(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
25 novembre 2010 (25.11.2010)

PCT

(10) Numéro de publication internationale
WO 2010/133795 A1

(51) Classification internationale des brevets :
G06F 7/58 (2006.01) *G06F 7/48* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2010/050955

(22) Date de dépôt international :
18 mai 2010 (18.05.2010)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0953362 20 mai 2009 (20.05.2009) FR

(71) Déposant *(pour tous les États désignés sauf US)* :
FRANCE TELECOM [FR/FR]; 6 place d'Alleray, F-75015 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* :
KOUNTOURIS, Apostolos [FR/FR]; 3 rue Saint-Joseph, F-38000 Grenoble (FR).

(74) Mandataire : **FRANCE TELECOM R&D/PIV/BREVETS**; BENETIERE Marion, 38-40, rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

[Suite sur la page suivante]

(54) Title : GENERATION OF PSEUDORANDOM NUMBERS

(54) Titre : GENERATION DE NOMBRES PSEUDO-ALEATOIRES

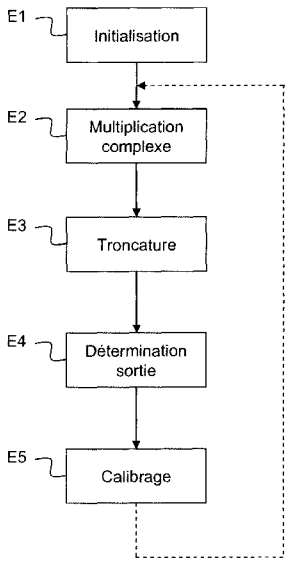

Fig. 2

E1... Initialization
E2... Complex multiplication
E3... Truncation
E4... Determination of output
E5... Calibration

(57) Abstract : The invention relates to a method for generating real signed pseudorandom numbers represented on an integer number w of bits, wherein said method comprises: an initialization step (E1) that includes determining an initial complex number and at least one multiplier, said multiplier being a complex number; a multiplication step (E2), for a given iteration, of a multiplicand by the multiplier; a truncation step (E3), by the application of a truncation function, of the real portion and of the imaginary portion of the multiplication result, respectively, the truncation result making it possible to determine the multiplicand of the following iteration and the truncation error making it possible to determine a pseudorandom number; and a calibration step (E5) for obtaining the multiplicand of the following iteration. The number of iterations is determined by the amount of pseudorandom numbers to be generated.

(57) Abrégé : L'invention concerne un procédé de génération de nombres pseudo-aléatoires réels signés représentés sur un nombre w entier de bits, lequel procédé comporte des étapes : d'initialisation (E1) comportant la détermination d'un nombre complexe initial et d'au moins un multiplicateur, lequel multiplicateur est un nombre complexe; de multiplication (E2), pour une itération donnée, d'un multiplicande par le multiplicateur; de troncature (E3), par application d'une fonction de troncature, respectivement de la partie réelle et de la partie imaginaire du résultat de la multiplication, le résultat de la troncature permettant de définir le multiplicande de l'itération suivante et l'erreur de troncature permettant de définir un nombre pseudo-aléatoire; de calibrage (E5) pour obtenir le multiplicande de l'itération suivante. Le nombre d'itérations est déterminé par la quantité de nombres pseudo-aléatoires à générer.

WO 2010/133795 A1

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))*

Génération de nombres pseudo-aléatoires

Le domaine de l'invention est celui de la génération de nombres pseudo-aléatoires (PRNG pour *Pseudo-Random Number Generator* en anglais). Plus précisément, l'invention concerne la génération de nombres pseudo-aléatoires notamment, mais pas seulement, pour des architectures matérielles contraintes en puissance de calcul, en mémoire et en énergie.

Il existe une multiplicité d'applications utilisant la génération de nombres pseudo-aléatoires que ce soit pour de la simulation, de l'analyse, de la prise de décision, de la sécurité informatique ou encore de la cryptographie, etc.

Parallèlement, il existe de nombreuses techniques de génération de nombres pseudo-aléatoires. Dans le livre intitulé, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, troisième édition Addison-Wesley, 1997, D. E. Knuth dresse un panorama assez exhaustif des techniques de génération et des générateurs de nombres pseudo-aléatoires existants ainsi que des tests envisagés pour l'évaluation de leur qualité.

Pour des architectures contraintes en puissance de calcul, en mémoire et en énergie, deux types de générateurs de nombres pseudo-aléatoires présentent un plus grand intérêt que les autres étant donné leur simplicité. Il s'agit des générateurs basés sur les registres à décalage et des générateurs linéaires basés sur l'arithmétique modulaire.

Un registre à décalage est tel que la série de bits obtenue en sortie du registre est décalée par rapport à la série de bits présentée en entrée. Par exemple, si on considère une série de 4 bits 1001 présentée en entrée d'un registre à décalage à droite, en sortie on obtient B100 où B est un bit aléatoire égal à 0 ou 1. On constate facilement qu'avec un seul registre on n'obtient qu'un seul bit aléatoire pour un traitement.

Si on souhaite générer un nombre aléatoire représenté sur plusieurs bits, on a alors deux solutions.

La première solution consiste à mettre en parallèle autant de registres à décalage que de bits aléatoires à générer. Cette première solution présente l'inconvénient d'être longue pour l'initialisation et coûteuse en matériel.

La deuxième solution consiste à répéter l'opération autant de fois que de bits aléatoires à générer. Cette deuxième solution présente l'inconvénient d'accroître le temps de génération d'un nombre aléatoire.

Un générateur linéaire basé sur l'arithmétique modulaire est tel que les nombres pseudo-aléatoires obtenus forment une suite dont chaque terme dépend du précédent selon la formule suivante :

$$S_{n+1} = (a \cdot S_n + c) \bmod d$$

où :

- S_n et S_{n+1} sont deux termes (ou deux nombres) consécutifs de la suite,
- a est un multiplicateur,
- c est un incrément,
- mod correspond au modulo et d au module (opération permettant de définir la congruence entre deux nombres).

La qualité d'un tel générateur dépend fortement du choix des paramètres a, c et d mais aussi du premier terme de la série (S_0).

En outre, ce type de générateur utilise des opérations en arithmétique modulaire ce qui génère une grande complexité sauf dans le cas particulier où d est une puissance de 2 et réduit, dans le cas général, la vitesse de génération d'un nombre aléatoire.

Les générateurs basés sur les registres à décalage et les générateurs linéaires basés sur l'arithmétique modulaire présentent tous les deux l'inconvénient, pour un procédé de génération itératif, d'utiliser en entrée du générateur le nombre obtenu en sortie lors de l'itération précédente. Ainsi, l'état interne du générateur est connu. Ceci rend impossible l'utilisation directe de tels générateurs dans des applications de sécurité ou de cryptographie.

Un des buts de l'invention est de remédier aux inconvénients de l'art antérieur précité.

Ainsi, la présente invention concerne, selon un premier aspect, un procédé de génération de nombres pseudo-aléatoires réels signés représentés sur un nombre w entier de bits, lequel procédé comporte des étapes :

- d'initialisation comportant la détermination d'un nombre complexe initial et d'au moins un multiplicateur, lequel multiplicateur est un nombre complexe,

- de multiplication, pour une itération donnée, d'un multiplicande, lequel multiplicande est un nombre complexe, par le multiplicateur, le résultat de la multiplication étant un nombre complexe dont la partie réelle et la partie imaginaire sont représentées sur 2w bits; le multiplicande de la première itération étant le nombre complexe initial,

- de troncature, par application d'une fonction de troncature, respectivement de la partie réelle et de la partie imaginaire du résultat de la multiplication, le résultat de la troncature permettant de définir le multiplicande de l'itération suivante et l'erreur de troncature permettant de définir un nombre pseudo-aléatoire,

- de calibrage pour obtenir le multiplicande de l'itération suivante sous la forme d'un nombre complexe dont la partie réelle et la partie imaginaire sont des nombres réels signés représentés sur le nombre w entier de bits et dont le module est compris entre une donnée minimum et une donnée maximum prédéfinies.

