(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 137 771***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **22 07035**

(51) Int Cl[8] : ***G 06 F 7/58*** *(2022.01)*

(12) **BREVET D'INVENTION** **B1**

(54) Procédé et dispositif de qualification d'un générateur de nombre(s) aléatoire(s), et procédé de conception du générateur de nombre(s) aléatoire(s).

(22) **Date de dépôt :** 08.07.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 12.01.24 Bulletin 24/02.

(45) **Date de la mise à disposition du public du brevet d'invention :** 31.05.24 Bulletin 24/22.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

(60) **Références à d'autres documents nationaux apparentés :**

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *THALES Société anonyme* — FR.

(72) **Inventeur(s) :** GARRIDO Eric, DUPIN Aurélien, CHRISTIN Antoine et QUATRAVAUX Lucile.

(73) **Titulaire(s) :** THALES Société anonyme.

(74) **Mandataire(s) :** Lavoix.

FR 3 137 771 - B1

Description

Titre de l'invention : Procédé et dispositif de qualification d'un générateur de nombre(s) aléatoire(s), et procédé de conception du générateur de nombre(s) aléatoire(s)

[0001] La présente invention concerne un procédé de qualification d'un générateur de nombre(s) aléatoire(s) pour le respect d'un seuil de taux d'entropie prédéfini.

[0002] La présente invention a également pour objet un dispositif électronique de qualification d'un générateur de nombre(s) aléatoire(s) pour le respect d'un seuil de taux d'entropie prédéfini.

[0003] L'invention concerne également un procédé de conception d'un générateur de nombre(s) aléatoire(s).

[0004] L'invention concerne le domaine de la génération de nombres aléatoires matériel, aussi appelé vraie génération de nombres aléatoires (de l'anglais *True Randon Number Generator* TRNG), par exemple embarqué au sein de composants hardware FPGA (de l'anglais *Field Programmable Gate Array*) ou ASIC (de l'anglais *Application-Specific Integrated Circuit*).

[0005] Il est connu de générer des nombres aléatoires à partir d'oscillateurs à anneau et d'un module d'acquisition acquérant, suivant une fréquence prédéfinie, un bit en sortie de chaque oscillateur à anneau. Le générateur comprend en outre généralement un module de composition implémentant une fonction de composition des bits acquis pour obtenir un bit généré. Chaque génération d'un bit généré par le générateur est appelée « tirage » et forme le nombre aléatoire.

[0006] A chaque tirage, les valeurs acquises comportent une partie déterministe liée à des caractéristiques déterminables de chaque oscillateur à anneau, et une partie aléatoire liée à des caractéristiques imprévisibles de chaque oscillateur à anneau.

[0007] Dans certaines applications telles que la cryptographie, il est nécessaire d'assurer que les bits générés lors de tirages successifs sont bien aléatoires.

[0008] Une manière de mesurer le caractère aléatoire est l'entropie de Shanon d'une suite de D tirages successifs. Plus l'entropie de Shannon est grande et plus la suite de D tirages successifs est imprévisible, i.e. aléatoire.

[0009] L'entropie de Shannon d'une variable X est l'incertitude de la variable X. L'entropie de Shannon de la variable X est définie par l'équation suivante :

[0010] [Math.1]

$$H_{sh}(X) = -E\left(Log_2(P(X=x))\right) = -\sum_x P(X=x)Log_2(P(X=x))$$

[0011] où $E(\ )$ est l'espérance,

[0012] $Log_2(\ )$ est le logarithme en base 2,

[0013] Σ est la somme

[0014] x est toute valeur prise par la variable X, et

[0015] $P(X = x)$ est la probabilité que la variable X prenne la valeur x.

[0016] On définit en outre un taux d'entropie du générateur, comme étant égal à la limite, si elle existe, quand un nombre de tirages D tend vers l'infini, du rapport entre l'entropie de Shannon de la variable aléatoire $X = (S_1, S_2, \ldots, S_D)$ modélisant les D tirages successifs de la source d'aléa, divisé par le nombre D de tirages de bits successifs.

[0017] Ainsi, le taux d'entropie quantifie l'aléatoire de chaque bit généré à chaque tirage, lorsque le générateur de nombre(s) aléatoire(s) est en fonctionnement et qu'il génère les bits à la fréquence prédéfinie.

