QUATORZIEME COLLOQUE GRETSI - JUAN-LES-PINS - DU 13 AU 16 SEPTEMBRE 1993

Un circuit intégré pour la simulation de Canal Gaussien

D. Degrugillier, G. Graton, M. Jézéquel.

Laboratoire "Circuits Intégrés Télécom"
Ecole Nationale Supérieure des Télécommunications de Bretagne
Technopôle de Brest-Iroise B.P. 832, 29285 Brest Cedex, France.

RÉSUMÉ

Cet article présente l'architecture et les performances d'un circuit intégré à application spécifique (ASIC) qui permet la simulation d'un canal gaussien à des rapports signal à bruit programmables, dans une grande plage de bruit (entre -5 et +15 dB, par pas de 0.1 dB). Ce circuit, construit autour d'algorithmes numériques, se substitue complètement au banc de caractérisation analogique du canal. Le générateur numérique, implanté sur une technologie CMOS précaractérisé 1µm à deux niveaux de métal, fournit plus de 40 millions d'échantillons de bruit blanc gaussien par seconde.

ABSTRACT

This paper presents the architecture and the performances of an ASIC for digital noise generation. This circuit allows the simulation of a gaussian channel with programmable signal-noise ratio between -5 and +15 dB, by steps of 0.1 dB. The noise generator chip, built with a digital algorithm, takes the place of the analogue characterisation bench of the channel. This ASIC, integrated in 1µm double metal level CMOS standard cells technology, allows the generation of over 40 million samples of gaussian white noise per seconde.

1. INTRODUCTION

La mise au point des systèmes de communications numériques (son, image, données) requiert une bonne connaissance du canal de transmission, dont la simulation est faite par des moyens logiciels et matériels. Dans ce dernier cas, l'emploi d'un générateur de bruit analogique pour modéliser le canal rend indispensable l'utilisation d'un convertisseur analogique-numérique pour permettre l'analyse numérique en aval du système. De plus, il est souvent très compliqué de fixer et reproduire précisément les caractéristiques de bruit du type de canal considéré; en particulier, la mesure de la puissance de bruit s'effectue à l'aide d'un appareillage (filtres, voltmètres,...) haut de gamme et demande beaucoup de précautions.

Une alternative à la complexité de la caractérisation du bruit est la génération programmée de ce bruit, sous une forme matérielle proche de ce qui est réalisé par le logiciel. Le générateur de bruit, construit autour d'algorithmes numériques, peut alors se substituer complètement au banc de caractérisation analogique du canal.

C'est l'objet de cet article qui présente l'architecture et les performances d'un circuit intégré à application spécifique (ASIC) permettant la simulation d'un canal qui vérifie les impératifs statistiques d'un bruit blanc gaussien à des rapports signal à bruit programmables, dans une grande plage de bruit (entre -5 dB et +15 dB, par pas de 0.1 dB). Nous présentons donc l'algorithme de génération du bruit numérique blanc gaussien avant d'aborder l'architecture et les performances du circuit intégré correspondant.

2. ALGORITHME DE GENERATION DU BRUIT BLANC GAUSSIEN

La génération du bruit blanc gaussien consiste à générer une variable aléatoire Y qui suit la loi gaussienne de valeur moyenne $\mu=0$ et de variance $\sigma^2= (2.E/N_0)^{-1}$ où E/N_0 représente le rapport signal à bruit, la puissance moyenne du signal étant normalisée à 1. De plus, la fonction d'autocorrélation doit être égale à σ^2 à la position 0 ($R_y(0)=\sigma^2$) et nulle ou négligeable ailleurs pour qu'il soit blanc.

2.1 Génération de variables aléatoires

Une variable aléatoire de fonction de distribution donnée peut être obtenue à partir d'autres distributions, plus simples, généralement de l'équidistribution. En ce qui nous concerne, pour obtenir la distribution gaussienne, nous supposons pouvoir générer une variable aléatoire uniformément répartie entre 0 et 1, qui constitue la base de construction de la variable gaussienne désirée.

En réalité, une variable aléatoire qui représente le bruit du canal doit être continue. Cependant, dans notre cas, comme pour celui de simulations sur ordinateur, cette variable est approximée par une suite de valeurs discrètes (échantillons) dont la répartition suit la loi de Gauss avec les paramètres σ et μ cités ci-dessus.