Le nombre d'itérations est déterminé par la quantité de nombres pseudo-aléatoires à générer.

Le procédé de génération de nombre pseudo-aléatoires selon l'invention repose sur un calcul simple de multiplication de nombres complexes se traduisant par des multiplications et des additions de nombres réels.

Le procédé présente une grande capacité en pouvant générer au moins w bits aléatoires par itération.

L'opération de troncature permet de scinder en deux parties le résultat de la multiplication, la partie permettant de générer un nombre pseudo-aléatoire pouvant être connue et la partie permettant de générer le multiplicande suivant restant secrète. Ainsi, l'état interne du générateur n'est pas révélé par la sortie du générateur.

Selon une caractéristique préférée, la partie réelle et la partie imaginaire du multiplicateur sont des nombres réels signés représentés sur le nombre w entier de bits, le module du multiplicateur étant compris entre une valeur minimum et une valeur maximum prédéfinies et la valeur absolue du produit de la partie réelle par la partie imaginaire étant supérieure à une troisième valeur prédéfinie.

Selon une caractéristique préférée, la valeur minimum est égale à 1 et la valeur maximum est égale à 2.

Les conditions remplies par le multiplicateur permettent de définir un procédé de génération de nombres pseudo-aléatoires de bonne qualité en évitant les inconvénients d'un calcul récursif qui peut dégénérer et tendre vers l'obtention du même nombre à chaque itération ou encore devenir périodique de telle sorte qu'un même nombre est périodiquement généré.

Selon une caractéristique préférée, la partie réelle et la partie imaginaire du nombre complexe initial et du multiplicande sont des nombres réels signés représentés sur le nombre w entier de bits et le module du nombre complexe initial et le module du multiplicande sont compris entre la donnée minimum et la donnée maximum prédéfinies.

La détermination du nombre complexe initial est arbitraire dans un ensemble de nombres complexes dont la partie réelle et la partie imaginaire sont des nombres réels signés représentés sur un nombre w entier de bits et dont le module est compris entre un minimum et un maximum prédéfinis.

L'étape de calibrage permet de s'assurer que le multiplicande utilisé pour une itération donnée satisfait aux mêmes conditions que le nombre complexe initial.

Selon une caractéristique préférée, la fonction de troncature appartient à la liste suivante :

- fonction partie entière,
- fonction partie entière par excès,
- fonction d'arrondi.

Les différentes fonctions de troncature sont équivalentes du point de vue de la génération de nombres pseudo-aléatoires. Néanmoins le fait de pouvoir choisir entre différentes fonctions de troncature offre une plus grande souplesse pour la mise en œuvre du procédé.

Selon une caractéristique préférée, l'étape d'initialisation comporte la détermination du nombre w entier de bits.

Ainsi, le procédé selon l'invention offre une grande flexibilité et est facilement adaptable en fonction de l'application dans laquelle il est mis en œuvre.

Selon une caractéristique préférée, l'étape d'initialisation comporte la détermination de la fonction de troncature.

Ce choix d'initialisation supplémentaire augmente la difficulté pour un observateur malveillant de trouver la configuration du générateur par une approche essai/erreur directe. Ceci présente un intérêt pour les applications de sécurité informatique.

Selon une caractéristique préférée, le procédé selon l'invention comporte une étape de détermination d'une sortie, laquelle sortie est un nombre pseudo-aléatoire obtenu par concaténation d'un premier nombre de bits les plus significatifs de l'erreur de troncature de la partie réelle et d'un deuxième nombre de bits les plus significatifs de la partie imaginaire du résultat de la multiplication.

Selon une caractéristique préférée, la sortie déterminée est sur w bits et le premier nombre et le second nombre sont égaux à $\frac{w}{2}$.

L'avantage de cette approche est que les bits de poids faible qui peuvent engendrer des périodicités courtes du procédé de génération de

nombres pseudo-aléatoires sont éliminés. Un autre avantage est que l'obtention du nombre pseudo-aléatoire généré en sortie se fait avec un minimum d'opérations.

Selon une caractéristique préférée, le procédé selon l'invention comporte une étape de détermination d'une sortie, laquelle sortie est un nombre pseudo-aléatoire sur w bits obtenu à partir respectivement d'une opération effectuée entre un nombre entier h positif de bits les plus significatifs et le même nombre h de bits les moins significatifs de l'erreur de troncature de la partie réelle et de la même opération effectuée entre le nombre entier h positif de bits les plus significatifs et le même nombre h de bits les moins significatifs de la partie imaginaire du résultat de la multiplication.

Cette opération permet de mélanger les bits de poids faible avec les bits de poids fort. Cette solution est particulièrement avantageuse pour des applications pour lesquelles il est souhaitable de limiter les contraintes sur les paramètres d'initialisation (notamment du multiplicateur).

Selon une caractéristique préférée, l'opération est un OU exclusif.

Cette opération de mélange est la plus simple.

Selon une caractéristique préférée, le procédé selon l'invention comporte la prédétermination d'une valeur seuil de nombre d'itérations et l'initialisation d'un compteur du nombre d'itérations, lequel compteur du nombre d'itérations est incrémenté à chaque itération de telle sorte que lorsque la valeur du compteur du nombre d'itérations atteint la valeur seuil de nombres d'itérations on change le multiplicateur.

Ceci permet d'éviter un nombre trop important d'itérations avec le même multiplicateur et permet donc d'obtenir un procédé de génération de nombres pseudo-aléatoires de bonne qualité dans la mesure où grâce à cette approche il n'est pas possible de retrouver périodiquement le même nombre pseudo-aléatoire en sortie.

Selon une caractéristique préférée, le procédé selon l'invention comporte la prédétermination d'une valeur seuil de nombre d'itérations et l'initialisation d'un compteur du nombre d'itérations, lequel compteur du

nombre d'itérations est incrémenté à chaque itération de telle sorte que lorsque la valeur du compteur du nombre d'itérations atteint la valeur seuil de nombres d'itérations, le multiplicande est remplacé par un nombre complexe dont la partie réelle et la partie imaginaire sont des nombres réels signés représentés sur le nombre w entier de bits et dont le module est compris entre la donnée minimum et la donnée maximum prédéfinies.

Ceci permet d'éviter un nombre trop important d'itérations à partir du même nombre complexe initial et permet donc d'obtenir un procédé de génération de nombres pseudo-aléatoires de bonne qualité en empêchant de retrouver périodiquement le même nombre pseudo-aléatoire en sortie.

L'invention concerne aussi un dispositif de génération de nombres pseudo-aléatoires réels signés représentés sur un nombre w entier de bits, lequel dispositif comporte des moyens :

- d'initialisation permettant de déterminer un nombre complexe initial et au moins un multiplicateur, lequel multiplicateur est un nombre complexe,
- de multiplication, pour une itération donnée, d'un multiplicande, lequel multiplicande est un nombre complexe, par le multiplicateur, le résultat de la multiplication étant un nombre complexe dont la partie réelle et la partie imaginaire sont représentées sur 2w bits; le multiplicande de la première itération étant le nombre complexe initial,
- de troncature, par application d'une fonction de troncature, respectivement de la partie réelle et de la partie imaginaire du résultat de la multiplication, le résultat de la troncature permettant de définir le multiplicande de l'itération suivante et l'erreur de troncature permettant de définir un nombre pseudo-aléatoire,
- de calibrage permettant d'obtenir le multiplicande de l'itération suivante sous la forme d'un nombre complexe dont la partie réelle et la partie imaginaire sont des nombres réels signés représentés sur le nombre w entier de bits et dont le module est compris entre une donnée minimum et une donnée maximum prédéfinies;

le nombre d'itérations étant déterminé par la quantité de nombres pseudo-aléatoires à générer.