[0018] Ainsi, le taux d'entropie est une valeur comprise entre zéro et un. L'unité du taux d'entropie est le bit d'entropie par bit généré. Si le taux d'entropie est proche de zéro, alors chaque bit généré est déterministe et la suite de tirages est facilement déterminable. A l'inverse, si le taux d'entropie est proche de un, alors chaque bit généré est imprévisible et la suite de tirages est difficilement déterminable. Le taux d'entropie dépend de la modélisation stochastique qui donne un sens aux probabilités d'occurrence des motifs $X = (S_1, S_2, \ldots, S_D)$. Il est en pratique dans l'état de l'art difficile à calculer ou estimer, quand le modèle stochastique introduit notamment des dépendances entre les bits extraits successivement des oscillateurs à anneaux, et de surcroit sur des modèles de source d'aléa combinant plusieurs oscillateurs à anneaux.

[0019] Pour certaines applications, telles que celles décrites dans la norme AIS 31 du BSI (de l'allemand, *Bundesamt für Sicherheit in der Informationstechnik*), les exigences portant sur ces sources d'aléa sont renforcées en rendant obligatoire, pour le plus haut niveau de sécurité, la justification de la véritable imprédictibilité des échantillons générés.

[0020] La preuve de ce caractère imprédictible était auparavant définie uniquement par des tests statistiques des bit(s) produits en sortie du générateur de nombre(s) aléatoires.

[0021] Cette preuve requiert dorénavant une modélisation stochastique du fonctionnement interne du générateur de nombre(s) aléatoire(s) et une preuve que le taux d'entropie par bit généré dans le modèle stochastique est supérieur à un seuil imposé (0,997 bit d'entropie par bit dans le standard AIS 31).

[0022] Dans l'état de l'art actuel, de nombreuses sources d'aléa physiques embarquées en technologie hardware FPGA ou ASIC exploitent le jitter de signaux d'horloge produits par des oscillateurs à anneaux. Pour ce type de sources, plusieurs modélisations stochastiques sont envisagées. Une première modélisation « simple » considère les bits échantillonnés comme indépendants et applique un modèle gaussien sur la variable physique échantillonnée à chaque tirage. La preuve de sécurité pour ces modèles rudi-

mentaires s'avère insuffisante pour une évaluation de haut niveau car :

- la variance mesurée expérimentalement (permettant de paramétrer le modèle) résulte en fait de l'action de plusieurs sources physiques de bruits combinées difficilement séparables, certaines non modélisées et potentiellement manipulables par un attaquant, et
- l'hypothèse d'indépendance des échantillons successivement produits n'est pas justifiée ni démontrée.

[0023] Une modélisation plus aboutie, est celle de l'article « On the security of oscillator-based random number generators" de Matthieu Baudet, David Lubicz, Julien Micolod, et André Tassiaux. Cet article introduit, pour une source d'aléa à base d'oscillateurs, un modèle stochastique de l'évolution de la phase des signaux d'horloge générés sous la forme d'un processus de Wiener. La source de bruit prise en compte par ce modèle est uniquement le bruit « blanc » issue de l'agitation thermique électronique qui perturbe localement le signal d'horloge de l'oscillateur. Or, ce bruit n'est pas manipulable par un attaquant, et est par nature indépendant de toutes les autres sources de bruits. De plus, ce modèle ne suppose pas que les bits extraits successivement sont indépendants. Au contraire, il décrit l'évolution de la phase entre deux instants successifs. Cette évolution est ainsi modélisée comme la somme de deux termes : un premier terme déterministe qui traduit l'évolution moyenne caractérisée par la période du signal d'horloge généré par l'oscillateur, et un second terme issu du bruit thermique correspondant à un saut aléatoire « gaussien » dont la variance est proportionnelle à la durée.

[0024] Seule cette seconde modélisation, que nous nommons modélisation « thermique » dans la suite du document, permet d'apporter une preuve compatible du plus haut niveau de sécurité.

