Implémentation du TRNG

5.1 Introduction.

Nous avions vu dans le chapitre 2 les différentes solutions de réalisation d'un TRNG (amplification directe du bruit, échantillonnage d'oscillateurs, utilisation de fonctions physiquement non-clonables, échantillonnage de signaux chaotiques) avant de conclure sur l'intérêt de la solution d'échantillonnage de signaux chaotiques.

Ainsi, étant donné l'importance de la génération de signaux chaotiques, une étude des différentes architectures possibles répondant à nos contraintes de basse consommation a été proposée au chapitre 4. De cette étude, une solution optimale versus le cahier des charge a été testée et validée par simulation. Celle-ci est donc intégrée dans la structure TRNG proposée dans ce chapitre à laquelle viendront se rajouter quelques blocs dont la description sera proposée.

Enfin, une validation de la structure sera réalisée et mise en avant par rapport aux solutions concurrentes.

5.2 Architecture du TRNG Proposé.

Le principe d'une architecture d'oscillateur chaotique, utilisant une topologie incluant une fonction non linéaire discrète a été déjà documenté dans la littérature (i.e. [6],[35],[20]).

Nous allons utiliser dans le circuit comme générateur du signal à échantillonner la sortie de l'oscillateur chaotique et les circuits associés décrits dans le chapitre 4.

Nous associons un étage de conversion de cette source d'incertitude afin d'obtenir des patrons binaires de caractéristique aléatoire.

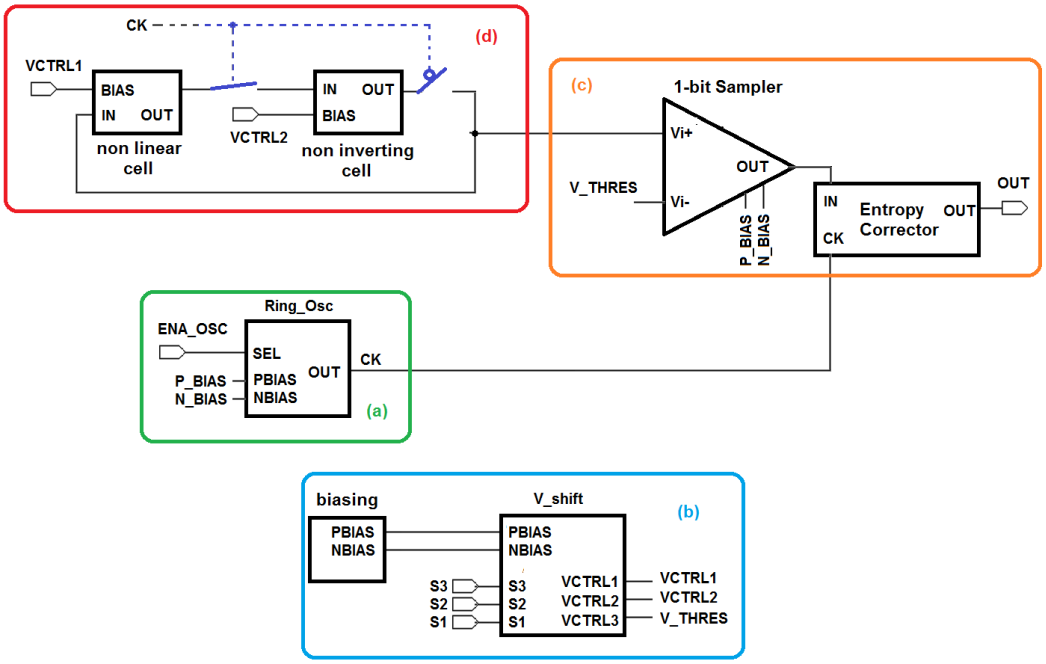

FIGURE 5.1 – Diagramme en blocs du TRNG proposè

5.2.1 Description du système.

Cette architecture en temps discret est constituée par des éléments de base présentés dans la figure 5.1 qui sont :

(a) Un oscillateur périodique, générant un signal de cadencement du système.

(b) Un circuit de polarisation du système.

(c) Un oscillateur chaotique générant un signal avec des variations d'amplitude non périodiques, utilisé comme source d'entropie.

(d) Un convertisseur du signal analogique chaotique en un signal binaire aléatoire. Il est accompagné d'un correcteur numérique d'entropie qui assure une distribution binaire uniforme des niveaux logiques '1' et '0'.

Enfin la nature chaotique, non prédictif de la sortie de l'oscillateur chaotique, permet une utilisation comme une source qui ressemble au bruit amplifié qui sera transformé postérieurement vers des variations binaires erratiques.

5.2.2 L'oscillateur chaotique.

L'oscillateur chaotique, avec le circuit de *biasing*, correspond au système décrit au sein du chapitre 4. Ainsi, comme introduit dans la figure 4.3, l'oscillateur chaotique à temps discret est constitué :

- D'un générateur d'horloge générant un signal d'horloge **CK** oscillant entre les tensions 0 et 3,3V pour une fréquence de 250kHz.
- D'un élément non linéaire et un étage suiveur qui forment une boucle de mémorisation cadencé par **CK**, en réalisant des itérations qui emmènent le circuit dans un état chaotique.
- D'une référence de tension qui permet de fournir au convertisseur 1 bit deux références de tension P_{BIAS} et N_{BIAS} dont les valeurs sont respectivement égales à 2,5V et 0,5V ainsi que les tensions de polarisation de la boucle non linéaire.

5.2.3 Convertisseur à 1 bit.

Le convertisseur à 1 bit est réalisé à partir d'un comparateur de tension. Ainsi, les signaux provenant de la sortie du bloc oscillateur chaotique, versus la sortie **OUT** sont discriminées à l'aide du convertisseur via une comparaison avec la tension de seuil V_{THRES} fournie par une référence de tension. Ainsi, les signaux générés sont binaires et peuvent être ensuite exploités par des routines numériques de quantification.

Avant de s'attaquer à la conception en tant que telle du circuit convertisseur 1 bit, une phase de modélisation a été réalisée afin de justifier de l'approche orientée par la solution proposée.

5.2.3.1 Modélisation comportementale du convertisseur 1 bit.

Afin d'appréhender la modélisation comportementale d'un convertisseur 1 bit, un certain nombre d'hypothèses doivent être définies en amont. Ainsi, nous allons considérer un comparateur possédant des caractéristiques idéales en bande passante-vitesse, soit un temps de propagation négligeable. En revanche, nous allons considérer la caractéristique d'hystérésis comme faisant partie du comparateur.