L'invention concerne encore, un produit programme d'ordinateur comprenant des instructions de code de programme enregistrées sur ou transmises par un support lisible par un ordinateur, pour mettre en œuvre les étapes du procédé décrit ci-dessus lorsque ledit programme fonctionne sur ordinateur.

D'autres caractéristiques et avantages de la présente invention apparaîtront dans la description ci-après de modes de réalisation préférés décrits en référence aux figures dans lesquelles :

- la figure 1 illustre une représentation dans un plan d'un ensemble de nombres complexes,
- la figure 2 représente un mode de réalisation d'un procédé de génération de nombres pseudo-aléatoires,
- la figure 3 représente un mode de réalisation d'un dispositif de génération ou générateur de nombre pseudo-aléatoires apte à mettre en œuvre le procédé de la figure 2.

Dans un mode de réalisation non limitatif de l'invention décrit ci-après, on considère un procédé de génération et un générateur de nombres pseudo-aléatoires générant des nombres signés représentés sur w bits (w étant un nombre entier positif), avec :

- un bit réservé pour le signe,
- un bit réservé pour la partie entière,
- (w - 2) bits réservés pour la partie fractionnelle (partie du nombre située après la virgule).

En variante, w est un nombre entier égal à une puissance de 2 soit, par exemple, 8, 16, 32, 64.

On convient d'appeler E l'ensemble des nombres ainsi représentés. L'ensemble E est un sous-ensemble de l'ensemble R des nombres réels et

comprend des nombres x ayant un développement binaire sur w bits $[x_0, x_1, ..., x_{w-1}]$, avec x_0 le bit de poids le plus fort et x_{w-1} le bit de poids le plus faible.

Un nombre x de l'ensemble E est tel que :

$$x = (-1)^{x_0} . \left(\sum_{k=1}^{w-1} x_k . 2^{-(k-1)} \right).$$

De manière analogue, on représente un nombre complexe par un couple (y,z) de nombres réels, chacun appartenant à l'ensemble E et ayant un développement binaire sur w bits. Un nombre complexe ainsi représenté comporte w bits pour la partie réelle et w bits pour la partie imaginaire.

On convient d'appeler G l'ensemble des nombres complexes représentés de cette façon, soit :

$$G = \{(y,z) \text{ avec } y \text{ et } z \in E\}.$$

La **figure 1** illustre une représentation dans un plan de l'ensemble G des nombres complexes ainsi défini.

L'ensemble G peut être représenté par une grille de 2^{w-1} lignes et 2^{w-1} colonnes. Les coordonnées des $(2^{w-1}.2^{w-1})$ points aux intersections des lignes et colonnes de cette grille sont des nombres appartenant à l'ensemble E.

La figure 1 fait également apparaître la représentation d'un sous-ensemble D de l'ensemble G.

Le sous-ensemble D est défini comme l'ensemble des points de l'ensemble G compris entre deux cercles concentriques de rayons R_1 et R_2, soit :

$$D = G \cap \left\{ (y,z) \in R^2 \text{ avec } R_1 \leq \sqrt{y^2 + z^2} \leq R_2 \right\}.$$

R_1 et R_2 sont deux nombres réels positifs. R_2 est supérieur à R_1 et la valeur de R_2 n'excède pas la valeur 2 pour le mode de représentation considéré (nombres signés représentés sur w bits avec un bit pour le signe, un bit pour la partie entière, et (w - 2) bits pour la partie fractionnelle).

Dans la suite de la description, on considère $R_1 = 1$ et $R_2 = 2$.

Le procédé de génération et le générateur selon l'invention permettent de générer des nombres pseudo-aléatoires signés représentés sur w bits (c'est-à-dire appartenant à l'ensemble E) par l'exécution d'une multiplication de nombres complexes.

On réitère cette multiplication de nombres complexes autant de fois que la quantité de nombres pseudo-aléatoires souhaités.

Les calculs et opérations nécessaires pour effectuer ce calcul récursif sont décrits ci-après pour un mode particulier de réalisation de l'invention.

La **figure 2** représente un mode de réalisation d'un procédé de génération de nombres pseudo-aléatoires.

La première étape E1 est une étape d'initialisation.

Au cours de cette étape, on détermine les valeurs d'un nombre complexe initial (y_0, z_0) et d'un nombre complexe multiplicateur (y_m, z_m).

Le nombre complexe initial (y_0, z_0) n'intervient que dans la première multiplication de nombres complexes du calcul récursif comme multiplicande initial.

Le multiplicateur (y_m, z_m) intervient à chaque itération du calcul récursif tant qu'il n'est pas explicitement modifié.

Le nombre complexe initial (y_0, z_0) est choisi arbitrairement dans le sous-ensemble D défini précédemment.

Les valeurs du multiplicateur (y_m, z_m) sont choisies de façon à obtenir un générateur de nombres pseudo-aléatoires de bonne qualité en évitant certains inconvénients dus au calcul récursif.

La qualité d'un générateur de nombres pseudo-aléatoires est donnée par les résultats obtenus à une suite de tests statistiques tels que ceux

présentés dans le livre de D. E. Knuth précédemment cité, la suite Diehard de G. Marsaglia ou encore la suite du NIST (pour *National Institute of Standards and Technology* en anglais), etc.

Un premier inconvénient à éviter est que le calcul récursif dégénère progressivement vers la valeur 0 (ou vers un dépassement de la capacité du dispositif). En effet, dans ces conditions, les bits obtenus et donc les nombres obtenus ne sont plus pseudo-aléatoires. Ceci peut se produire lorsque le module du multiplicateur défini par $r_m = \sqrt{y_m^2 + z_m^2}$ est proche de 1 (inférieur ou supérieur à 1).

Un deuxième inconvénient peut se rencontrer lorsque le module du multiplicateur (soit $r_m = \sqrt{y_m^2 + z_m^2}$) est voisin de 1. Dans ce cas, l'argument φ_m du multiplicateur peut s'exprimer sous la forme $\varphi_m \approx 2\pi\frac{p}{q}$, avec p et $q \in N$, N étant l'ensemble des entiers positifs. Lorsque le module du multiplicateur est voisin de 1 alors le calcul récursif correspond à une fonction quasi-périodique et présente une forte probabilité de devenir périodique pour de faibles valeurs de q. En conséquence, les bits obtenus et donc les nombres obtenus sont périodiquement les mêmes.

Un troisième inconvénient peut se produire lorsque y_m ou z_m est voisin de 0. Dans ces conditions, le caractère aléatoire des bits générés et donc des nombres générés n'est plus garanti. Ce risque est plus grand pour les bits de poids faible.

Afin d'éviter ces inconvénients, les valeurs du multiplicateur (y_m, z_m) sont choisies dans le sous-ensemble D de telle sorte qu'elles satisfont les conditions suivantes :

$$\begin{cases} 1+\varepsilon_1 < \sqrt{y_m^2 + z_m^2} < 1+\varepsilon_2 \text{ avec } \varepsilon_1 = \sqrt{2}.2^{-(w-1)} \text{ et } \varepsilon_2 \geq 2.2^{-(w-1)} \\ |y_m . z_m| > 2^{-(\frac{w}{2}-1)} \end{cases}.$$

Selon la première condition, le module du multiplicateur est compris entre une valeur minimale et une valeur maximale telles que le module du multiplicateur est supérieur à 1 sans être très supérieur à 1. Cette première condition permet d'éviter des problèmes de périodicité du deuxième inconvénient cité et les problèmes de dégénérescence du premier inconvénient cité.

Le respect de la seconde condition entraine que l'argument du multiplicateur ne peut pas être égal à 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$. Cette deuxième condition permet d'éviter de perdre le caractère aléatoire des bits générés, ceci correspondant au troisième inconvénient cité.

Le choix des paramètres d'initialisation (nombre complexe initial et multiplicateur) est tel que le générateur de nombres pseudo-aléatoires selon l'invention est stable et non cyclique et le demeure pour un très grand nombre d'itérations.