[0025] En pratique, une source d'aléa complète combine plusieurs oscillateurs. En particulier, ceci permet : en premier lieu d'augmenter la quantité d'entropie capturée à chaque instant et donc d'augmenter le débit d'échantillons en sortie ; et par ailleurs de tenir compte d'une « marge de sécurité » en supposant par principe que certaines sources élémentaires sont possiblement « en panne » et ne contribuent pas à l'entropie (afin de tenir compte de phénomènes physiques exceptionnels - métastabilité dans le processus d'échantillonnage, SEU, au autre qui ne sont pas directement pris en compte dans le modèle stochastique).

[0026] La méthodologie de preuve sur ces modèles repose sur trois piliers : la définition du modèle stochastique « thermique », un processus expérimental permettant d'estimer les paramètres du modèle « thermique », et une méthode permettant de caractériser le taux d'entropie en fonction des paramètres du modèle « thermique ».

[0027] On connait de l'article « On the security of oscillator-based random number ge-

nerators" de Matthieu Baudet, David Lubicz, Julien Micolod, et André Tassiaux, le modèle stochastique « thermique », sous forme de processus de Wiener bien établi utilisable pour chaque oscillateur à anneau, et gouverné plus précisément par 3trois paramètres spécifiques de chaque oscillateur :

- le rapport cyclique du signal d'horloge produit par l'oscillateur (qui caractérise l'écart possible entre la durée où le signal d'horloge atteint son amplitude haute, et celle où il est en position basse)
- la dérive qui caractérise la période moyenne du signal d'horloge produit par l'oscillateur
- la volatilité qui caractérise la variance de la phase proportionnelle à la durée entre 2 acquisitions.

[0028] Un quatrième paramètre commun à tous les oscillateurs est la fréquence d'échantillonnage des signaux d'horloge produit par les oscillateurs, qui fixe la durée entre deux acquisitions.

[0029] En outre, on connait de l'article « Towards an oscillator based TRNG with a certified entropy rate », de David Lubicz et Nathalie Bochard, une méthode d'estimation expérimentale des paramètres précités spécifiques à chaque oscillateur.

[0030] Concernant la caractérisation du taux d'entropie, dans l'état de l'art de la modélisation « thermique », seul le cas de la combinaison des sources élémentaires par une fonction XOR binaire est envisagé. Autrement dit la fonction ne fournit qu'un seul bit de sortie par échantillonnage. Avec ce modèle stochastique il est en effet difficile de déduire un seuil d'entropie si la source utilise une fonction quelconque pour combiner les bits unitaires issus des différentes sources élémentaires.

[0031] Ceci est d'autant plus vrai si la source combine les bits issus des différentes sources en un vecteur composé de plusieurs bits en sortie, plutôt qu'en un unique bit (c'est-à-dire si la fonction de combinaisons prend L bits en entrée - issus de L sources élémentaires - pour dériver un vecteur de k bits en sorties). Or, l'utilisation d'une fonction XOR pour recombiner les flux binaires des sources élémentaires devient peu efficace dès que le nombre de sources élémentaires combinées augmente. La quantité d'entropie « prouvée » sur le bit en sortie est alors bien inférieure à la somme des entropies prouvées pour chaque source élémentaire (et de toute façon nécessairement inférieure à 1 quel que soit le nombre de sources élémentaires en entrée). Beaucoup d'entropie disponible en amont de la fonction de combinaison est ainsi « gaspillée », ce qui limite les performances.

[0032] Ainsi, les articles précités sont en mesure de quantifier l'entropie associée à un générateur de nombre(s) aléatoire(s), seulement dans un cas particulier où la fonction de composition est une fonction XOR qui ne fournit qu'un seul bit à chaque échantillonnage. Or, l'utilisation d'une telle fonction est très limitée. D'autres fonctions de

recombinaisons permettraient d'obtenir des sources d'aléa plus performantes, mais elles ne sont pas modélisées à ce jour et ne permettent donc pas d'apporter la preuve de sécurité attendue.

[0033] Il est donc particulièrement difficile de réussir à concevoir un générateur de nombre(s) aléatoire(s) combinant plusieurs oscillateurs qui soit qualifié pour le respect d'un seuil du taux d'entropie τ lorsque la fonction de composition est notamment vectorielle, c'est à dire lorsqu'une sortie de la fonction de composition forme un vecteur bits. Autrement dit, les méthodes de l'art antérieur ne s'appliquent pas à la conception d'un générateur de nombre(s) aléatoire(s) dans lequel la fonction de composition fournit en sa sortie plusieurs bits à chaque période d'échantillonnage.