En effet, le fait de modéliser l'hystérésis nous permettra de prévoir le comportement du comparateur dans un statut de pire cas (*"worstcase"*). Cela est particulièrement identifiable lorsque le comparateur doit gérer les pics de surtension (*"overshoots"*) lors de la commutation du signal mais également lorsqu'il fait face à des variations instantanées pouvant modifier l'état de sortie

Le phénomène d'hystérésis se manifeste comme une dépendance du signal de sortie sur l'état actuel de l'entrée, ainsi que de l'antérieur à celui-ci. Dans le cas du comparateur de tension, ceci signifie le fait d'avoir deux seuils de comparaison : un seuil haut (V_{TRIP+}) et un seuil bas (V_{TRIP-}), utilisés respectivement lors de la croissance et décroissance du signal d'entrée. (figure 5.2)

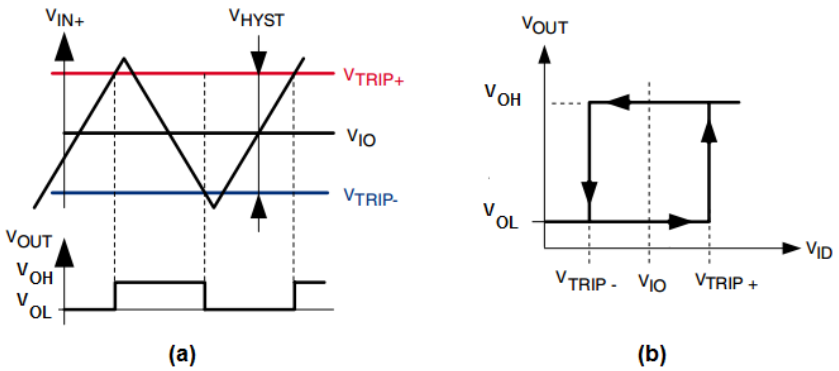

FIGURE 5.2 – Comparateur (a) Modèle (b) Caractéristique entrée V_{ID}-sortie V_{OUT}

Pour notre application (Fig.5.2.(a)), une approximation linéarisée est définie via la mise en équation suivante :

$$V_{OUT(V_{IN})} = \begin{cases} V_{OL}, & \text{si } V_{IN} \leq V_{TRIP-} \\ V_{OL}, & \text{si } V_{TRIP-} < V_{IN} < V_{TRIP+} \text{ et } V_{IN_{actuel}} < V_{IN_{anterieur}} \\ V_{OH} & \text{si } V_{TRIP-} < V_{IN} < V_{TRIP+} \text{ et } V_{IN_{actuel}} > V_{IN_{anterieur}} \\ V_{OH}, & \text{si } V_{IN} \geq V_{TRIP+} \end{cases} \tag{5.1}$$

Si à partir des équations précédents, nous exprimons la taille de la bande d'hystérésis ΔV_{TRIP} définie par :

$$\Delta V_{TRIP} = V_{TRIP+} - V_{TRIP+} \tag{5.2}$$

Nous pouvons exprimer les tensions de seuil haute et basse, ΔV_{TRIP+} et ΔV_{TRIP-}, en fonction de la tension de seuil moyenne V_{IO} via les deux équations suivantes :

$$V_{TRIP+} = V_{IO} + \frac{\Delta V_{TRIP}}{2} \tag{5.3}$$

$$V_{TRIP-} = V_{IO} - \frac{\Delta V_{TRIP}}{2} \tag{5.4}$$

Afin de répondre aux contraintes du cahier des charges précédemment fixé par les états fournis en sortie de l'oscillateur chaotique, la modélisation comportementale du comparateur 1 bit doit posséder les caractéristiques suivantes :

- V_{IO} défini par un élément externe.
- $\Delta V_{TRIP} = 20mV$
- $V_OL = 0V \rightarrow$ "0"
- $V_OH = 3.3V \rightarrow$ "1"

La bande d'hystérésis a été volontairement réduite à une valeur inférieure à 100mV (sur les simulations comportementales, nous utilisons une valeur de 20mV, i.e.), ceci représentant moins d'un dixième de la dynamique. Ainsi, la modélisation prend en

compte l'effet de l'hystérésis et son impact sur des conditions extrêmes de variations instantanées sur la dynamique (figure 5.4).

A fin d'économiser de la mémoire dans l'analyse de donnés, nous prenons des valeurs stables de tension à la sortie de l'oscillateur chaotique, à intervalles réguliers fixés par la fréquence de l'oscillateur de référence. L'inconvénient de ce modèle est l'absence des transitions dûs à la commutation des interrupteurs.

La présence de telles variations de durée instantanée peuvent avoir deux effets possibles sur la sortie du comparateur. Dans un cas idéal, des transitions instantanées instables se présentent dans ces instants. Dans une autre possibilité, l'hystérésis peut provoquer un état de mémorisation par rapport à l'évolution montée ou descente des variations de commutation.

Afin d'évaluer et de valider le comportement du modèle, nous avons considéré de telles variations. La figure 5.3 illustre le signal provenant de l'oscillateur chaotique vu dans le chapitre 4, avec des sur-sous tensions instantanées, aussi que la version plus optimiste du modèle.

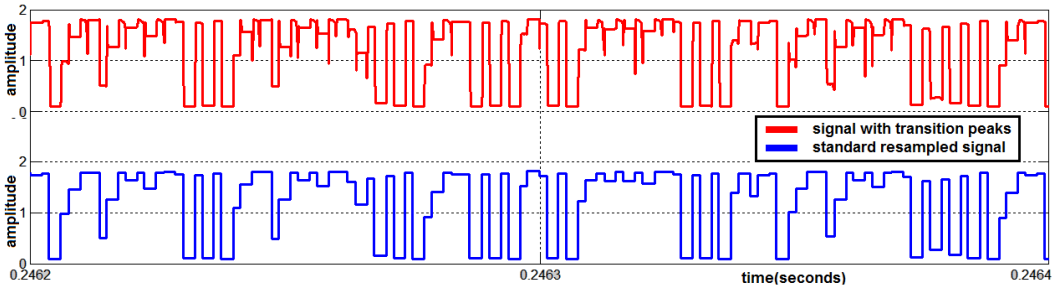

FIGURE 5.3 – Signal d'entrée du comparateur (en considérant ou pas les transitions de commutation).

La figure 5.4 illustre, sur le signal optimiste du modèle, l'action du comparateur avec et sans la bande d'hystérésis. Avec le seuil placé proche de la limite supérieure de la dynamique, $V_{THRES} = 1{,}75\text{V}$ (où les surtensions transitoires apparaissent le plus souvent). Nous pouvons observer la différence entre les deux modes qui se traduit par un effet mémoire sur les transitions consécutives, qui représente un incrément sur la quantité de zéros (ou de uns) sur la suite binaire de sortie.

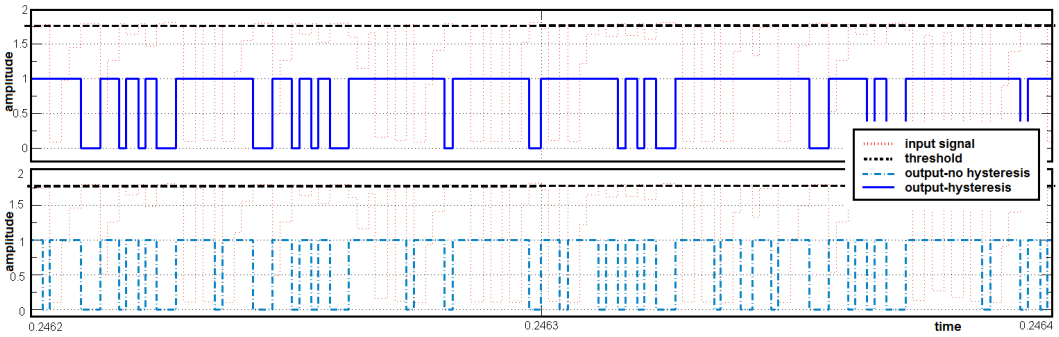

FIGURE 5.4 – Effet de l'hystérésis sur le modèle du comparateur (V_{THRES} = 1,75V).

