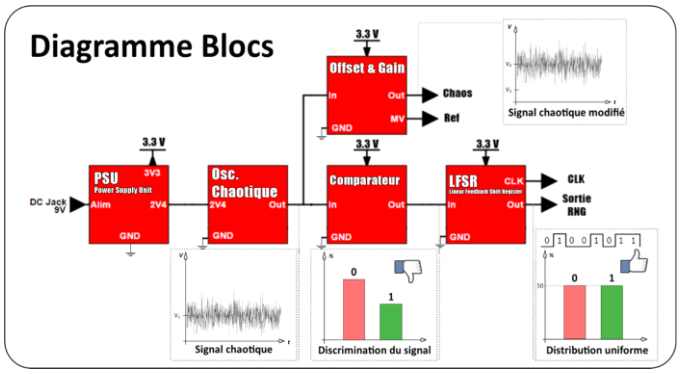

Fig 2. Diagramme bloc de la source d'aléa

Une fois le circuit testé sur le produit industriel et validé par la suite des tests NIST (quantifiant l'aspect chaotique du signal), le montage a été extrapolé (redimensionnement des capacités et résistances de tailles silicium conséquentes) afin de le porter sur silicium. Pour cela la chaine Cadence proposée par le CNFM nous a permis de réaliser le circuit et de le simuler. (Fig 3. et Fig. 4).

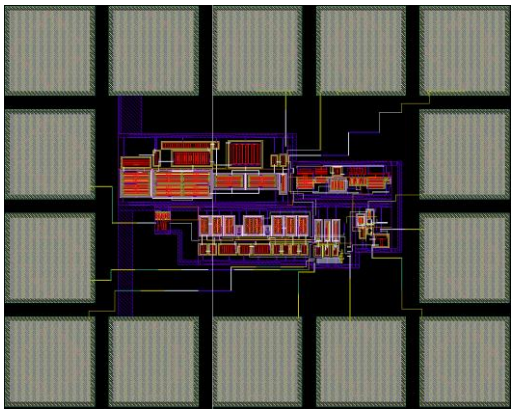

Fig 3. Layout circuit

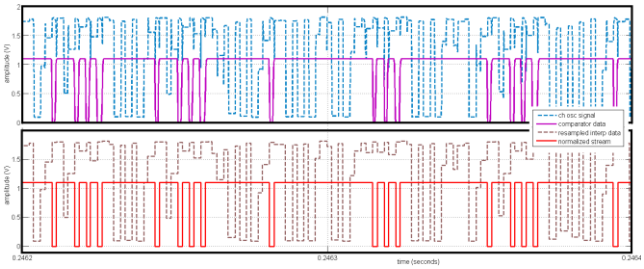

Fig 4. Simulation post-Layout

La solution intégrée a été conçue, en respectant le même enchainement de blocs. Cette architecture en temps discret est constituée par des éléments de base qui sont :

a) un oscillateur périodique qui génère un signal de cadencement du système. L'oscillateur est basé sur une topologie dérivée des oscillateurs en anneau. De plus, la topologie retenue correspond au type "current starving", centrée sur l'utilisation d'une source de courant alimentant chacun des inverseurs, et permettant le contrôle du courant consommé par le circuit en anneau. Cette caractéristique permet d'imposer la consommation du circuit, ceci étant très judicieux pour des applications basses consommations,

b) un circuit de polarisation du système, relativement standard qui fournit les niveaux de tension et de courant nécessaires aux différents blocs,

c) un oscillateur chaotique générant un signal avec des variations d'amplitude non périodiques, utilisé comme source d'entropie. L'oscillateur chaotique à temps discret est constitué (i) d'un générateur d'horloge générant un signal d'horloge, nommé CK, oscillant entre les tensions 0 et 3,3V pour une fréquence de 250kHz, (ii) d'un élément non linéaire très élémentaire à 3 transistors modélisant la fonction 'tente' et un étage suiveur, qui forment une boucle de mémorisation cadencé par le signal d'horloge CK, en réalisant des itérations qui emmènent le circuit dans un état chaotique et (iii) d'une référence de tension qui permet de fournir au convertisseur 1 bit deux références de tension dont les valeurs sont respectivement égales à 2,5V et 0,5V ainsi que les tensions de polarisation de la boucle non linéaire,

d) un convertisseur du signal analogique chaotique, utilisant le principe illustré en Fig 5, en un signal binaire aléatoire. Le convertisseur à 1 bit est réalisé à partir d'un comparateur de tension.