[0034] A cet effet, l'invention a pour objet un procédé de qualification d'un générateur de nombre(s) aléatoire(s) pour le respect d'un seuil prédéfini de taux d'entropie, le générateur de nombre(s) aléatoire(s) comprenant :

- un nombre d'oscillateurs à anneau, chacun générant un signal créneau,
- un module d'acquisition d'une valeur du signal créneau de chaque oscillateur à anneau suivant une fréquence d'acquisition, et
- un module de composition connecté au module d'acquisition et propre à fournir, depuis les valeurs acquises des signaux créneaux, un vecteur de bits formant le nombre aléatoire, par application auxdites valeurs d'une fonction de composition,

[0035] le taux d'entropie du générateur de nombre(s) aléatoire(s) étant la limite, quand un nombre de générations de vecteurs de bits tend vers l'infini, d'un rapport entre l'entropie de Shannon par bit d'une suite des vecteurs de bits successivement généré, et le nombre de générations successives,

[0036] le procédé étant mis en œuvre par un dispositif électronique de qualification et comprenant les étapes suivantes :

- réception du nombre d'oscillateurs à anneau compris dans le générateur de nombre(s) aléatoire(s), de la fonction de composition, de la fréquence d'acquisition de la valeur du signal créneau de chaque oscillateur à anneau, d'au moins un paramètre intrinsèque à chaque oscillateur à anneau et du seuil prédéfini de taux d'entropie,
- pour chaque oscillateur à anneau, détermination d'un majorant d'un biais à partir du ou des paramètres intrinsèques à l'oscillateur à anneau et de la fréquence d'acquisition,
- estimation d'un minorant du taux d'entropie du générateur de nombre(s) aléatoire(s) à partir du nombre d'oscillateurs à anneau reçu, de la fonction de composition reçue et de chaque majorant de biais déterminé,
- comparaison du minorant estimé au seuil prédéfini de taux d'entropie, et

– qualification du générateur de nombre(s) aléatoire(s) uniquement si le minorant estimé est supérieur au seuil prédéfini de taux d'entropie.

[0037] Avec le procédé selon l'invention, l'estimation du minorant de taux d'entropie garantit un taux d'entropie du générateur supérieur au minorant estimé qui est lui-même supérieur au seuil prédéfini de taux d'entropie.

[0038] Suivant des modes de réalisation particuliers, le procédé comprend une ou plusieurs des caractéristiques suivantes, prise(s) isolément ou suivant toutes les combinaisons techniquement possibles :

[0039] - pour chaque oscillateur à anneau, les paramètres intrinsèques sont représentatifs d'un modèle stochastique thermique dans chaque oscillateur à anneau et comprennent : un rapport cyclique du signal créneau de chaque oscillateur à anneau et une volatilité du modèle thermique de l'oscillateur à anneau,

[0040] - la fonction de composition est une fonction linéaire des valeurs acquises des signaux créneaux,

[0041] - la fonction de composition est un code correcteur linéaire caractérisé par une longueur égale au nombre d'oscillateurs à anneau, une dimension égale au nombre de bits dans le vecteur de bits et une distance minimale prédéfinie,

[0042] - l'étape d'estimation comprend :

[0043] une détermination d'un majorant d'un biais en sortie de la fonction de composition du générateur de nombre(s) aléatoire(s) à partir des majorants du biais de chaque oscillateur à anneau, et

[0044] une estimation du minorant du taux d'entropie du générateur de nombre(s) aléatoire(s) selon l'équation suivante :

[0045] $$H_{min} = \frac{1}{k}\left(k - \frac{(2^k-1)B_F^2}{2\ln(2)} - \Delta\left(\left(2^k-1\right)B_F\right)\right)$$

[0046] où ln( ) est le logarithme népérien, et

[0047] $$\Delta(B_F) = \frac{1}{\ln(2)}\left(\left(1-B_F\right)\ln\left(1-B_F\right) + B_F - \frac{B_F^2}{2}\right),$$

[0048] - lors l'étape d'estimation, le majorant du biais en sortie de la fonction de composition est égal au produit des majorants des biais de chaque oscillateur à anneau, et

[0049] - l'étape de réception comprend la réception d'une marge quantifiant un nombre d'oscillateur(s) à anneau dont une contribution au minorant estimé est nulle,

[0050] lors de l'étape d'estimation, le minorant de taux d'entropie est estimé en outre à partir de la marge.