A l'issue de l'étape E1 d'initialisation, on présente le nombre complexe initial (y_0, z_0) en entrée du générateur (ou dispositif de génération) et on introduit le multiplicateur (y_m, z_m) dans un module de calcul du générateur. En l'occurrence, le module de calcul du générateur est un multiplicateur de nombres complexes.

Les étapes suivantes E2 à E5 sont répétées autant de fois que la quantité de nombres pseudo-aléatoires à générer.

L'étape E2 est une étape de multiplication de nombres complexes.

Les nombres complexes intervenant dans la multiplication appartiennent au sous-ensemble D défini plus haut.

A la première itération, on obtient un couple (y_1, z_1) défini par la multiplication de nombres complexes suivante :

$$(y_1, z_1) = (y_0 + jz_0).(y_m + jz_m)$$
$$= y_1 + jz_1$$

où (y_0, z_0) et (y_m, z_m) sont respectivement le nombre complexe (ou multiplicande) initial et le multiplicateur déterminés au cours de l'étape E1.

A la $k^{ième}$ itération, on obtient un couple de valeurs (y_k, z_k) défini par :

$$(y_k, z_k) = (y_{k-1} + jz_{k-1}).(y_m + jz_m)$$
$$= (y_{k-1}y_m - z_{k-1}z_m) + j(y_{k-1}z_m + z_{k-1}y_m)$$
$$= y_k + jz_k$$

où

- (y_{k-1}, z_{k-1}) est un nombre complexe obtenu à partir du résultat de la multiplication réalisée à l'itération précédente k-1 et correspond au multiplicande de l'itération courante k,
- (y_m, z_m) est le multiplicateur déterminé au cours de l'étape E1.

A partir de ce dernier développement, on constate que la multiplication de nombres complexes nécessite quatre multiplications et deux additions pour obtenir la partie réelle et la partie imaginaire du résultat à partir de la partie réelle et de la partie imaginaire du nombre complexe (ou multiplicande) présenté en entrée du générateur.

On déduit également de ce développement que la partie réelle et la partie imaginaire du résultat sont chacune représentées sur 2w bits.

Le résultat de la multiplication de nombres complexes (c'est-à-dire la partie réelle y_k et la partie imaginaire z_k obtenues) est stocké dans un accumulateur double longueur (*Double Length Accumulator* en anglais).

L'étape suivante E3 est une étape de troncature.

Comme on l'a souligné précédemment, le résultat de la multiplication de nombres complexes réalisée à l'étape E2 comporte une partie réelle et une partie imaginaire, chacune représentée sur 2w bits.

Avant de passer à l'itération suivante, on tronque la partie réelle et la partie imaginaire afin d'obtenir une représentation sur w bits. Cette opération est réalisée à l'aide d'un opérateur de troncature.

De manière générale, la troncature permet, à partir d'un nombre n représenté sur 2w bits, d'obtenir un nombre $\tilde{n}$ représenté sur w bits.

Cette opération peut être réalisée en utilisant une des fonctions suivantes : partie entière (arrondi proche de 0), partie entière par excès (arrondi éloigné de 0), arrondi.

En appliquant la fonction partie entière, on obtient :

$$\tilde{n} = \lfloor n \cdot 2^{w-2} \rfloor \cdot 2^{-(w-2)}.$$

En appliquant la fonction partie entière par excès, on obtient :

$$\tilde{n} = \left(\lfloor n \cdot 2^{w-2} \rfloor + (-1)^{[n>0]} \cdot 2^{-(w-2)} \right).$$

En appliquant la fonction d'arrondi, on obtient :

$$\tilde{n} = \lfloor n \cdot 2^{w-2} + 0{,}5 \rfloor \cdot 2^{-(w-2)}.$$

La troncature introduit une erreur τ telle que $\tau = n - \tilde{n}$. L'erreur τ est représentable sur w bits.

Dans le cas de l'invention, la troncature est appliquée à des nombres complexes. L'erreur introduite par cette opération comporte w bits en provenance de la partie réelle et w bits en provenance de la partie imaginaire.

Il est intéressant de conserver ces 2w bits qui sont des bits aléatoires.

On convient de désigner par une fonction Q_w l'opération de troncature et de récupération de l'erreur de troncature.

Par exemple, si on applique la fonction Q_w à un nombre n représenté sur 2w bits en utilisant la fonction arrondi, on obtient :

$$Q_w(n) = \{\tilde{n}, \tau_n\} = \begin{cases} \tilde{n} = \lfloor n \cdot 2^{w-2} + 0{,}5 \rfloor \cdot 2^{-(w-2)} \\ \tau_n = (n - \tilde{n}) \cdot 2^{-(w-2)} \end{cases}$$

où

- $\tilde{n}$ est le résultat de la troncature du nombre n,

- τ_n est l'erreur de troncature.

Ainsi, à l'étape E3, on applique la fonction Q_w à la partie réelle y_k et à la partie imaginaire z_k obtenues à l'étape précédente E2 de multiplication de nombres complexes. On obtient alors :

$$\begin{cases} Q_w(y_k) = \{\tilde{y}_k , \tau_{y_k}\} \\ Q_w(z_k) = \{\tilde{z}_k , \tau_{z_k}\} \end{cases}$$

avec :

- $\tilde{y}_k$ et $\tilde{z}_k$ correspondent au résultat de la troncature respectivement de la partie réelle y_k et de la partie imaginaire z_k,

- τ_{y_k} et τ_{z_k} représentent l'erreur de troncature correspondant aux bits tronqués respectivement pour la partie réelle y_k et pour la partie imaginaire z_k.

τ_{y_k} et τ_{z_k} sont chacun représentés sur w bits. Ainsi, on a :

$$\begin{cases} \tau y_k = \left[\tau y_{k_0} , \tau y_{k_1} , \ldots , \tau y_{k_{(w-1)}} \right] \\ \tau z_k = \left[\tau z_{k_0} , \tau z_{k_1} , \ldots , \tau z_{k_{(w-1)}} \right] \end{cases}.$$

L'étape suivante E4 est une étape de détermination de la sortie du générateur de nombres pseudo-aléatoires.

La sortie du générateur est déterminée à partir des w bits de τ_{y_k} et des w bits de τ_{z_k}.

Ainsi, on peut générer une sortie d'au plus 2w bits en prenant un premier nombre de bits les plus significatifs de τ_{y_k} et un deuxième nombre de bits les plus significatifs de τ_{z_k} puis de les concaténer.

On convient de retenir le même nombre de bits les plus significatifs de τ_{y_k} que de bits les plus significatifs de τ_{z_k} puis de les concaténer.

Pour obtenir un générateur avec une qualité optimum, on retient les $\frac{w}{2}$ bits les plus significatifs de τ_{y_k} et les $\frac{w}{2}$ bits les plus significatifs de τ_{z_k}.

On dispose alors de w bits aléatoires qui définissent la sortie S du dispositif de génération de nombres pseudo-aléatoires selon l'invention.

Par bits significatifs, on entend les bits tels qu'ils représentent un nombre dont la valeur est proche du nombre auquel la troncature a été appliquée.

La sortie S du générateur de nombres pseudo-aléatoires peut s'exprimer de la façon suivante :

$$S = \left[\tau_{y_{k_0}}, \tau_{y_{k_1}}, \ldots, \tau_{y_{k_{(\frac{w}{2}-1)}}}, \tau_{z_{k_0}}, \tau_{z_{k_1}}, \ldots, \tau_{z_{k_{(\frac{w}{2}-1)}}} \right].$$

S est la représentation sur w bits d'un nombre pseudo-aléatoire signé.

L'étape suivante E5 est une étape de calibrage.

Les calculs et opérations décrits ci-dessus sont réalisés autant de fois que la quantité de nombres pseudo-aléatoires souhaités.

Ces calculs et opérations sont réalisés dans le sous-ensemble D défini plus haut.