2.1.1 Génération de variables aléatoires uniformes

Générer une variable aléatoire uniforme est équivalent à générer une suite de nombres entiers aléatoires entre 0 et M (M entier grand) qui sont normalisés par rapport à M et par

conséquent réduits dans l'intervalle [0,1]. Toutefois, nous nous contenterons du caractère pseudo-aléatoire des nombres générés si ceux-ci respectent les conditions suivantes: la distribution des nombres est uniforme; les nombres générés sont statistiquement indépendants; les séquences de nombres peuvent être reproduites après une période donnée, la plus longue possible; l'algorithme de calcul du nombre aléatoire est rapide et son implantation sur silicium est possible. La méthode des registres à décalage bouclés de longueurs maximales satisfait ces conditions [1]. Nous présentons, figure 1, un registre à décalage bouclé de longueur maximale avec N=4 étages, de polynôme générateur $h(D)= 1 + X + X^4$. Après initialisation par un mot de 4 bits (différent de 0 0 0 0), le registre génère une séquence périodique de bits de période $2^N-1=15$.

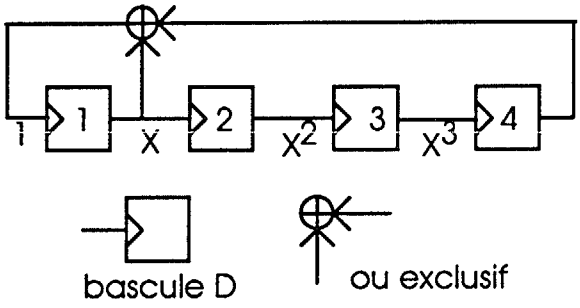

Figure 1-Registre à décalage bouclé

Afin de disposer de nombres pseudo-aléatoires, il faut regrouper les bits générés de façon à pouvoir les interpréter comme des nombres. La méthode choisie consiste à prendre L bits à partir de L sorties de bascules du registre où $2^L-1=M$. Ainsi, un nombre pseudo-aléatoire , codé sur L bits, est généré à chaque période d'horloge qui rythme le registre à décalage. Ces nombres prennent leurs valeurs dans l'intervalle [0, 2^L-1] ou dans l'intervalle [0,1[après normalisation par 2^L. En fait, la normalisation par 2^L n'est pas utile. En effet, nous pouvons considérer que chaque donnée, codée sur L bits, représente la partie fractionnaire du nombre pseudo-aléatoire. Dans ce cas, un nombre pseudo-aléatoire codé sur L bits, qui prend ses valeurs dans l'intervalle [0, 1[, est obtenu directement à chaque période d'horloge du registre. Cette méthode donne de très bons résultats statistiques à condition de respecter certaines conditions [1].

2.1.2 Génération de variables aléatoires gaussiennes.

La méthode retenue est celle de la somme asymptotique. Elle applique le théorème de la Limite Centrale qui s'énonce comme suit: "La somme de p variables aléatoires indépendantes, de même loi de distribution, de moyenne μ et de variance σ^2, converge vers la loi de distribution gaussienne, de moyenne $p\mu$ et de variance $p\sigma^2$, lorsque p croît. Ainsi, avec p variables pseudo-aléatoires uniformes indépendantes X_i (i=1 à p), de valeurs dans l'intervalle [0,1[, de moyenne $\mu_{Xi}=1/2$ et de variance $\sigma_{Xi}^2=1/12$, la variable pseudo-aléatoire $Y= X_1+X_2+...X_p$ est approximativement gaussienne, de moyenne $\mu_Y=p/2$ et de variance $\sigma_Y^2=p/12$. L'algorithme de génération du bruit blanc gaussien peut alors être le suivant: à partir de p registres à décalage bouclés de longueurs maximales, on génère p variables pseudo-aléatoires uniformes indépendantes X_i (i=1 à p) de valeurs dans l'intervalle [0,1[; la somme de ces p variables X_i puis la soustraction par la quantité p/2 donne une variable pseudo-aléatoire approximativement gaussienne, de valeurs dans l'intervalle [-p/2 ; +p/2[; enfin, la multiplication de Y par la quantité $\sigma(12/p)^{1/2}$ produit une variable gaussienne de moyenne nulle et de variance σ^2.