[0051] L'invention a également pour objet un produit programme d'ordinateur comprenant des instructions logicielles qui, lorsqu'elles sont exécutées par un ordinateur, mettent en œuvre un procédé de qualification tel que décrit ci-dessus.

[0052] L'invention a également pour objet un procédé de conception d'un générateur de

nombre(s) aléatoire(s) comprenant :

- un nombre d'oscillateurs à anneau, chacun générant un signal créneau,
- un module d'acquisition d'une valeur du signal créneau de chaque oscillateur à anneau suivant une fréquence d'acquisition, et
- un module de composition connecté au module d'acquisition et propre à fournir, depuis les valeurs acquises des signaux créneaux, un vecteur de bits formant le nombre aléatoire, par application auxdites valeurs d'une fonction de composition,

[0053] le taux d'entropie du générateur de nombre(s) aléatoire(s) étant la limite, quand un nombre de générations de vecteurs de bits tend vers l'infini, d'un rapport entre l'entropie de Shannon par bit d'une suite des vecteurs de bits successivement généré, et le nombre de générations successives,

[0054] le procédé comprenant les étapes suivantes :

- réception du nombre d'oscillateurs à anneau, de la fonction de composition et d'au moins un paramètre intrinsèque à chaque oscillateur à anneau,
- initialisation d'une valeur de la fréquence d'acquisition,
- qualification du générateur de nombre(s) aléatoire(s) par un procédé de qualification tel que décrit plus haut, à partir du nombre d'oscillateurs à anneau, de la fonction composition comprenant les coefficients réglables, le(s) paramètre(s) intrinsèque(s), et de la valeur de la fréquence d'acquisition,

[0055] tant que le générateur de nombre(s) aléatoire(s) n'est pas qualifié lors de l'étape de qualification, le procédé comprend en outre les étapes suivantes :

- modification de la fréquence d'acquisition et de préférence de la fonction de composition, et réitération de l'étape de qualification.

[0056] L'invention a également pour objet un dispositif électronique de qualification électronique de qualification d'un générateur de nombre(s) aléatoire(s) pour le respect d'un seuil prédéfini de taux d'entropie, le générateur de nombre(s) aléatoire(s) comprenant :

- un nombre d'oscillateurs à anneau, chacun générant un signal créneau,
- un module d'acquisition d'une valeur du signal créneau de chaque oscillateur à anneau suivant une fréquence d'acquisition, et
- un module de composition connecté au module d'acquisition et propre à fournir, depuis les valeurs acquises des signaux créneaux, un vecteur de bits formant le nombre aléatoire, par application auxdites valeurs d'une fonction de composition,

[0057] le taux d'entropie du générateur de nombre(s) aléatoire(s) étant la limite, quand un nombre de générations de vecteurs de bits tend vers l'infini, d'un rapport entre l'entropie de Shannon par bit d'une suite des vecteurs de bits successivement généré, et le nombre de générations successives,

[0058] le dispositif électronique de qualification comprenant :

- un module d'entrée propre à recevoir le nombre d'oscillateurs à anneau compris dans le générateur de nombre(s) aléatoire(s), la fonction de composition, la fréquence d'acquisition de la valeur du signal créneau de chaque oscillateur à anneau, au moins un paramètre intrinsèque à chaque oscillateur à anneau, et le seuil prédéfini de taux d'entropie,
- un module de calcul propre à déterminer, pour chaque oscillateur à anneau, un majorant d'un biais à partir du ou des paramètres intrinsèques à l'oscillateur à anneau et à partir de la fréquence d'acquisition,

[0059] le module de calcul étant en outre propre à estimer le minorant du taux d'entropie du générateur de nombre(s) aléatoire(s) à partir du nombre acquis d'oscillateurs à anneau, de la fonction de composition acquise et de chaque majorant de biais déterminé,

- un module de comparaison du minorant estimé au seuil prédéfini de taux d'entropie, et
- un module de sortie propre à qualifier le générateur de nombre(s) aléatoire(s) uniquement si le minorant estimé est supérieur au seuil prédéfini de taux d'entropie.