Afin de vérifier le comportement devant des variations plus écartées , nous allons placer le seuil dans une région vers le milieu de la dynamique ($V_{THRES} = 1$V). Nous pouvons constater (figure 5.5) que l'opération du comparateur est plus classique. La modélisation de l'hystérésis n'a pas d'impact que ce soit positif ou négatif.

Nous obtenons alors bien le comportement classique d'un comparateur comme le montre la figure 5.5 , ceci étant justifié par une gamme de variation assez grande de la sortie de l'oscillateur chaotique. Pour une valeur basse, de la tension de seuil, les résultats sont identiques.

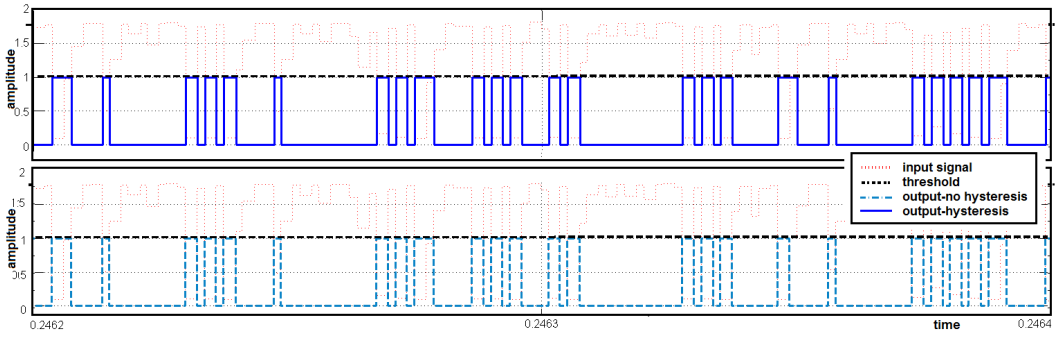

FIGURE 5.5 – Effet de l'hystérésis sur le modèle du comparateur.

La figure 5.6 illustre en termes des distributions binaires, une moyenne de résultats sur les signaux générés par le modèle de l'oscillateur chaotique.

Nous pouvons constater que la distribution binaire suit l'évolution de la tension de seuil. Nous avons donc une région près de la moitié de la dynamique possédant une distribution uniforme mais de variations très peu fréquentes, donc ayant plus de possibilités d'avoir des séquences proches du périodique. Nous allons donc favoriser la plage supérieure de la dynamique avec des variations abruptes et erratiques, qui permettront de favoriser une sortie plus équilibrée en utilisant la compensation numérique après.

L'autre point important correspond aux différences entre l'ajout d'hystérésis. La distribution pressente une variation plus importante dans le cas de seuillage dans la partie supérieure de la dynamique. Dans ce cas, l'incrément de 1's , comme vu dans la figure 5.4 implique une transition perdue et pas un 1 incrusté entre un bloc de 0's. Cette situation correspond au *worstcase*, dans lequel nous perdons de l'information en augmentant des séries de valeurs monotones.

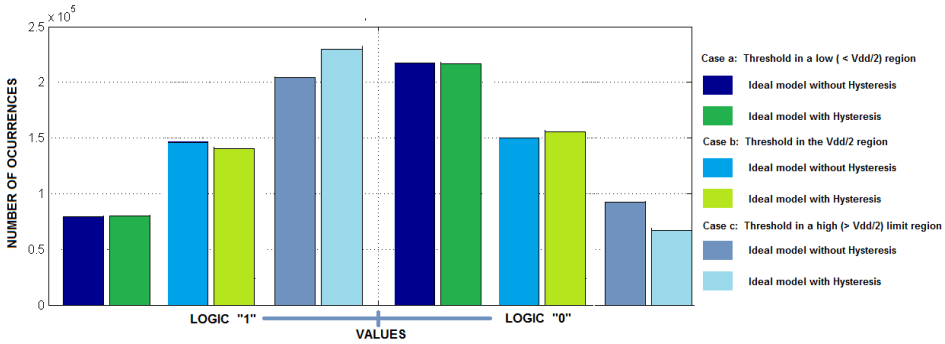

FIGURE 5.6 – L'effet de l'hystérésis dans trois placements du seuil.

Étant donné les résultats précédemment énoncés, nous avons décidé de favoriser le modèle avec hystérésis et réaliser des tests permettant d'en définir le pire cas (*"worstcase"*) de fonctionnement. Ce pire cas, nous permettra ensuite de définir la configuration à appliquer à un correcteur d'entropie placé en aval du comparateur 1 bit et dont la présentation sera abordée dans la suite de ce manuscrit.

Aux simulations précédemment abordées, les pics de commutations instantanées n'ont pas été pris en compte dans les transitions du signal. Ces pics devraient rajouter beaucoup plus d'aléa mettant en avant le modèle avec hystérésis. nous allons comparer à postériori l'hypothèse avec le fonctionnement obtenu sur les signaux de sortie de l'oscillateur chaotique, lors de la phase de simulation du circuit proposé dans la section suivante.

5.2.3.2 Conception du circuit.

Le convertisseur à 1 bit (fig. 5.7) est constitué d'un comparateur de tension auquel s'ajoute en sortie un étage de *buffer*. Cette architecture permet d'obtenir une sortie binaire de données à partir du signal analogique fourni par l'oscillateur chaotique.

Pour répondre aux contraintes de faible consommation, de rapidité, nous pouvons lister trois types de topologies de comparateurs pouvant être utilisées, soient :

- un amplificateur en boucle ouverte, sans compensation interne.
- un système avec alimentation positive, qui utilise une structure une structure similaire à une *flip-flop* afin d'augmenter la vitesse de comparaison
- un système avec capacités commutées.

De ces trois topologies, seule la structure en boucle ouverte semble répondre à nos contraintes. En effet, les autres topologies requièrent d'un signal d'horloge plus rapide que celui de la référence que nous utilisons pour l'oscillateur chaotique. Ainsi, en terme de consommation mais aussi de complexité aussi bien sur la phase de conception que de modélisation des états métastables, ces deux dernières solutions ont été mises de coté au profit de la solution en boucle ouverte.

Ainsi, pour réaliser cette structure en boucle ouverte, nous avons utilisé un comparateur contenant un OTA du type ***rail-to-rail***, basé sur une architecture "symétrique" [5], comme le montre la figure 5.7. Cette architecture utilise deux amplificateurs différentiels (N et P) en parallèle. Ainsi, pour de faible tension d'entrée, l'amplificateur N est inactif alors que l'amplificateur P est opérationnel. A tension d'entrée élevée, c'est l'opération inverse qui se déroule.