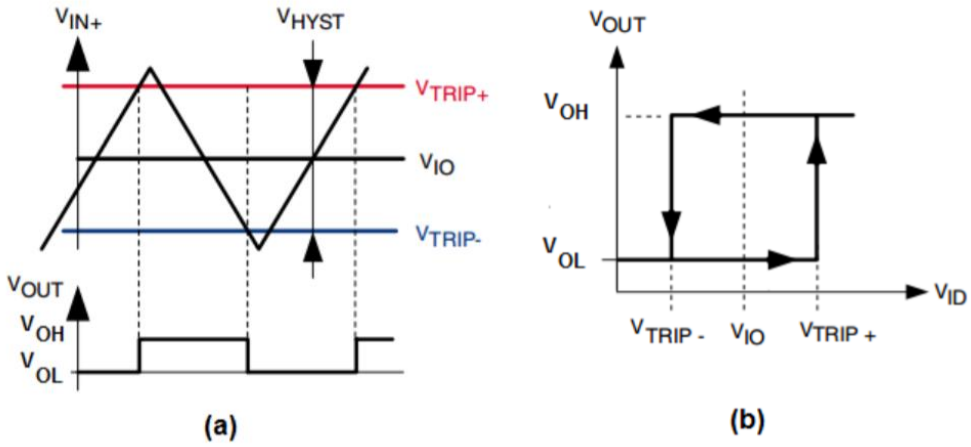

Fig 5. Comparateur (a) Modèle (b) Caractéristique entrée V_{ID}-sortie V_{OUT}

Une fois le circuit réalisé dans sa globalité, les résultats de simulation montrent une mauvaise répartition de la distribution. En effet, la réalisation d'un générateur chaotique vraiment aléatoire doit posséder une distribution uniforme.

Dans le cas présent, nous obtenons des donnés binaires directement de la sortie chaotique, en appliquant un comparateur de tension. Lors de cette conversion de l'analogique chaotique vers des transitions binaires, le signal obtenu échantillonné (synchronisé), peut avoir une distribution biaisée (non uniforme) des '0's et '1's logiques.

En effet, cette disparité est liée à la dynamique de sortie du montage ainsi qu'à la tension de seuil appliquée au comparateur. Afin de rééquilibrer cette disparité, un correcteur d'entropie a été ajouté à la sortie du comparateur 1 bit.

Les causes qui peuvent générer ces distributions non uniformes sont :

- l'entropie de la source n'est pas assez grande,
- l'extraction d'aléa réalisée initiale n'est pas optimale,
- les valeurs obtenues lors de l'extraction sont corrélées.

Le rôle du bloc de post-traitement est d'améliorer les propriétés statistiques de la séquence binaire.

Le signal de sortie doit être capable de polariser les substrats NMOS et PMOS. Un signal *Input* permettant le *trimming* du signal de sortie a été ajouté. Ainsi, deux niveaux de tension sont possibles avec ce circuit: (i) 0-400mV et (ii) 2,5V - 2,9V. Un bloc d'offset permet de fournir un signal centré autour de 200mV et 2,7V. Une dérive autour de cette tension d'offset est de 400mV, tensions acceptables par les substrats des transistors.

IV. Résultats

Le circuit résultant est présenté en Figure 6. et la simulation du circuit avant fabrication (simulation post layout), mise en évidence en Figure 7.