2.2 Résultats de simulation

Dans le but de valider notre choix de méthode, de nombreuses simulations ont été réalisées. Elles consistent dans le calcul des fonctions de distribution et d'autocorrélation. Elles ont été exécutées à partir d'un programme écrit en C qui décrit le comportement de l'algorithme de génération précédent. Le programme comportemental est initialisé par: le nombre de générateurs pseudo-aléatoires et leurs polynômes correspondant; le mot d'initialisation pour chaque registre à décalage bouclé de longueur maximale et les sorties de bascules utilisées pour la génération des nombres pseudo-aléatoires uniformes codés sur L bits à chaque période d'horloge; les conditions de calcul des fonctions de distribution et d'autocorrélation. Ces différentes possibilités de programmation nous ont permis de déterminer les caractéristiques des registres pseudo-aléatoires et des variables uniformes générées à partir de ces registres pour satisfaire les impératifs du cahier des charges.

Les figures 2a et 2b donnent les résultats obtenus relativement aux fonctions de distribution et d'autocorrélation, respectivement, dans le cas de 16 registres à décalage bouclés de longueurs maximales d'au moins 15 étages où chaque registre génère une variable pseudo-aléatoire uniforme codée sur 11 bits.

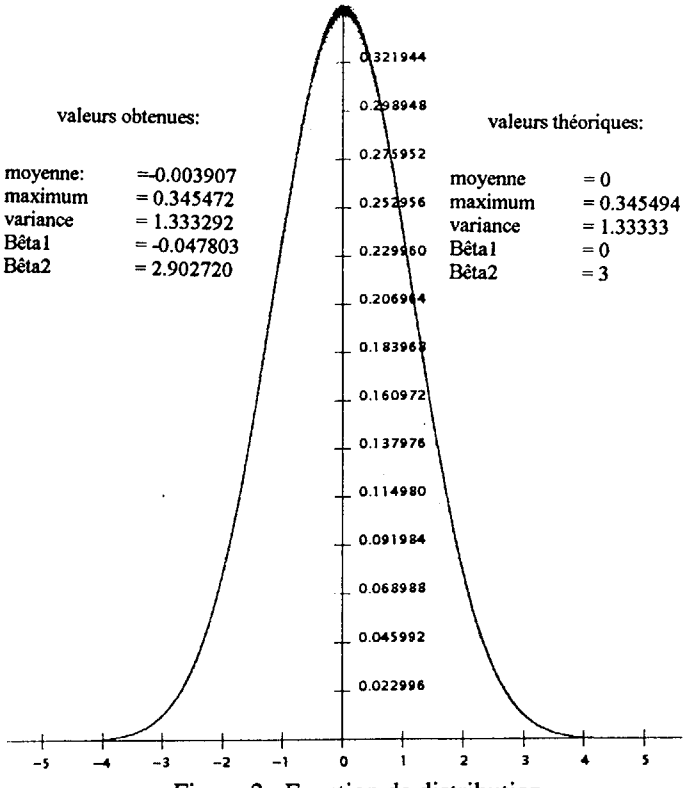

Figure 2a-Fonction de distribution

En ce qui concerne la figure 2a, on donne en légende, les valeurs théoriques et celles issues de la simulation, de la

moyenne, du maximum de la fonction, de la variance et des coefficients de "skewness" (Bêta 1) et "kurtosis" (Bêta 2) qui testent la nature gaussienne de la courbe [2]. Dans notre cas, on doit avoir Bêta 1 = $\mu_3^2/\mu_2^3 = 0$ et Bêta 2 = $\mu_4/\mu_2 = 3$ où μ_i est le moment d'ordre i. Les résultats obtenus pour 10^8 échantillons sont corrects avec toutefois une erreur effective sur la moyenne et les termes Bêta1 et Bêta2. Cette erreur est dûe au fait que le générateur délivre une variable pseudo-aléatoire dans l'intervalle [-p/2; +p/2[. Pour corriger cette erreur d'intervalle à droite ouvert, il faut ajouter à la variable normale une quantité égale à un demi-quantum de l'intervalle [-p/2; +p/2[c'est à dire $1/2.2^{-11}.16 = 2^{-8}$.