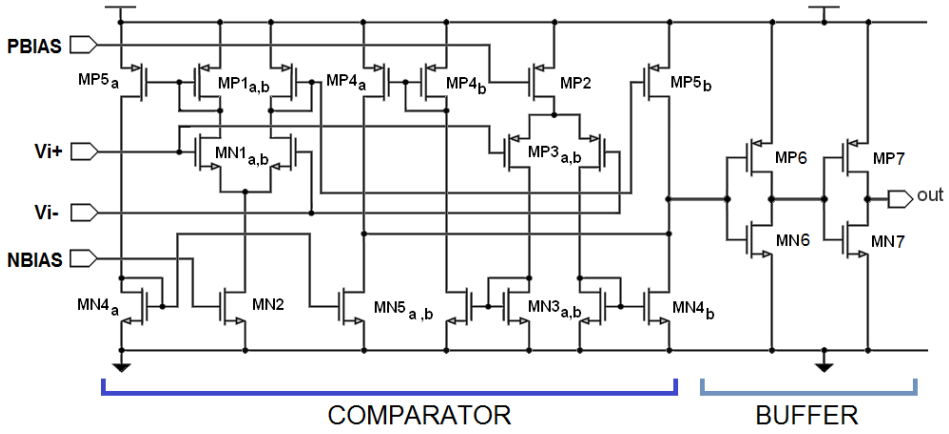

FIGURE 5.7 – OTA-Comparateur (a) schématique (b) symbole

La règle garantissant un fonctionnement en mode *rail-to-rail* est de disposer d'une tension d'alimentation suffisante pour avoir l'équation ci dessous vérifiée :

$$V_{DD} \geq V_{GS_p} + V_{GS_n} + 2V_{D_{sat}} \tag{5.5}$$

Où les tensions V_{GS_n} et V_{GS_p} correspondent respectivement aux tensions grille-sources des transistors de chaque paire différentielle d'entrée, $MN1[a,b]$ et $MP3[a,b]$. La tension $V_{D_{sat}}$ correspond à la tension minimale de drain dans les transistors qui opèrent comme sources de courant ($MN2$ et $MP2$).

Le seuil de référence est établi par une tension provenant du circuit de références programmable introduit dans le chapitre précédent. Dans un but d'optimisation de la consommation, l'amplificateur utilise une faible courant de polarisation. Il est donc nécessaire d'ajouter un étage d'adaptation en sortie du comparateur.

Les variations à la sortie de l'amplificateur en boucle ouverte sont finalement adaptées afin de convenir aux niveaux digitaux. Ceci a été réalisé à l'aide d'un *buffer* de sortie formé par deux inverseurs CMOS (constitués des transistors **MN6/MP6** et **MN7/MP7**). Il permet en même temps d'augmenter la capacité de sortie du circuit.

5.2.3.3 Dimensionnement des composants.

Le dimensionnement des composants du comparateur est délicat dans le sens ou les deux amplificateurs N et P doivent fonctionner de façon alternée. En effet, si un recouvrement de la zone de fonctionnement apparaît, cela permet d'ôter les problématiques de linéarité sur la zone centrale mais au profit d'une sur-consommation sensible. Par ailleurs, le fonctionnement de ce comparateur a été calibré pour fonctionner à basse consommation, d'où les tailles des transistors possédant des longueurs plus conséquentes que les largeurs. Ainsi, le tableau 5.1 résume les tailles ayant été retenues.

Transistors	Dimensions	Transistors	Dimensions
MP1(a :b)	$\frac{2\times2}{15}$	MN1(a :b)	$\frac{7\times1}{5}$
MP2	$\frac{4\times2}{15}$	MN2	$\frac{4\times1}{5}$
MP3(a :b)	$\frac{4}{0.5}$	MN3(a :b)	$\frac{2\times1}{5}$
MP4(a :b)	$\frac{2\times1}{5}$	MN4(a :b)	$\frac{2\times2}{15}$
MP5(a :b)	$\frac{2\times2}{15}$	MN5(a :b)	$\frac{2\times1}{5}$

TABLE 5.1 – Dimensionnement du comparateur

Les deux cellules inverseuses placées l'une derrière l'autre, assurent la fonctionnalité de *buffer*. Ils assurent ainsi la remise en forme du signal pour être exploité d'un point de vue digital pour la suite du circuit. La taille des composants est proposée dans le tableau 5.2

Cellules inverseuse 1		Cellule inverseuse 2	
MP1	MN1	MP2	MN2
$\frac{2\times0.45}{15}$	$\frac{0.5}{15}$	$\frac{2\times0.5}{5}$	$\frac{0.5}{5}$

TABLE 5.2 – Dimensionnement du buffer de sortie

5.2.3.4 Résultats.

Après avoir validé d'un point de vue simulation le fonctionnement du comparateur, celui ci a été réalisé sur silicium. L'importance de la symétrisation de la structure

est importance via la prise en compte de notion de *matching*. Ceci a été bien pris en compte via la taille des transistors retenue, comme le montre la figure 5.8

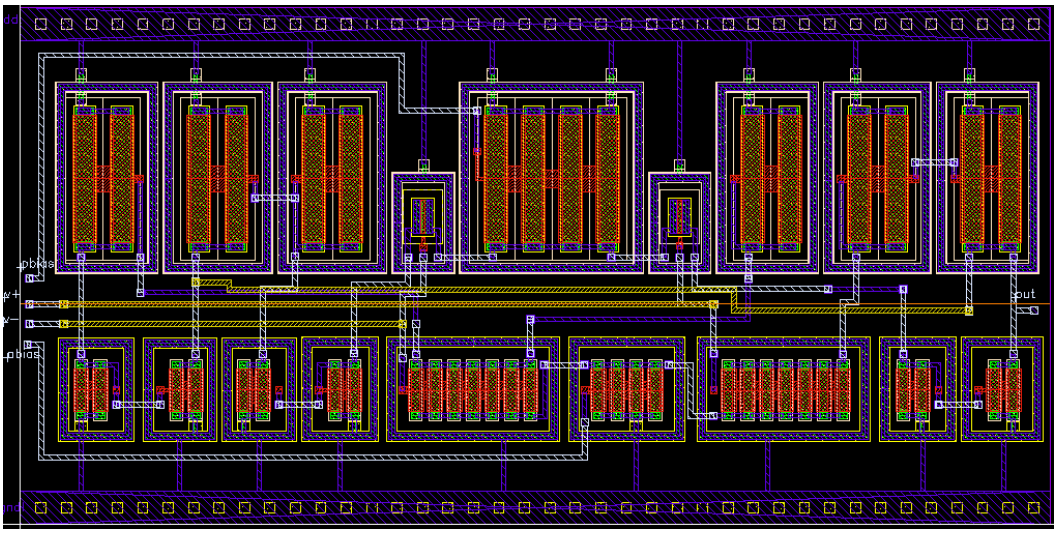

FIGURE 5.8 – Layout de la cellule OTA.

La figure 5.9 indique la réponse, en fréquence en magnitude et en phase de l'OTA en boucle ouverte sous différentes valeurs de charge. Nous allons travailler sur une faible capacité de charge avant de connecter vers le *buffer*, donc la plage de 200fF correspond correctement à nos besoins (même si dans le système lae marge de phase n'apporte aucun intérêt lorsqu'on est en boucle ouverte).

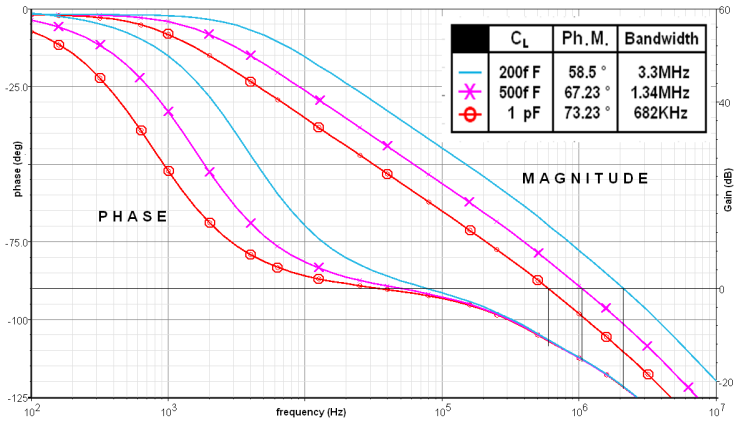

FIGURE 5.9 – Réponse en fréquence de l'OTA.