L'étape de calibrage permet de s'assurer que les calculs et opérations sont réalisés dans le sous-ensemble D.

L'itération k+1 comporte une multiplication de nombres complexes d'un nombre complexe ou multiplicande par le multiplicateur (y_m, z_m) obtenu à l'étape E1.

On convient de désigner par (y'_k, z'_k) le multiplicande de l'itération k+1.

Le multiplicande de l'itération k+1 est obtenu à partir du résultat de la multiplication de nombres complexes réalisée à l'itération précédente k.

La multiplication de nombres complexes est effectuée dans le sous-ensemble D. Par conséquent, le multiplicande (y'_k, z'_k) appartient au sous-ensemble D.

On rappelle, pour mémoire, que le sous-ensemble D est un ensemble de nombres complexes dont la partie réelle et la partie imaginaire sont des nombres signés représentés sur w bits (un bit pour le signe, un bit pour la partie entière et (w - 2) bits pour la partie fractionnelle) et dont le module est compris entre une valeur minimum R_1 et une valeur maximum R_2.

Le multiplicande (y'_k, z'_k) de l'itération k+1 est déduit du couple $(\tilde{y}_k, \tilde{z}_k)$, résultat de la troncature de chacune des composantes du couple (y_k, z_k), lui-même résultat de la multiplication de nombres complexes réalisée à l'itération k.

Les composantes du couple $(\tilde{y}_k, \tilde{z}_k)$ sont représentées sur w bits.

Ainsi, si $(\tilde{y}_k, \tilde{z}_k)$ appartient à D, c'est-à-dire que le module de $(\tilde{y}_k, \tilde{z}_k)$ est compris entre la valeur minimum R_1 et la valeur maximum R_2, alors on prend :

$$(y'_k, z'_k) = (\tilde{y}_k, \tilde{z}_k),$$

où

- $(\tilde{y}_k, \tilde{z}_k)$ est le résultat de la troncature par la fonction Q_w appliquée à chacune des composantes du couple (y_k, z_k).

Dans le cas contraire, $(\tilde{y}_k, \tilde{z}_k)$ n'appartient pas à D signifie que le module de $(\tilde{y}_k, \tilde{z}_k)$ n'est pas compris entre la valeur minimum R_1 et la valeur maximum R_2. Ceci peut, par exemple, se produire lorsque le calcul récursif dégénère.

Si $(\tilde{y}_k, \tilde{z}_k)$ n'appartient pas à D, l'équation suivante est alors satisfaite :

$$\left(\frac{\tilde{y}_k}{2}\right)^2 + \left(\frac{\tilde{z}_k}{2}\right)^2 \geq \left(\frac{\left(R_2 - 2^{-(w-1)}\right)}{2}\right)^2$$

et on prend :

$$(y'_k, z'_k) = \left(\frac{\tilde{y}_k}{2}, \frac{\tilde{z}_k}{2} \right),$$

où

- $(\tilde{y}_k, \tilde{z}_k)$ est le résultat de la troncature par la fonction Q_w appliquée à chacune des composantes du couple (y_k, z_k),

- R_2 est le rayon du cercle ayant permis de définir le sous-ensemble D.

A l'issue de l'étape E5, on présente le couple (y'_k, z'_k) en entrée du dispositif de génération de nombres pseudo-aléatoires et le procédé reprend à l'étape E2 pour générer un nouveau nombre pseudo-aléatoire.

Le procédé selon l'invention est décrit ci-dessus pour un mode de réalisation particulier. Cependant, plusieurs variantes à ce mode de réalisation peuvent être envisagées.

Selon une première variante, au cours de l'étape d'initialisation E1, on détermine le nombre de bits aléatoires à générer et/ou la fonction de troncature à utiliser. Ces paramètres supplémentaires d'initialisation sont fournis au dispositif de génération de nombres pseudo-aléatoires.

Selon une deuxième variante, à l'issue de l'étape d'initialisation E1, on fournit au dispositif de génération de nombres pseudo-aléatoires l'argument φ_m du multiplicateur à la place des valeurs de la partie réelle et de la partie imaginaire de ce multiplicateur, soit le couple (y_m, z_m).

Selon une autre variante, au cours de l'étape d'initialisation E1, on définit plusieurs (au moins deux) multiplicateurs.

En variante, on effectue une réinitialisation du générateur afin d'éviter un nombre trop important d'itérations avec les mêmes valeurs d'initialisation (nombre complexe initial ou multiplicateur).

Pour cela, on prédétermine une valeur seuil de nombre d'itérations (CI_{lim}) et on initialise à zéro un compteur CI du nombre d'itérations.

Puis, à chaque itération, on incrémente le compteur CI du nombre d'itérations.

Selon une première variante à cette variante, lorsque la valeur seuil de nombre d'itérations est atteinte (soit $CI \geq CI_{lim}$), on réinitialise le dispositif de génération de nombre pseudo-aléatoires avec un multiplicateur différent de celui utilisé au cours des itérations précédentes.

Selon une deuxième variante à cette variante, lorsque la valeur seuil de nombre d'itérations est atteinte (soit $CI \geq CI_{lim}$), on réinitialise le dispositif de génération de nombres pseudo-aléatoires en présentant en entrée de celui-ci non pas le multiplicande obtenu à l'issue de l'étape E5 de calibrage mais un nombre complexe arbitrairement choisi dans le sous-ensemble D, de la même façon que pour le nombre complexe initial (y_0, z_0).

Les deux sous variantes précédentes ne sont pas exclusives l'une de l'autre et peuvent être mises en œuvre simultanément.

Dans certains cas d'application, on peut souhaiter limiter les contraintes des paramètres déterminés au cours de l'étape E1 d'initialisation.

On peut notamment souhaiter supprimer la contrainte sur l'argument du multiplicateur, celui-ci pouvant alors prendre les valeurs 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$.

Pour garantir avec ces nouvelles conditions, un très bon niveau de qualité au générateur de nombres pseudo-aléatoires, on fait varier l'étape E4 de détermination de la sortie du générateur de nombres pseudo-aléatoires.

On détermine les w bits aléatoires qui définissent la sortie S du dispositif de génération de nombres pseudo-aléatoires selon l'invention en

effectuant respectivement une opération entre un nombre entier positif h de bits les plus significatifs et le même nombre entier positif h de bits les moins significatifs de τ_{y_k} (partie réelle du résultat de la multiplication de nombres complexes) et la même opération entre les h bits les plus significatifs et les h bits les moins significatifs de τ_{z_k} (partie réelle du résultat de la multiplication de nombres complexes).

Pour obtenir un générateur avec une qualité optimum, on prend $h = \frac{w}{2}$.

A titre d'exemple non limitatif de l'invention, l'opération effectuée peut être un OU exclusif (ou XOR pour *eXclusive OR* en anglais).

Ainsi, en appliquant l'opérateur OU exclusif, on obtient :

$$S = \left[\left[\tau_{y_{k_0}}, \tau_{y_{k_1}}, \ldots, \tau_{y_{k_{(\frac{w}{2}-1)}}}\right] \otimes \left[\tau_{y_{k_{(\frac{w}{2})}}}, \tau_{y_{k_{(\frac{w}{2}+1)}}}, \ldots, \tau_{y_{k_{(w-1)}}}\right], \left[\tau_{z_{k_0}}, \tau_{z_{k_1}}, \ldots, \tau_{z_{k_{(\frac{w}{2}-1)}}}\right] \otimes \left[\tau_{z_{k_{(\frac{w}{2})}}}, \tau_{z_{k_{(\frac{w}{2}+1)}}}, \ldots, \tau_{z_{k_{(w-1)}}}\right]\right].$$

Selon une autre variante, on effectue une détection de cycles par un des algorithmes connus de détection de cycles. Il peut, par exemple s'agir de l'algorithme du lièvre et de la tortue présenté dans le livre de D.E. Knuth cité précédemment, ou de l'algorithme présenté par R.P. Brent dans "*An improved Monte Carlo factorization algorithm*", 1980, BIT 20, 176-184, etc.