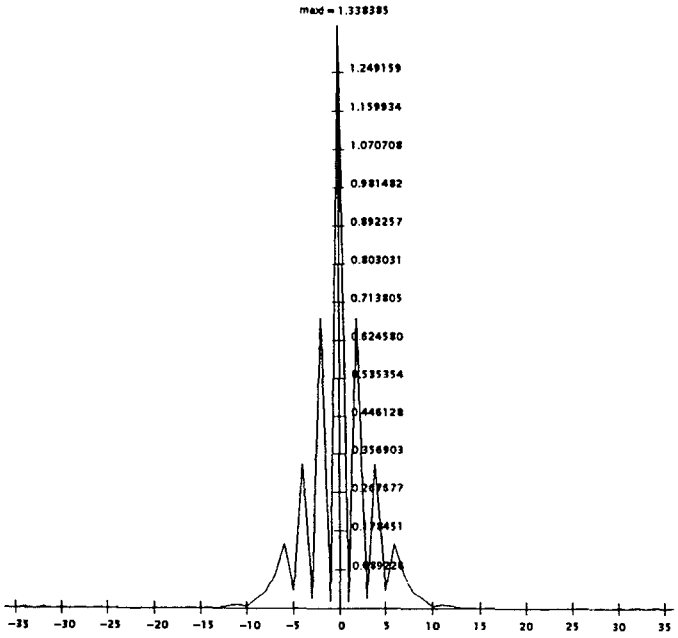

Figure 2b- Fonction d'autocorrélation

La courbe d'autocorrélation de la figure 2b, obtenue pour 10^6 échantillons, ne satisfait pas les spécifications du générateur de bruit blanc gaussien. En effet, on a bien une valeur proche de σ^2 en 0, mais la fonction ne s'annule pas partout ailleurs. Toutefois, on peut remarquer la présence de minimums notamment en K=±5; ±10; ...Aussi, en prenant un échantillon sur 5 consécutifs, la forme de la fonction d'autocorrélation se rapproche fortement de celle du bruit blanc.

On note r'_i la valeur contenue dans la $i^{ème}$ bascule d'un registre à décalage bouclé de longueur maximale au temps t et r_i la valeur au temps t-1. On a:

$$\begin{pmatrix} r'_1 \\ r'_2 \\ r'_3 \\ r'_4 \\ . \\ . \\ r'_{n-1} \\ r'_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & b_3 & . & . & b_{n-2} & b_{n-1} & b_n \\ 1 & 0 & 0 & . & . & 0 & 0 & 0 \\ 0 & 1 & 0 & . & . & 0 & 0 & 0 \\ 0 & 0 & 1 & . & . & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & 1 & 0 & 0 \\ 0 & 0 & 0 & . & . & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \\ . \\ . \\ r_{n-1} \\ r_n \end{pmatrix}$$

où $b_1, b_2, b_3,...,b_{n-1}, b_n$ sont les coefficients du polynôme générateur du registre à décalage bouclé de longueur maximale.

On élève la matrice de transfert à la puissance 5. Le générateur pseudo-aléatoire obtenu avec les nouvelles valeurs de la matrice donne la séquence désirée. L'avantage de cette méthode réside dans le fait que le registre à décalage bouclé modifié est synchronisé avec la même fréquence d'horloge que le registre initial.

Les résultats, après correction de la fonction de distribution, donnent une courbe similaire à celle de la figure 2a. On obtient pour cette courbe: moyenne=0.0000; maximum=0.344940; variance=1.333310; Bêta1=-0.009785; Bêta2=2.918922.

La figure 3 donne les résultats, après correction, de la fonction d'autocorrélation. Elle satisfait le cahier des charges proposé.