[0060] Ces caractéristiques et avantages de l'invention apparaitront plus clairement à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple non-limitatif, et faite en référence aux dessins annexés, sur lesquels :

[0061] [Fig.1] la [Fig.1] est une représentation schématique d'un générateur de nombre(s) aléatoire(s) ;

[0062] [Fig.2] la [Fig.2] est une représentation schématique d'un dispositif électronique de qualification du générateur de nombre(s) aléatoire(s) de la [Fig.1] ;

[0063] [Fig.3] la [Fig.3] est un organigramme d'un procédé de qualification du générateur de nombre(s) aléatoire(s) de la [Fig.1] ; et

[0064] [Fig.4] la [Fig.4] est un organigramme d'un procédé de conception du générateur de nombre(s) aléatoire(s) de la [Fig.1].

[0065] On décrit en référence à la [Fig.1], un générateur de nombre(s) aléatoire(s) 10. Le générateur de nombre(s) aléatoire(s) 10 est par exemple un dispositif électronique propre à être intégré à une carte électronique et embarqué dans un système électronique tel qu'un système électronique de cryptographie.

[0066] Le générateur de nombre(s) aléatoire(s) 10 comprend un nombre L d'oscillateurs à anneau 11 (de l'anglais *ring oscillator*), un module d'acquisition 12 connecté aux L oscillateurs à anneau 11, et un module de composition 13 connecté aux sorties du module d'acquisition 13.

[0067] Le générateur de nombre(s) aléatoire(s) 10, aussi appelé générateur 10, est propre à générer, depuis les L oscillateurs à anneau 11, un vecteur de k bits V formant le

nombre aléatoire et comprenant k bits V_i.

[0068] Le nombre L d'oscillateurs à anneau 11 est par exemple compris entre seize et cent vingt-huit. Ce nombre L dépend de l'application du générateur de nombre(s) aléatoire(s) 10 et de contraintes de volume, de poids, et/ou de puissance électrique associées à l'application.

[0069] Chaque oscillateur à anneau 11 est un circuit électronique logique comprenant un nombre impair de portes logiques 14 dont une fonction logique est « NON » (de l'anglais, *Not gate*). Les portes logiques 14 sont connectées les unes aux autres formant une boucle de connexion. Préférentiellement, chaque oscillateur à anneau 11 comprend trois, cinq ou sept portes de fonction logique « NON ».

[0070] Un point de sortie 15 est défini entre deux portes logiques. Le point de sortie 15 est connecté à une entrée du module d'acquisition 12. Chaque oscillateur à anneau 11 comprenant un nombre impair de porte logique « NON », la valeur du signal S_i au point de sortie 15 oscille entre un potentiel haut correspondant à une valeur de bit égale à un, et un potentiel bas correspondant à une valeur de bit égale à zéro. Ainsi, le signal S_i au point de sortie 15 est un signal créneau ayant une période propre T_i et un rapport cyclique α_i, par exemple déterminés expérimentalement.

[0071] Le module d'acquisition 12 comprend un oscillateur 16 connecté à un compteur 17, lui-même connecté à une bascule 18.

[0072] L'oscillateur 16 est par exemple un oscillateur à anneau comportant une pluralité de portes logiques 14 et un point de sortie 15. De même que pour les oscillateurs à anneau 11, le signal Z au point de sortie 15 de l'oscillateur 16 est un signal créneau de période propre T. Ainsi, le signal Z comprend un front montant après chaque expiration d'une durée égale à la période propre T.

[0073] Le compteur 17 est connecté au point de sortie 15 de l'oscillateur 16, recevant ainsi le signal Z. Le compteur 17 est en outre connecté à une entrée d'horloge 19 de la bascule 18. Le compteur 17 est propre à incrémenter une valeur de compteur à chaque fois que le signal Z comprend un front montant. Le compteur 17 est en outre propre à fournir un signal d'horloge CLK comprenant un front montant lorsque le compteur atteint une valeur prédéfinie N. Lorsque le signal d'horloge CLK comprend un front montant, le compteur 17 réinitialise la valeur du compteur à zéro.