La **figure 3** représente un mode de réalisation d'un dispositif de génération ou générateur de nombres pseudo-aléatoires apte à mettre en œuvre le procédé décrit ci-dessus.

Le dispositif de génération (ou générateur) de nombres pseudo-aléatoires selon l'invention permet de générer des nombres pseudo-aléatoires signés représentés sur w bits tels que ceux appartenant à l'ensemble E défini plus haut par l'exécution d'une multiplication de nombres complexes.

Le dispositif GEN de génération de nombres pseudo-aléatoires représenté à la figure 3 comporte un module INIT d'initialisation.

Le module INIT détermine un nombre complexe initial (y_0, z_0) et le présente en entrée EN du générateur GEN tel que décrit ci-dessus dans l'étape E1 d'initialisation. y_0 et z_0 sont chacun des nombres réels signés représentés sur w bits.

Le nombre complexe initial (y_0, z_0) est présenté une fois en entrée du générateur GEN d'où les pointillés entre le module INIT d'initialisation et l'entrée EN.

Le module INIT d'initialisation détermine également un multiplicateur (y_m, z_m) et l'introduit dans un module MC de calcul du générateur GEN. y_m et z_m sont chacun des nombres réels signés représentés sur w bits.

Le module MC de calcul est un multiplicateur de nombres complexes.

Le module MC de calcul réalise itérativement autant de multiplications de nombres complexes que la quantité de nombres pseudo-aléatoires à générer.

Ainsi, au cours d'une itération k, le module MC de calcul effectue une multiplication de nombres complexes entre un multiplicande (y'_{k-1}, z'_{k-1}) obtenu à partir du résultat de la multiplication réalisée à l'itération précédente k-1 et le multiplicateur (y_m, z_m) déterminé par le module INIT d'initialisation. Ainsi, le module MC de calcul réalise l'étape E2 décrite précédemment.

En sortie du module MC de calcul on obtient un couple (y_k, z_k) dont chacune des composantes est représentée sur 2w bits.

Le générateur GEN de nombres pseudo-aléatoires comporte un accumulateur double longueur DLA dans lequel est stocké le résultat de la multiplication de nombres complexes effectuée par le module MC de calcul.

Le dispositif GEN de génération de nombres pseudo-aléatoires comporte également un module TR de troncature et de récupération d'erreur de troncature tel que décrit à l'étape E3 ci-dessus

Le générateur GEN de nombres pseudo-aléatoires comporte aussi un module S0 de détermination de la sortie du générateur de nombres pseudo-aléatoires tel que précédemment décrit à l'étape E4.

En référence à l'étape E4, le module SO de détermination de la sortie du générateur permet à partir des erreurs de troncature (obtenues en sortie du module TR) d'une troncature respectivement de chacune des composantes du couple (y_k, z_k) de retenir w bits parmi les bits aléatoires générés. Les w bits retenus représentent un nombre S pseudo-aléatoire. Le nombre S est présenté en sortie SO du générateur GEN.

Le générateur GEN de nombres pseudo-aléatoires comporte aussi un module CAL de calibrage qui permet de déterminer le multiplicande (y'_k, z'_k) de l'itération suivante.

En référence à l'étape E5 décrite ci-dessus, le module CAL de calibrage permet à partir d'une troncature de chacune des composantes du couple (y_k, z_k) de définir le couple de valeurs (y'_k, z'_k) dont chacune des composantes est représentée sur w bits.

Le couple de valeurs (y'_k, z'_k) ainsi obtenu est ensuite présenté en entrée EN du dispositif GEN de génération de nombres pseudo-aléatoires pour la réalisation de l'itération suivante afin d'obtenir un nouveau nombre pseudo-aléatoire.

Les modules INIT d'initialisation, TR de troncature, SO de détermination de la sortie du générateur et CAL de calibrage peuvent être des modules

logiciels formant un programme d'ordinateur. L'invention concerne donc également un programme d'ordinateur pour un dispositif de génération de nombre pseudo-aléatoires comprenant des instructions de code de programme pour faire exécuter le procédé précédemment décrit par le dispositif.

Les différents modules logiciels peuvent être stockés dans ou transmis par un support de données. Celui-ci peut être un support matériel de stockage, par exemple un CD-ROM, une disquette magnétique ou un disque dur, ou bien un support transmissible tel qu'un signal électrique, optique ou radio.

L'invention peut être mise en œuvre dans toute application utilisant la génération de nombres pseudo-aléatoires que ce soit pour de la simulation, de l'analyse, de la prise de décision, de la sécurité ou encore de la cryptographie, etc.

L'architecture matérielle comprenant un multiplicateur de nombres complexes et un accumulateur double longueur est très simple et adaptée pour être mise en œuvre sur des microprocesseurs embarqués, des processeurs spécialisés dans le traitement des signaux (ou DSP pour *Digital Signal Processor* en anglais) ou encore des processeurs au silicium.

L'invention peut donc être utilisée dans des applications contraintes en puissance de calcul, en mémoire et en énergie. En particulier, l'invention peut être utilisée dans des réseaux de capteurs.

L'état interne du générateur selon l'invention n'est pas révélé par les résultats obtenus en sortie de celui-ci. Un tel générateur peut être utilisé pour définir des dispositifs d'authentification/chiffrement en fournissant une partie secrète équivalente à une clé privée et une partie visible équivalente à une clé publique. Ainsi, l'application d'un tel générateur peut être la sécurisation de communications, notamment dans des réseaux de capteurs/actionneurs contraints en puissance de calcul, en mémoire et en énergie.

REVENDICATIONS

1. Procédé de génération de nombres pseudo-aléatoires réels signés représentés sur un nombre w entier de bits, destiné à être mis en œuvre dans un dispositif embarqué, caractérisé en ce qu'il comporte des étapes :

- d'initialisation (E1) comportant la détermination d'un nombre complexe initial et d'au moins un multiplicateur, lequel multiplicateur est un nombre complexe (y_m, z_m), qui satisfait les conditions suivantes :

$$\begin{cases} 1+\varepsilon_1 < \sqrt{y_m^2 + z_m^2} < 1+\varepsilon_2 \text{ avec } \varepsilon_1 = \sqrt{2}.2^{-(w-1)} \text{ et } \varepsilon_2 \geq 2.2^{-(w-1)} \\ |y_m . z_m| > 2^{-(\frac{w}{2}-1)} \end{cases} ;$$

- de multiplication (E2), pour une itération donnée, d'un multiplicande, lequel multiplicande est un nombre complexe, par le multiplicateur, le résultat de la multiplication étant un nombre complexe dont la partie réelle et la partie imaginaire sont représentées sur 2w bits; le multiplicande de la première itération étant le nombre complexe initial,

- de troncature (E3), par application d'une fonction de troncature, respectivement de la partie réelle et de la partie imaginaire du résultat de la multiplication, le résultat de la troncature permettant de définir le multiplicande de l'itération suivante et l'erreur de troncature permettant de définir un nombre pseudo-aléatoire,

- de calibrage (E5) pour obtenir le multiplicande de l'itération suivante sous la forme d'un nombre complexe dont la partie réelle et la partie imaginaire sont des nombres réels signés représentés sur le nombre w entier de bits et dont le module est compris entre une donnée minimum et une donnée maximum prédéfinies;

le nombre d'itérations étant déterminé par la quantité de nombres pseudo-aléatoires à générer.

2. Procédé selon la revendication 1, caractérisé en ce que la partie réelle et la partie imaginaire du multiplicateur sont des nombres réels signés représentés sur le nombre w entier de bits, le module du multiplicateur étant compris entre une valeur minimum et une valeur maximum prédéfinies et la valeur absolue du produit de la partie réelle par la partie imaginaire étant supérieure à une troisième valeur prédéfinie.