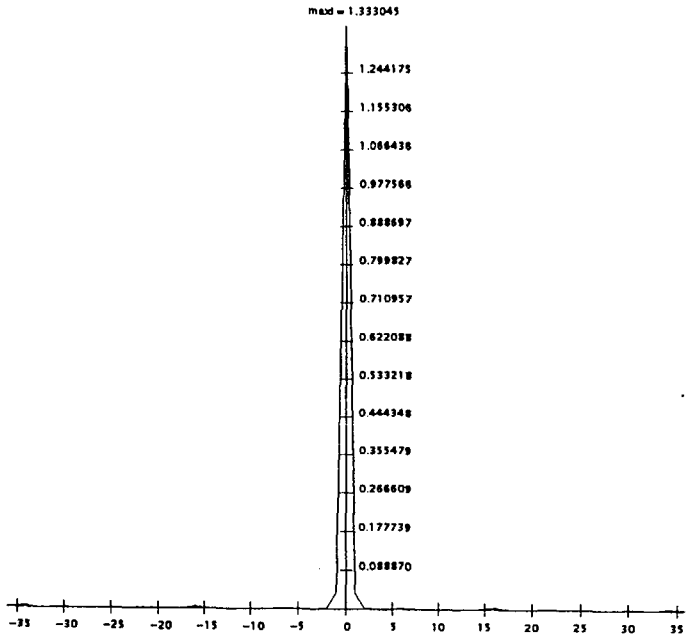

Figure 3- Fonction d'autocorrélation corrigée.

3. ARCHITECTURE DU CIRCUIT

3.1 Réalisation du générateur de variables uniformes

On peut générer les 16 variables pseudo-aléatoires uniformes codées sur 11 bits par l'intermédiaire de 16 registres à décalage bouclés. Toutefois, cette solution conduit à une surface silicium nécessaire importante. De plus, élever la matrice de transfert à l'ordre 5 augmente le nombre de termes non nuls dans cette matrice et, de ce fait, complique la structure de chacun de ces registres.

Une autre méthode consiste en l'utilisation de générateurs multiports modulo 2 dont la description et la synthèse sont décrites dans [3]. Toutefois, cette méthode ne s'applique que lorsque le facteur de réduction de la fréquence (5 dans notre cas) est une puissance entière de 2 .

Pour réaliser le générateur de variables uniformes, nous avons donc choisi une solution intermédiaire que nous résumons dans les tableaux 1 et 2

Le tableau 1 donne la valeur de la période de quelques polynômes générateurs d'ordre allant de 15 à 21.

En particulier, on écrit la période en produits de nombres premiers. Ceci nous permet de rejeter tous les polynômes dont la période contient le chiffre 5 comme facteur premier.

polynôme	période
$x^{15}+x^{14}+1$	32767= 7.31.151
$x^{16}+x^{15}+x^{13}+x^{4}+1$	65535=3.5.17.257
$x^{17}+x^{14}+1$	131071=131071
$x^{18}+x^{7}+1$	262143=3^3.7.19.73
$x^{19}+x^{18}+x^{17}+x^{14}+1$	524287=524287
$x^{20}+x^{17}+1$	1048575=3.5^2.11.31.41
$x^{21}+x^{19}+1$	2097151=7^2.127.337

Tableau 1

Le tableau 2 donne les valeurs de la puissance N, pour chacun des polynômes restants, qui satisfont à la simplicité d'écriture des matrices de transfert correspondantes (minimum de 1 dans la matrice et donc minimum de OU EXCLUSIF dans la structure du registre). Il nous faut 16 variables uniformes dont 4 sont issues des 4 polynômes qui ont des solutions. Il nous reste donc 12 variables uniformes à générer à partir des matrices de transfert.

polynôme	Puissance N
$x^{15}+x^{14}+1$	-
$x^{17}+x^{14}+1$	9297,9298 18597
$x^{18}+x^{7}+1$	52375,52376,52377 104754,104755 126254
$x^{19}+x^{18}+x^{17}+x^{14}+1$	5296,5297,5298 10597 264789 à 264792 473929,473930
$x^{21}+x^{19}+1$	35,36,37,38 7586,7587 60760 1048579 à 1048584 1078952 à 1078955