[0074] La bascule 18 est par exemple une bascule D (pour Data). La bascule 15 comprend L entrées de données connectées aux points de sortie 15 des L oscillateurs à anneau 11. La bascule comprend en outre l'entrée d'horloge 19 connectée au compteur 17. La bascule 15 comprend en outre L sorties de données connectées au module de composition 14. Chaque sortie de données est donc associée à une entrée de données respective.

[0075] Lorsque la bascule 18 reçoit le front montant du signal d'horloge CLK via son entrée

d'horloge 19, la bascule 18 acquière, via ses entrées de données, les valeurs S_i des signaux aux points de sortie 15 de chacun des L oscillateurs à anneau 11. La bascule 18 maintient à chacune de ses sorties de données, la valeur acquise par l'entrée de donnée associée, jusqu'à ce que le signal d'horloge CLK comprenne un nouveau front montant.

[0076] On comprend alors que le module d'acquisition 12 acquière les valeurs des signaux S_i aux points de sortie 15 de chaque oscillateur à anneau 11 à chaque expiration du délai $\Delta T = NT$, où N un la valeur prédéfinie du compteur 17. Autrement dit, une fréquence d'acquisition f_{acq} du module d'acquisition 12 est égale à l'inverse du délai ΔT.

[0077] Le module de composition 13 est connecté aux sorties de données de la bascule 18 et est propre à recevoir les valeurs maintenues S_i par la bascule 18 pendant la durée égale à ΔT. Le module de composition 13 implémente une fonction de composition F propre à convertir les L valeurs reçues par ses entrées, en un vecteur V de bits comprenant k bits V_i.

[0078] On entend par « vecteur de bits » une pluralité de valeurs de bits V_i réunies sous forme d'une ligne ou d'une colonne. Chaque composante V_i du vecteur de bits V est soit égal à zéro, soit à un.

[0079] Le nombre k de bits du vecteur de bits est par exemple compris entre deux et soixante-quatre.

[0080] La fonction de composition F est une fonction booléenne propre à convertir les L bits d'entrée S_i en le vecteur de bits V comprenant k composantes V_i.

[0081] Par exemple, la fonction de composition F est une fonction linéaire connue en soi. Ainsi, chaque bit $V_i$du vecteur de bits V en sortie du module de composition 13 est une combinaison linéaire des L bits en entrée du module de composition S_i. La fonction F est par exemple formulable sont la forme suivante :

[0082] [Math.2]

$$V = F(S_1, \ldots, S_L) = f[S_1, \ldots, S_L]$$

[0083] où f est une matrice comprenant une pluralité de lignes, une pluralité de colonnes et un coefficients C pour chaque ligne et chaque colonne.

[0084] Les coefficients C sont réglables. On entend par « réglables » le fait qu'une valeur est affectable à chaque coefficient C.

[0085] En variante encore, la fonction de composition F est un code correcteur linéaire, aussi appelé code linéaire. De manière connue en soi, le code linéaire est caractérisé par une longueur, une dimension et une distance minimale d.

[0086] La longueur du code linéaire est, dans le cas d'espèce, égale au nombre L d'oscillateurs à anneau 11 du générateur 10. La dimension du code linéaire est dans le cas d'espèce égale au nombre k de bits V_i dans le vecteur de bits V. La distance minimale d est une grandeur prédéfinie inférieure ou égale au nombre L d'oscillateurs

à anneau 11. La dimension minimale d assure que chaque bit V_i du vecteur de bits V est une combinaison d'au moins d bits S_i en entrée du module de composition 13.

[0087] Si la fonction de composition F est un code linéaire, la fonction F est alors construite à partir d'une matrice génératrice de sorte à ce que chaque composante du vecteur de bits V soit une somme des L bits admis en entrée de la fonction, pondérés par des coefficients de la matrice génératrice.

[0088] Le module de composition 13 est par exemple connecté à un autre dispositif électronique non représenté. Le module de composition 13 fournit à ce dispositif le vecteur de bits V à la fréquence d'acquisition f_{acq}.

[0089] En référence à la [Fig.2], on décrit un dispositif électronique de qualification 20 du générateur de nombre(s) aléatoire(s) 10 pour le respect d'un seuil de taux d'entropie prédéfini H_{cible}. Le seuil de taux d'entropie H_{cible} est prédéterminé, par exemple égal à 0,997.