La figure 5.10 indique les formes d'onde à la sortie du circuit et du *buffer*, sous un signal d'entrée sinusoïdale d'amplitude 3V et fréquence 200kHz, et une capacité de charge de 500fF. La figure indique un déphasage du signal en sortie du comparateur ainsi qu'une dégradation du signal attendue (on commence à sortir de la zone de gain constant), mais avec le buffer de sortie nous arrivons à récupérer le signal carré

souhaité en phase. En termes de consommation, le système requiert une moyenne de 600nA, et en repos 440nA, avec une surtension de commutation de 1μA.

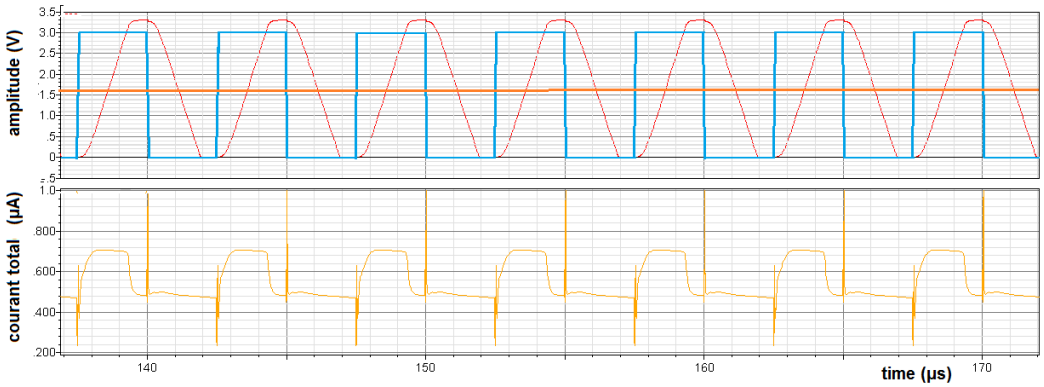

FIGURE 5.10 – Réponse transitoire du comparateur.

5.2.4 Correcteur d'entropie.

Comme décrit précédemment, un générateur 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 obtenue échantillonné (synchronisé), peut avoir une distribution biaisé (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 corrélés.

Le rôle du bloc de post-traitement est d'améliorer les propriétés statistiques de la séquence binaire. D telles améliorations impliquent une réduction sur le débit de sortie.
Parmi les correcteurs numériques nous pouvons citer les suivants :

Correcteur XOR.

C'est le correcteur le plus simple. Il consiste à appliquer une fonction *ou exclusif* sur des blocs de taille fixe avant les envoyer à la sortie. L'avantage de cette technique est la quantité réduite de composants nécessaires, par contre, le débit de sortie est

réduit proportionnellement à la taille du groupe de bits du correcteur utilisés pour générer un bit debiasé.

Correcteur de Von Neumann.

Ce type de correcteur utilise une fonction non linéaire qui réalise une discrimination pour réduire les séries de valeurs répétitives et consécutives.
Une telle discrimination permet idéalement d'enlever le *biasing* et obtenir une distribution uniforme. L'inconvénient de cette solution c'est la réduction du débit de sortie ainsi que la faiblesse contre des signaux avec des traces de périodicité (des groupes de séquences aléatoires qui se répètent, comme dans le cas des PRNG-LFSR).

Correcteur du type LFSR.

Le *LFSR*[1] est un correcteur basé sur une fonction linéaire. Ce type de circuit est souvent utilisé dans la création de PRNGs, du au fait que :

- L'implémentation matérielle d'un LFSR est relativement simple
- les séquences de sortie possèdent de bonnes propriétés statistiques
- Leur comportement peut être modélisé mathématiquement et algorithmiquement.

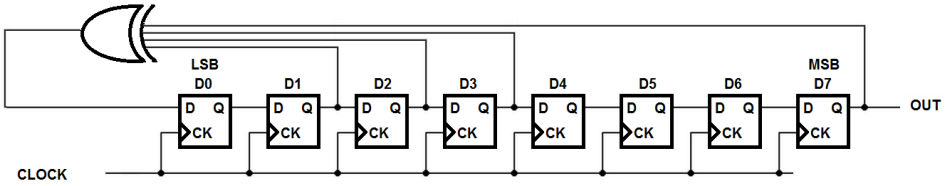

FIGURE 5.11 – Correcteur du type LFSR avec *taps* externes

Un *LFSR* de taille L consiste en L registres en cascade de 1 bit, synchronisés par un même signal d'horloge (fig. 5.12). Cette association permet de stocker les L-1 dernières données à la sortie de chaque registre au bout de chaque coup d'horloge.
Les opérations que véhiculent les registres cascadés choisis sur un polynôme générateur (*taps*) correspondent à la somme (modulo 2)[2].
Le polynôme générateur du LFSR possède la forme :

$$f_{(X)} = a_1 X_1 \oplus a_2 X_2 \oplus \cdots \oplus a_{L-1} X_{L-1} \tag{5.6}$$

De forme qu'à chaque coup d'horloge ($a_L = [0, 1]$),

$$X_1 = f_{(x)} \tag{5.7}$$
$$X_2 = X_1 \ldots \tag{5.8}$$
$$X_{L-1} = X_{L-2} \tag{5.9}$$

1. Linear Feedback Shift Register
2. opérateur ou exclusif

Par exemple, pour un LFSR à 8 bits (figure 5.12.a), le polynôme générateur de ce LFSR associé, d'ordre 7 est :

$$X_7 \oplus X_3 \oplus X_2 \oplus X_1 = f_{(X)} \tag{5.10}$$

Cette architecture, associée aux solutions proposées par le polynôme, produit un cycle de 128 valeurs pseudo aléatoires. Ce patron se répète cycliquement, comme le montre la figure 5.13.(a).

L'intérêt de ce type de système réalimenté est d'assurer la possibilité de disposer d'une distribution binaire équiprobable ou près de l'équiprobable.

Afin de profiter de la caractéristique de la distribution uniforme d'un LFSR, nous allons exécuter une opération additionnelle, avec un bit provenant d'une source aléatoire biaisée (*random seed*).

Dans ce cas, la séquence de sortie du LFSR devient non prédictive et non reproductible, avec une distribution binaire uniforme (figure 5.12).

5.2.5 Choix retenu.

Afin de rester sur un système simple, nous nous sommes orientés sur l'intégration d'un montage de type compression linéaire, autour d'un *LFSR* comme correcteur d'entropie et générateur de valeurs aléatoires.

Ainsi, la première étape a été de quantifier la taille de l'équation caractéristique du LFSR et donc du nombre de registres nécessaires à son implémentation. Pour cela, un jeu de simulation comportementales réalisés à partir des données récupérées des simulations (BSIM) de l'oscillateur chaotique, suivi du comparateur nous a permis de valider l'effet du correcteur ainsi que son architecture.