3. Procédé selon la revendication 2, caractérisé en ce que la valeur minimum est égale à 1 et la valeur maximum est égale à 2.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que la partie réelle et la partie imaginaire du nombre complexe initial et du multiplicande sont des nombres réels signés représentés sur le nombre w entier de bits et le module du nombre complexe initial et le module du multiplicande sont compris entre la donnée minimum et la donnée maximum prédéfinies.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que la fonction de troncature appartient à la liste suivante :

- fonction partie entière,
- fonction partie entière par excès,
- fonction d'arrondi.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que l'étape (E1) d'initialisation comporte la détermination du nombre w entier de bits.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que l'étape (E1) d'initialisation comporte la détermination de la fonction de troncature.

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comporte une étape (E4) de détermination d'une sortie, laquelle sortie est un nombre pseudo-aléatoire obtenu par concaténation d'un premier nombre de bits les plus significatifs de la partie réelle et d'un deuxième nombre de bits les plus significatifs de la partie imaginaire de l'erreur de troncature du résultat de la multiplication.

9. Procédé selon la revendication 8, caractérisé en ce que la sortie déterminée est sur w bits et le premier nombre et le second nombre sont égaux à $\frac{w}{2}$.

10. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comporte une étape (E4) de détermination d'une sortie, laquelle sortie est un nombre pseudo-aléatoire sur w bits obtenu à partir respectivement d'une opération effectuée entre un nombre entier h positif de bits les plus significatifs et le même nombre h de bits les moins significatifs de la partie réelle et de la même opération effectuée entre le nombre entier h positif de bits les plus significatifs et le même nombre h de bits les moins significatifs de la partie imaginaire de l'erreur de troncature du résultat de la multiplication.

11. Procédé selon la revendication 10, caractérisé en ce que l'opération est un OU exclusif.

12. Procédé selon l'une quelconque des revendications 1 à 11, caractérisé en ce qu'il comporte la prédétermination d'une valeur seuil de nombre d'itérations et l'initialisation d'un compteur du nombre d'itérations, lequel compteur du nombre d'itérations est incrémenté à chaque itération de telle sorte que lorsque la valeur du compteur du nombre d'itérations atteint la valeur seuil de nombres d'itérations on change le multiplicateur.

13. Procédé selon l'une quelconque des revendications 1 à 12, caractérisé en ce qu'il comporte la prédétermination d'une valeur seuil de nombre d'itérations et l'initialisation d'un compteur du nombre d'itérations, lequel compteur du nombre d'itérations est incrémenté à chaque itération de telle sorte que lorsque la valeur du compteur du nombre d'itérations atteint la valeur seuil de nombres d'itérations, le multiplicande est remplacé par un nombre complexe dont la partie réelle et la partie imaginaire sont des nombres réels signés représentés sur le nombre w entier de bits et dont le module est compris entre la donnée minimum et la donnée maximum prédéfinies.

14. Dispositif embarqué de génération de nombres pseudo-aléatoires réels signés représentés sur un nombre w entier de bits, caractérisé en ce qu'il comporte des moyens :

- d'initialisation (INIT) permettant de déterminer un nombre complexe initial et au moins un multiplicateur, lequel multiplicateur est un nombre complexe, (y_m, z_m), qui satisfait les conditions suivantes :

$$\begin{cases} 1+\varepsilon_1 < \sqrt{y_m^2 + z_m^2} < 1+\varepsilon_2 \text{ avec } \varepsilon_1 = \sqrt{2}.2^{-(w-1)} \text{ et } \varepsilon_2 \geq 2.2^{-(w-1)} \\ |y_m . z_m| > 2^{-(\frac{w}{2}-1)} \end{cases}$$

- de multiplication (MC), pour une itération donnée, d'un multiplicande, lequel multiplicande est un nombre complexe, par le multiplicateur, le résultat de la multiplication étant un nombre complexe dont la partie réelle et la partie imaginaire sont représentées sur 2w bits; le multiplicande de la première itération étant le nombre complexe initial,

- de troncature (TR), par application d'une fonction de troncature, respectivement de la partie réelle et de la partie imaginaire du résultat de la multiplication, le résultat de la troncature permettant de définir le multiplicande de l'itération suivante et l'erreur de troncature permettant de définir un nombre pseudo-aléatoire,

- de calibrage (CAL) permettant d'obtenir le multiplicande de l'itération suivante sous la forme d'un nombre complexe dont la partie réelle et la partie imaginaire sont des nombres réels signés représentés sur le nombre w entier de bits et dont le module est compris entre une donnée minimum et une donnée maximum prédéfinies;

le nombre d'itérations étant déterminé par la quantité de nombres pseudo-aléatoires à générer.

15. Produit programme d'ordinateur comprenant des instructions de code de programme enregistrées sur ou transmises par un support lisible par un ordinateur, pour mettre en œuvre les étapes du procédé selon l'une quelconque des revendications 1 à 13 lorsque ledit programme fonctionne sur ordinateur.