Tableau 2

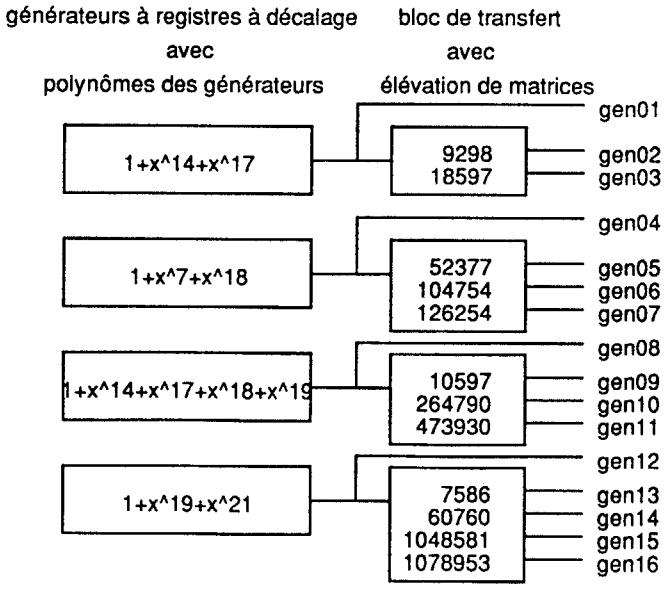

Figure 4-Architecture du bloc de génération

La figure 4 présente l'architecture du bloc de génération des 16 variables aléatoires uniformes. Elle est constituée des 4 registres à décalage bouclés et des 4 blocs de transfert réalisés avec des OU EXCLUSIF relativement aux matrices correspondantes.

Cette structure confère au générateur une période de $5.4*10^{21}$ échantillons ce qui correspond à $4*10^6$ années pour une fréquence d'horloge du générateur de 40 Mhz. Les simulations effectuées avec ce bloc de génération donnent des résultats tout à fait comparables à ceux des figures 2a et 3.

3.2 Architecture du circuit

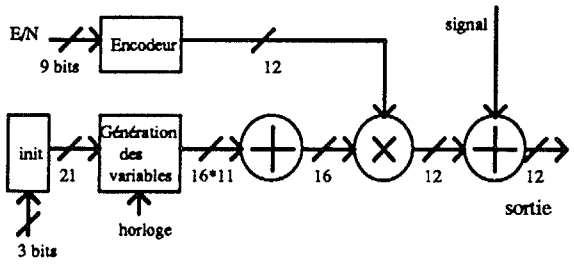

Figure 5 - Architecture du circuit

La figure 5 présente l'architecture du circuit. Elle est composée de : une cellule de génération des 16 variables uniformes discutée ci-dessus; une cellule pour initialiser les registres à décalage bouclés, manuellement ou par programmation; une cellule d'addition qui calcule la somme des 16 variables uniformes codées sur 11 bits. A la sortie de cette cellule on a une variable gaussienne codée sur 16 bits de valeur moyenne nulle et de variance égale à 16/12; une cellule pour la multiplication entre la variable gaussienne et la quantité $\sigma' = \sigma(12/16)^{1/2}$ codée sur 12 bits où σ est l'écart-type de la variable normale désirée; une cellule d'encodage qui calcule la quantité σ' à partir du rapport signal à bruit codé sur 9 bits; une cellule d'addition qui calcule la somme du signal avec le bruit blanc gaussien.

4. CONCLUSION

Le générateur de bruit numérique blanc gaussien a été conçu à l'aide des outils COMPASS. Les différentes simulations logiques effectuées ont permis de valider son bon fonctionnement jusqu'à des fréquences de 40 Mhz. Son retour de réalisation sur silicium en technologie CMOS précaractérisé 1µm à 2 niveaux de métal de ES2 est prévue fin 1993. Ce circuit permettra la simulation d'un canal gaussien et facilitera ainsi la contitution du banc de caractérisation de systèmes de communications numériques.

Références

[1]: J.K. HOLMES
"Cohérent spread spectrum systems"
Willey-Interscience Publication, New York 1982

[2]: P.R. KRIHNAIAH
"Analysis of variance"
"Handbook of statistics 1"
North Holland Publishing Company
Amsterdam, New York, Oxford 1980

[3] O. BRUGIA - M. PIOLI - W. WOLFOWICZ
"Multiport modulo-2 générators of pseudorandom binary séquences"
Proc Int-Symp on Circuits and Systems.
Roma, 1982, pp 852-855.