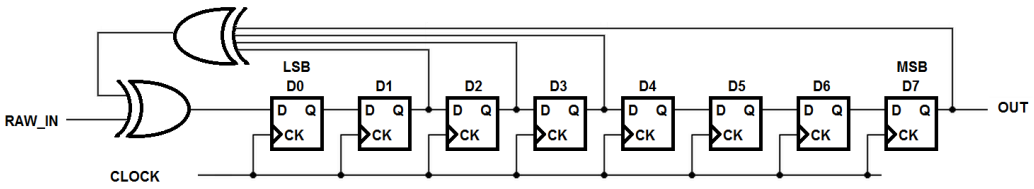

FIGURE 5.12 – Correcteur du type LFSR avec *taps* externes.

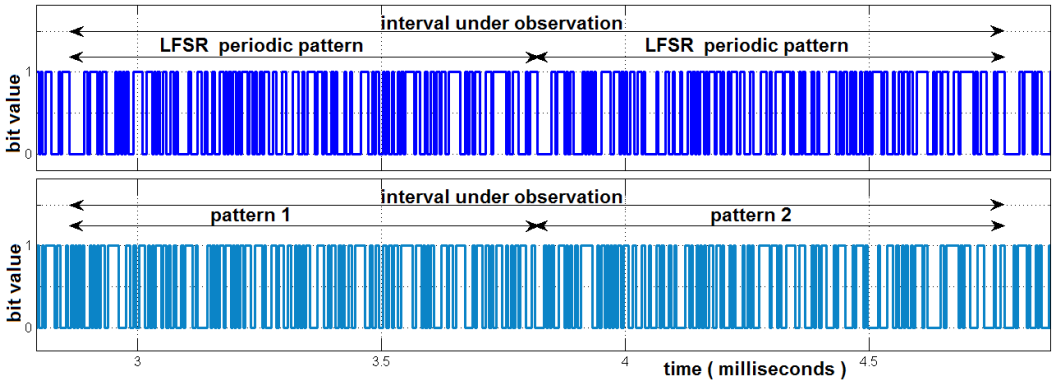

FIGURE 5.13 – LFSR
(a)independant-PRNG (b)avec injection du signal biaisé.

Une représentation statistique des résultats est illustrée en figure 5.14, montrant de façon complémentaire que l'effet d'injecter un signal biaisé aléatoire sur le LFSR n'affecte pas la distribution uniforme caractéristique d'un LFSR, mais ne fait qu'annuler l'effet cyclique des patrons aléatoires, inhérents d'un LFSR.

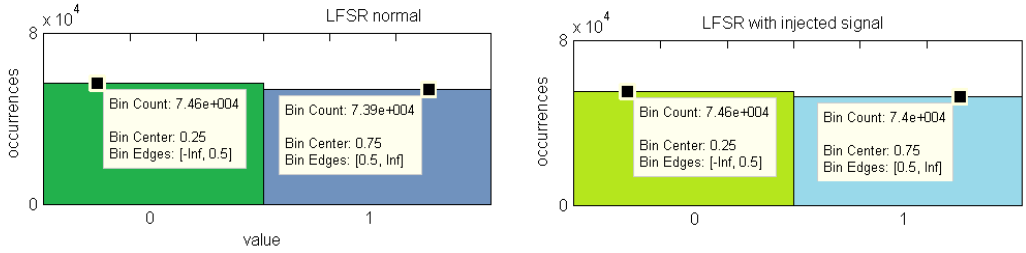

FIGURE 5.14 – Distribution binaire (a)LFSR solo (b) avec injection du signal biaisé.

Finalement, une topologie avec un LFSR de 8 bits avec la fonction affecté sur les taps **[8 6 5 4 1]** sera utilisée.

5.3 Réalisation sur silicium.

Une fois l'architecture de l'oscillateur chaotique validée, comme il a été montré au chapitre 4, auquel s'est ajoutée la validation de la structure convertisseur 1 bit (section 5.2.3), corrigée par le correcteur d'entropie (section 5.2.4), l'intégration de l'ensemble de ces blocs a été possible via la réalisation sur silicium en technologie AMS 0.35μm.

Ainsi, à l'aide des outils de Cadence, via les chaines Virtuoso et Layout XL, une architecture complète a été réalisée comme le montre la figure 5.15.

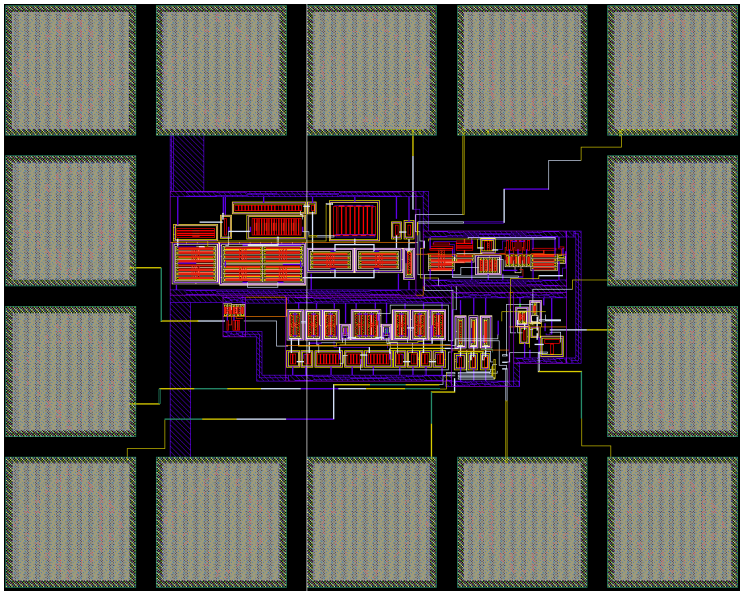

FIGURE 5.15 – Layout du subsystème.

La figure 5.16 illustre le circuit obtenu ayant une taille de $535\mu m \times 425\mu m$, incluant les plots.

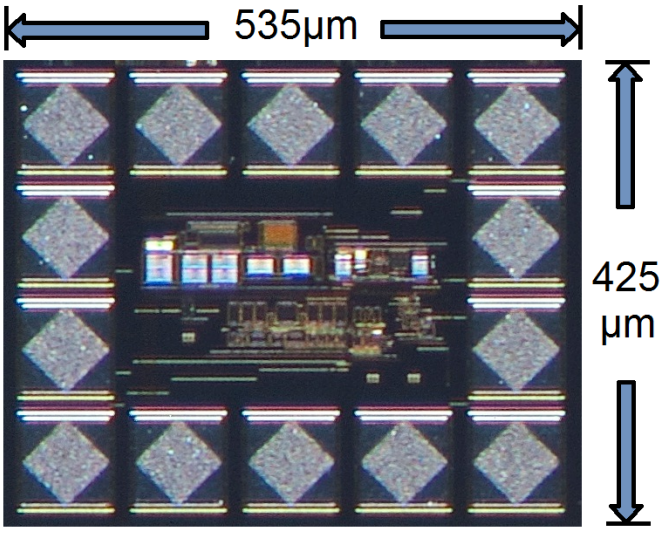

FIGURE 5.16 – Photographie du test chip réalisé.

Configuration Physique des broches.

La figure indique la distribution de pins sur le circuit integré fabriqué, mis sour boitier du type DIL14.