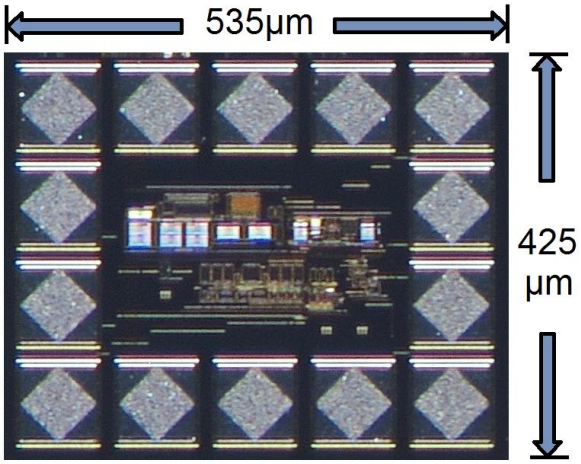

Fig 6. Photographie du test chip réalisé

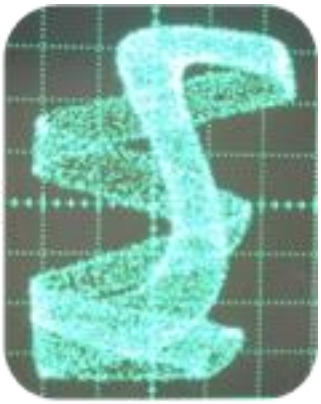

Fig 7. Test silicium du signal aléatoire de sortie

Des premiers tests ont été réalisés sur un test-chip modélisant la capacité équivalente des substrats. Ces tests ayant été concluant, les tests se sont poursuivis sur un produit 32bits. Les résultats en polarisant les substrats NMOS ont montré des résultats comparables à ceux obtenus avec la modélisation capacitive. Par contre concernant les résultats sur la polarisation des transistors PMOS, ceux-ci sont moins probants. Peut-être à cause d'un mauvais dimensionnent de la capacité de charge sur la modélisation, ou alors un souci lors de la séquence de test. Une étude de la compréhension de ce phénomène est en cours d'étude.

Concernant l'aléatoirité du signal, le NIST propose une batterie de tests de validation : FIPS 140-1 et FIPS 140-2. En effet, historiquement, ces deux successions de tests ont été développées comme outils de validation pour les systèmes de cryptage de type AES.

L'ensemble des tests NISTs ont été codés en langage Matlab et a permis de quantifier l'aléatoirité du signal résultant aussi bien d'un point de vue simulation que post fabrication. Les tests NISTs ont tous été réalisés avec succès.

V. Conclusion

Avec le marché de l'IoT en pleine expansion, ou la notion de sécurisation pour des applications telles que le bancaire, le biomédical, la domotique, etc… est incontournable, la réalisation d'une telle source ouvre de nombreuses perspectives dans la protection en locale des blocs sensibles au sein des circuits intégrés.

En plaçant une antenne à la sortie d'un signal aléatoire, cette solution pourrait ouvrir un nouveau champ d'application, la sécurisation des circuits aux attaques par champ électromagnétique…

Remerciements

Ces actions ont été menées avec un soutien du GIP-CNFM et du projet IDEFI-FINMINA ANR-2011-IDFI-017 dans le cadre du programme Grands Investissements d'Avenir (PIA1).

Références

1. Aguilar Angulo, J. A., Kussener, E., Barthelemy, H., Duval, B., Discrete chaos-based Random Number Generator, *IEEE FTFC Conference*, 2014.

2. Bucci, M., Germani, L., Luzzi, R., Trifiletti, A., Varanonuovo, M., A high-speed oscillator-based truly random number source for cryp- tographic applications on a smart card IC, *IEEE Transactions on Computers*, **52**(4), 403-409.

3. Tokunaga, C., Blaauw, D., Mudge, T., True random number generator with a metastability-based quality control, *IEEE Journal of Solid-State Circuits*, **43**(1), 78-85.
4. Matsumoto M., Yasuda S., Ohba R., Ikegami K., Tanamoto T., Fujita S., 1200um2 physical random-number generators based on SiN mosfet for secure smart-card application, *2008 IEEE International Solid-State Circuits Conference-Digest of Technical Papers*.
5. Holzer-Graf, S., Krinninger, T., Pernull, M., Schlffer, M., Schwabe, P., Seywald, D., Wieser, W., Discrete chaos-based Random Number GeneratorEfficient vector implementations of AES-based designs: a case study and new implemenations for Grostl, In Topics in CryptologyCT- RSA 2013 (pp. 145-161). Springer Berlin Heidelberg.
6. Mandal A.K., Parakash C., Tiwari, Performanceevaluationofcryptographic algorithms: DES and AES, 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), (pp. 1-5).
7. Kanai, Miyuki, Hirokazu Fujimaki, and Takeshi Shimizu, H-bridge circuit, U.S. Patent No. 7,902,884. 8 Mar. 2011.
8. Baru M. , de Oliveira O., Silveira F., A 2V rail-to-rail micropower CMOS comparator, Proceedings of the XI Conference of the Brazilian Microelectronics Society, 1996.
9. Paixao C. F., Fabris E., Bampi S. , Analysis and design of amplifiers and comparators in CMOS 0.35 um technology, Microelectronics Reliability 44.4 (2004): 657-664.
10. AMS. AMS 350nm Foundry Parameters http://ams.com/eng/Products/Full-Service-Foundry/Process-Technology/CMOS/0.35-m-CMOS-process
11. AMS. AMS 350nm Foundry Parameters http://ams.com/eng/Support/Foundry-Design-Support/Design-Documents/Process-Parameters.