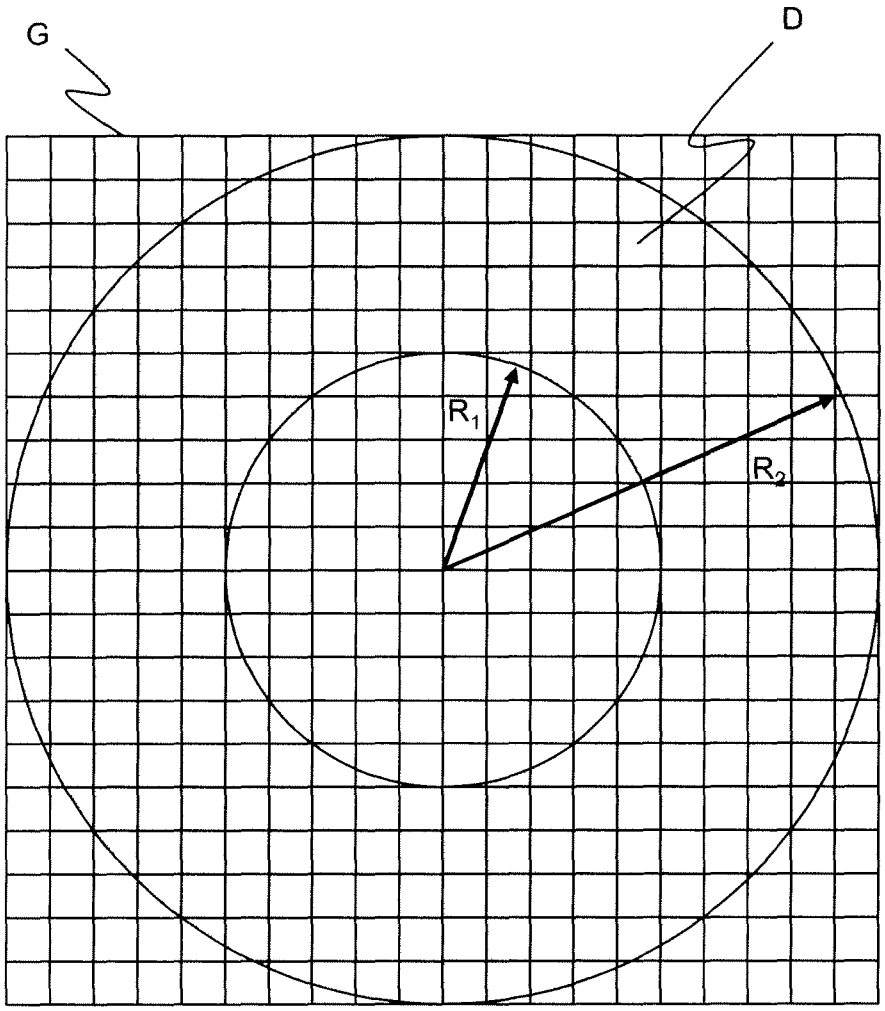

Fig. 1

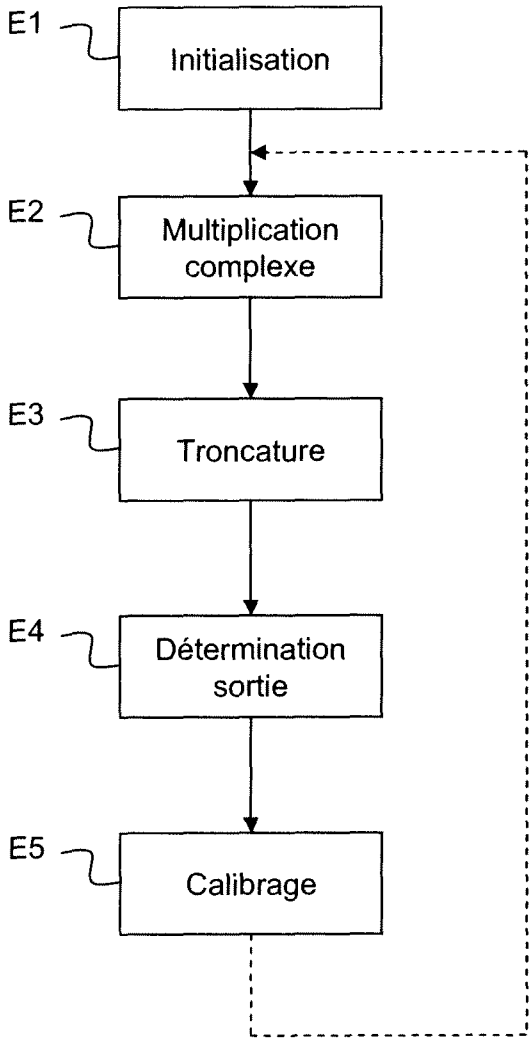
E1
Initialisation
E2
Multiplication complexe
E3
Troncature
E4
Détermination sortie
E5
Calibrage

Fig. 2

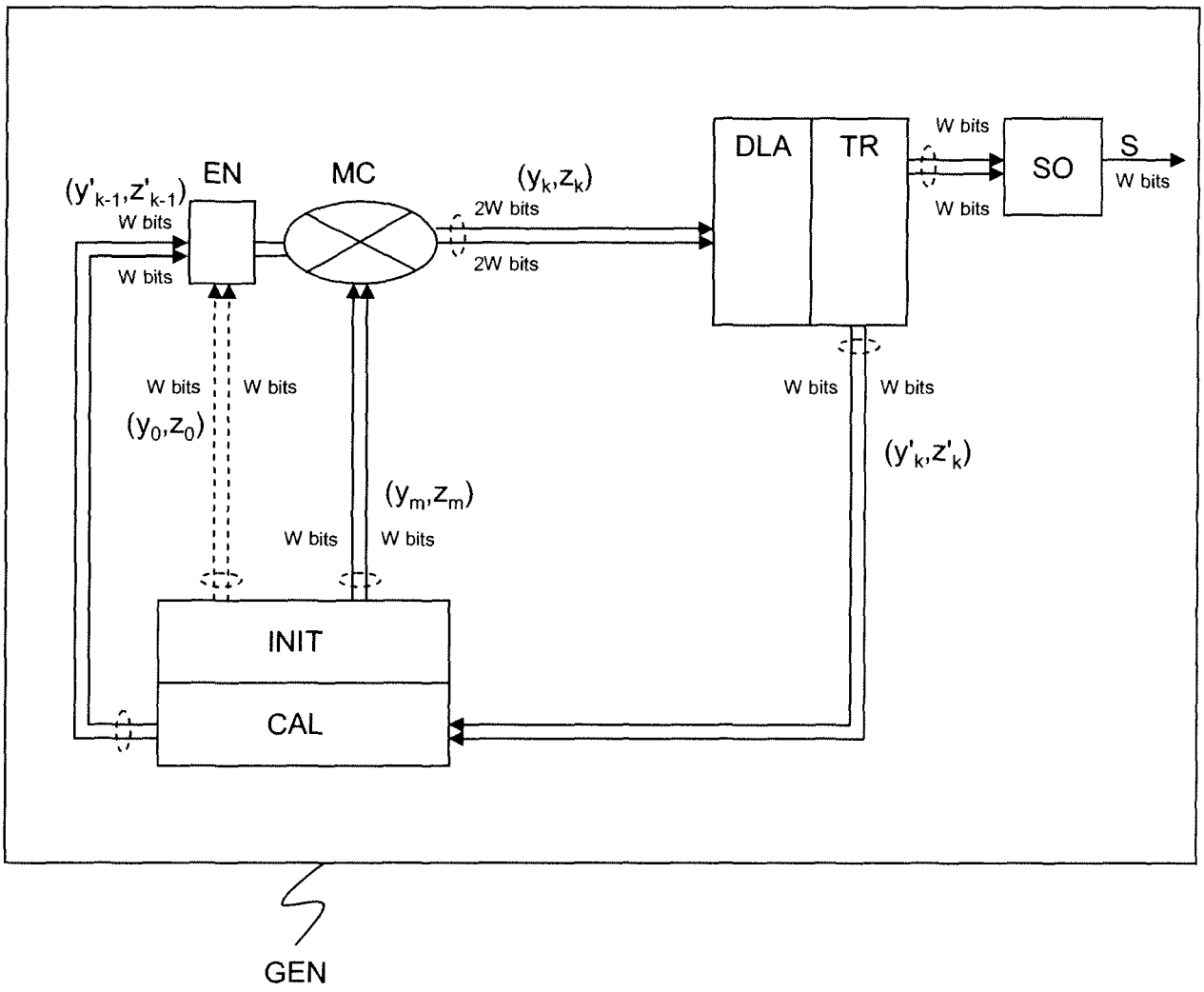
EN
MC
DLA
TR
SO
S
W bits
(y'_{k-1},z'_{k-1})
(y_k,z_k)
2W bits
(y_0,z_0)
(y_m,z_m)
(y'_k,z'_k)
INIT
CAL
GEN

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2010/050955

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F7/58
ADD. G06F7/48

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 012 214 A (FRANCE TELECOM [FR]) 7 January 2009 (2009-01-07) * abstract page 4, paragraph 23 page 6, paragraph 33 page 8, paragraph 51 - page 10, paragraph 57 figures 1,2,3a	1-15
A	FR 2 851 385 A (FRANCE TELECOM [FR]) 20 August 2004 (2004-08-20) * abstract page 2, line 22 - line 32 page 9, line 19 - page 16, line 2 figure 2	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 September 2010	05/10/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Post, Katharina

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2010/050955

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2012214 A	07-01-2009	AT 467166 T	15-05-2010
		FR 2918236 A1	02-01-2009
		US 2009006514 A1	01-01-2009
FR 2851385 A	20-08-2004	EP 1593220 A1	09-11-2005
		WO 2004075449 A1	02-09-2004

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2010/050955

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F7/58
ADD. G06F7/48

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 2 012 214 A (FRANCE TELECOM [FR]) 7 janvier 2009 (2009-01-07) * abrégé page 4, alinéa 23 page 6, alinéa 33 page 8, alinéa 51 - page 10, alinéa 57 figures 1,2,3a	1-15
A	FR 2 851 385 A (FRANCE TELECOM [FR]) 20 août 2004 (2004-08-20) * abrégé page 2, ligne 22 - ligne 32 page 9, ligne 19 - page 16, ligne 2 figure 2	1-15

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
7 septembre 2010	05/10/2010

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Post, Katharina

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2010/050955

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 2012214	A	07-01-2009	AT	467166 T	15-05-2010
			FR	2918236 A1	02-01-2009
			US	2009006514 A1	01-01-2009
FR 2851385	A	20-08-2004	EP	1593220 A1	09-11-2005
			WO	2004075449 A1	02-09-2004