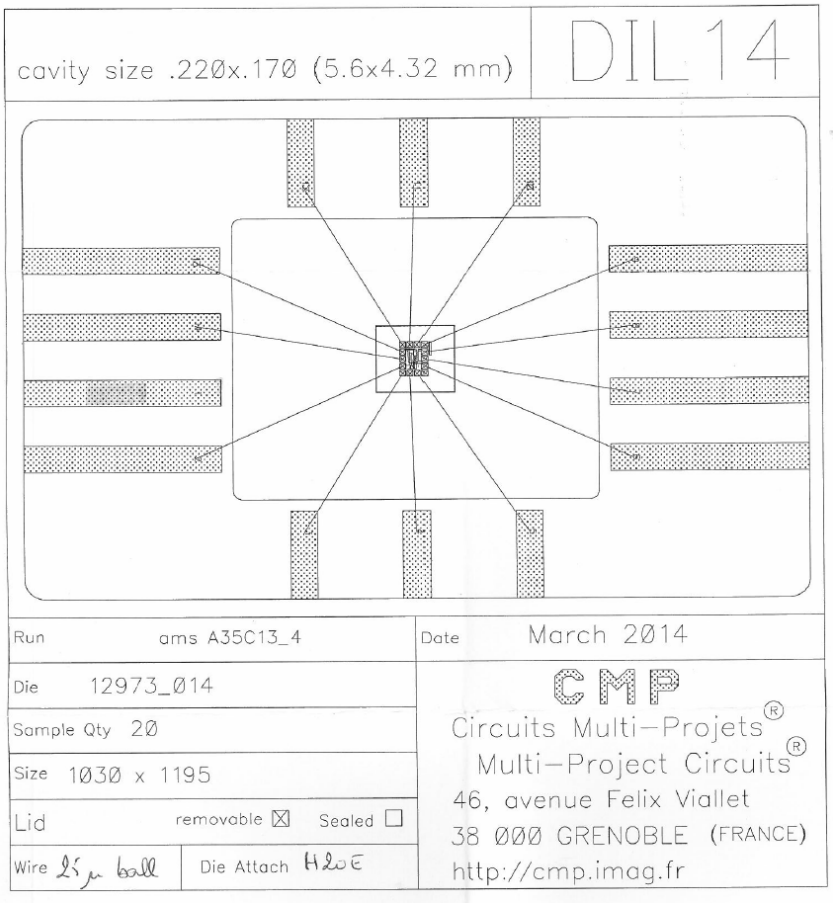

FIGURE 5.17 – Distribution des broches sur le chiptest

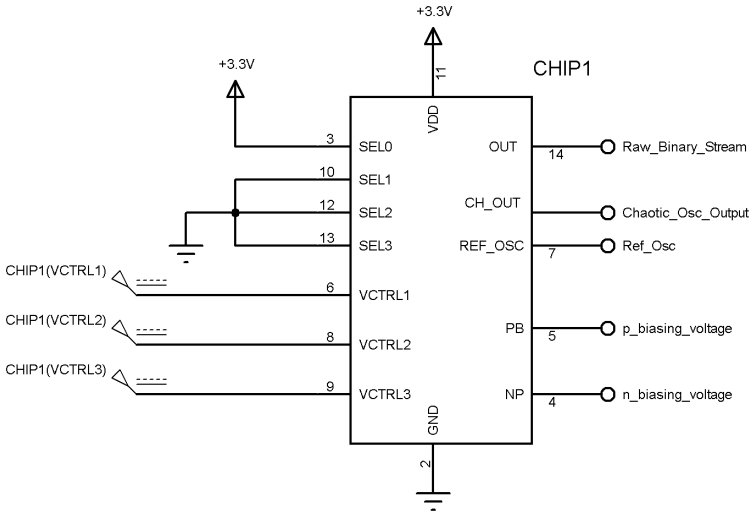

FIGURE 5.18 – Configuration de test sur le chiptest

5.4 Influence des conditions de tests.

De la même façon que sur l'expérience de Lorenz ([25]), nous avons constaté que le changement des paramètres de précision du calculateur entrainait des résultats ayant des caractéristiques différentes pendant la phase de simulation.

Notamment, l'ajout d'un délai avant le démarrage du système ou le changement du pas de simulation (paramètre *tstrobe*), ceci dans le but d'accélérer le temps de calcul pour avoir une quantité plus élevé de données génère des résultats de BSIM sur le signal chaotique différents à chaque changement de conditions.

Dans la partie de simulations pré-post Layout, l'une des caractéristiques du simulateur spectre est d'assigner par défaut des pas d'échantillonnage dynamique, en fonction de la convergence sur le signal de sortie. Cette particularité génère une quantité de points sur les transitions brusques, présents sur l'oscillateur chaotique qui fait des transitions plus des surtensions de commutation.

Afin d'avoir des pas réguliers sur les transitions plus stables du signal, nous sommes obligés de "normaliser" les données, permettant par la même occasion de réduire l'espace mémoire dans le logiciel d'analyse que nous utilisons (MatLab). Ceci est réalisé via une synchronisation du signal avec les transitions du signal d'horloge de référence.

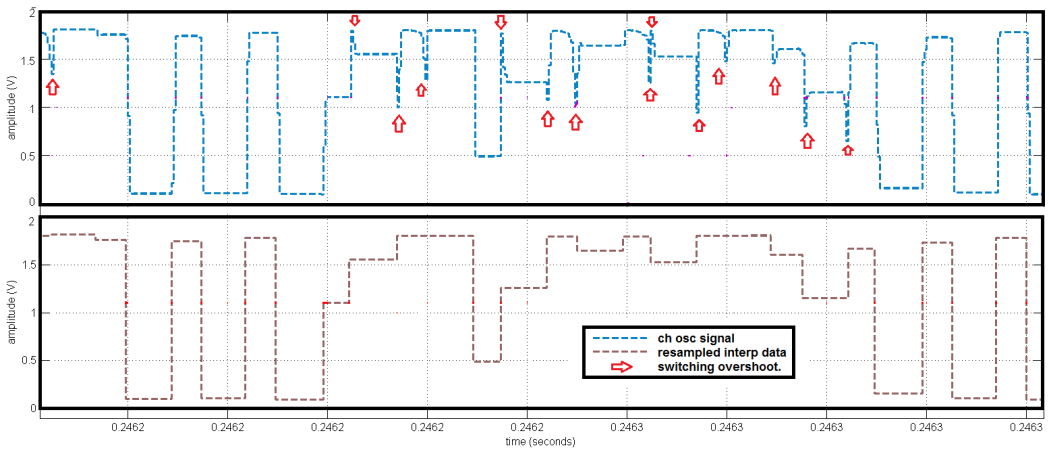

FIGURE 5.19 – Discrimination des surtensions du à la commutation du système lors de l'interpolation et re-échantillonnage du signal acquise.

Nous réalisons ensuite une interpolation-reéchantillonnage de données avec un pas constant, afin de normaliser et discrétiser sur des transitions . Nous perdons alors les transitions de commutation de l'oscillateur chaotique (figure 5.19), mais nous gagnons de la vitesse de calcul, espace mémoire et une réussite du 100 % pour la détection de changements de niveau sur la sortie du convertisseur à 1 bit (figure

5.20).

La figure 5.20 illustre le résultat de la normalisation de données avant et après avoir appliqué l'interpolation et raffiner le méthode de calcul. Les deux chronogrammes indiquent le signal de sortie de simulation avec un pas non uniforme ni aucune re-synchronisation comparé avec la sortie de l'oscillateur chaotique soumis au modèle du comparateur. Ainsi ,l'un prend en compte la sortie sans aucun traitement et un comparateur idéal ; tandis que l'autre prend la sortie normalisée et un comparateur avec un seuil pour comparer la validité de l'approche de la modélisation. Nous pouvons observer des bits qui sont perdus avec un comparateur idéal, alors qu'avec les signaux resynchronisés, les résultats du modèle et de la sortie normalisée sont les mêmes.

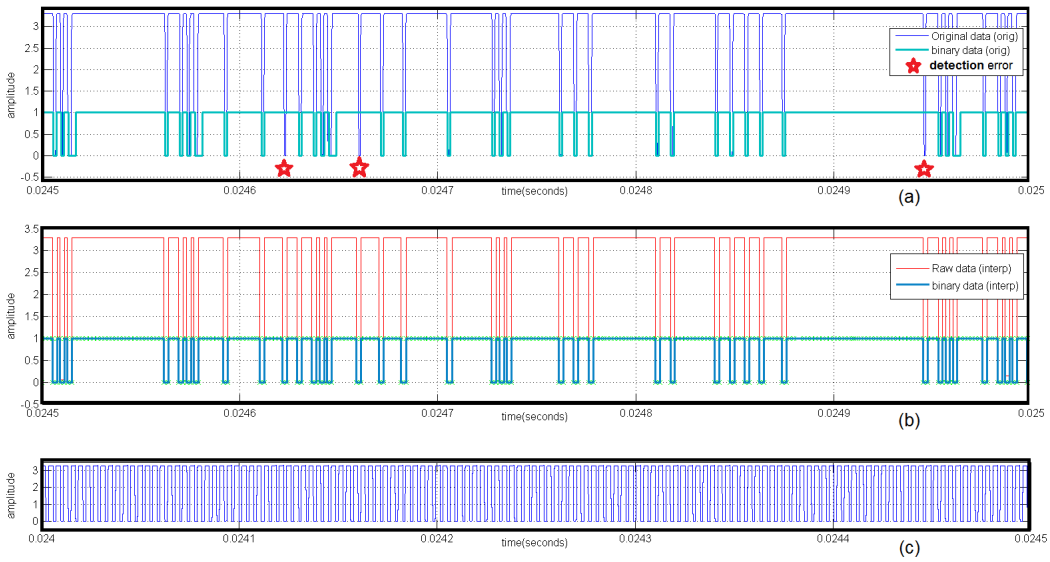

FIGURE 5.20 – Erreur de détection de données et correction par interpolation.

Chaque changement d'état correspond à une demi-période du signal d'horloge CLK, ce qui correspond a un débit de donnés brut de 500Kbps (approx), sur les conditions de test post Layout sur spectre.

Cependant l'implantation matérielle ajoute des capacitances parasites sur certains plots, notamment sur ceux qui etaient censés d'être une partie interne de la structure du systeme (sortie chaotique, sortie d'horloge de référence, biasing interne de base du circuit). Leurs caractéristiques se sont dégradées avec la présence des impédances (notamment du coté capacitif) des plots, en réduisant le débit de sortie.

La configuration des pins pour le test s'observe dans la figure 5.18. Cette dégradation a fait varier les points de biasing du circuit (n_{bias}, p_{bias}) et a eu une influence sur les points d'opération de la polarisation du système non linéaire par defaut. Deux options de récalibration possibles ont été choisis : un changement des tensions de

polarisation du circuit non linéaire, soit une variation sur la tension d'alimentation. Parmi les deux, la variation sur la tension d'alimentation de 3V à 2.7V a été la plus efficace, répétitive et avec moins d'influence par rapport à la charge des plots du test-chip parmi les chips testés du batch fabriqué. En revanche , la fréquence de sortie à été affectée (i.e. la fréquence de l'oscillateur changée de 250Khz à 140Khz) ainsi que les effets capacitifs en sortie sont plus observables.

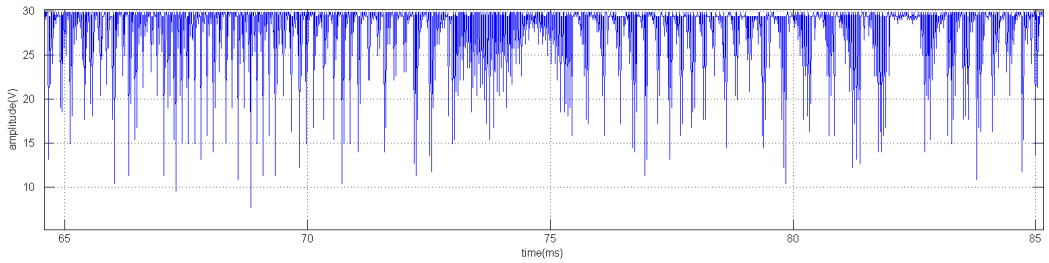

FIGURE 5.21 – Sortie Chaotique apres récalibration.

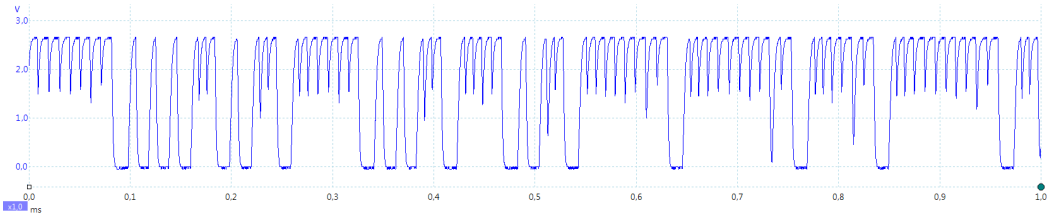

FIGURE 5.22 – détail de la sortie binaire sur le testchip.

Comme conditionnement sur les mesures de la sortie binaire aléatoire,(figures 5.21 et 5.22) nous avons utilisé une porte logique standard CMOS, afin de passer sur la plage exploitable pour la mesure avec le banc de test de la carte MyRio.

5.5 Conclusion.

Après avoir présenté l'oscillateur chaotique, bloc central du générateur d'aléa au sein du chapitre 4, celui-ci a été intégré au sein du TRNG afin de pouvoir en extraire les résultats exploitables pour le passage des tests d'aléa que nous étudierons dans le chapitre suivant.

Ainsi, après avoir explicité la structure du TRNG avec l'introduction de blocs de conversion entre une information analogique fournie par l'oscillateur chaotique et l'aspect de traitement numérique des informations, une présentation des résultats obtenus a été présentée que ce soit au niveau simulation pré, post Layout ou sur Silicium.

Malgré les effets des plots d'implantation sur certaines parties sensibles du circuit, le comportement aléatoire est maintenu, ainsi que le comportement chaotique du système non linéaire, avec une dégradation sur le débit du signal (qui passe à 70Kbps)

L'influence des variables sur l'oscillateur invalident les mesures de courant du circuit, étant donnée que pour une fréquence inférieure, les surtensions de commutation seront considerablement inférieures à celles obtenues sur le test d'extraction post-Layout sur Cadence.
Enfin, une présentation des résultats et l'impact de certains paramètres sur la structure a été mise en avant afin de justifier les conditions de test et les résultats associés. Partant de ces résultats, le passage aux différents tests d'aléa va être proposé dans le chapitre suivant afin de quantifier le caractère aléatoire du signal obtenu.