[0090] Le dispositif électronique de qualification 20 est par exemple un ordinateur mettant en œuvre un programme décrit ci-dessous.

[0091] Sur l'exemple de la [Fig.2], le dispositif électronique de qualification 20 comprend une unité d'affichage 22, au moins un périphérique 24, et une unité de traitement 30. L'unité d'affichage 22 est connectée à l'unité de traitement 30.

[0092] L'unité d'affichage 22 est par exemple un moniteur d'ordinateur propre à afficher, à destination d'un utilisateur, des informations issues de l'unité de traitement 30.

[0093] Le périphérique 24 comprend par exemple un clavier et/ou une souris pour permettre à un utilisateur d'interagir avec le dispositif électronique de qualification 20.

[0094] L'unité de traitement 30 comprend un processeur 34 connecté à une mémoire 36. La mémoire 36 stocke préférentiellement un produit programme d'ordinateur comprenant une pluralité de logiciels 40, 42, 44, 46, aussi appelés modules, ou briques logicielles. Ces logiciels comprennent des instructions logicielles qui, lorsqu'elles sont exécutées par le processeur 34 mettent en œuvre un procédé 100 de qualification du générateur de nombre(s) aléatoire(s).

[0095] Plus spécifiquement, la mémoire 36 stocke un module d'entrée 40 configuré pour recevoir, depuis l'utilisateur des informations sur le générateur 10 qui seront décrites ci-après. La mémoire 36 stocke également un module de calcul 42 propre à estimer un minorant H_{min} du taux d'entropie $^{\tau}$ du générateur 10 à partir des informations reçues par le module d'entrée 40. En outre, la mémoire 36 stocke un module de comparaison 44 propre à comparer le minorant estimé H_{min} avec un seuil H_{cible} de taux d'entropie $^{\tau}$ et un module de sortie 46 propre à qualifier le générateur 10 uniquement si le minorant H_{min} est supérieur au seuil de taux d'entropie H_{cible}.

[0096] En variante, les modules d'entrée 40, de calcul 42, de comparaison 44 et de sortie 46 sont stockés sur un support d'information non représenté. Le support d'information est

un support lisible par un ordinateur. Le support lisible d'information est un medium adapté à mémoriser des instructions électroniques et capable d'être couplé à un bus d'un système informatique.

[0097] A titre d'exemple, le support d'information est un disque optique, un CD-ROM, un disque magnéto-optique, une mémoire ROM, une mémoire RAM, une mémoire EPROM, une mémoire EEPROM, une carte magnétique, une carte optique ou une clé USB.

[0098] Le fonctionnement du dispositif électronique de qualification 20 va maintenant être décrit en référence à la [Fig.3] représentant un organigramme du procédé 100 de qualification du générateur de nombre(s) aléatoire(s) 10 pour le respect du seuil de taux d'entropie prédéfini H_{cible}.

[0099] Selon un premier mode de réalisation, le signal en sortie S_i de chaque oscillateur à anneau 11 comporte une partie aléatoire modélisée par un modèle thermique dû à une agitation thermique d'électrons à l'intérieur dudit oscillateur à anneau 11.

[0100] Selon ce modèle, à chaque tirage j, le signal de sortie a par exemple pour valeur :

[0101] [Math.3]

$$S_i(j) = R[a_i]\left(\varphi_i(T_0 + j\Delta T)\, mod\ 1\right)$$

[0102] où $R[a_i]$ est la fonction créneau sur l'intervalle $[0\,;\,1[$ qui vaut 0 sur l'intervalle $[0\,;\,a_i[$ et qui vaut 1 sur l'intervalle $]a_i\,;\,1[$,

[0103] $\varphi_i(T_0 + j\Delta T)$ est la phase relative entre ledit oscillateur à anneau 11 et l'oscillateur 16 du module d'acquisition 12, lors de la j-ième acquisition après un instant initial T_0, et

[0104] $mod\ 1$ est la fonction de congruence modulo 1.

[0105] On comprend alors que le signal de sortie S_i comprend un biais compris entre -1 et 1 et dont une valeur est égale à $2a_i - 1$.

[0106] La partie aléatoire dans le signal de sortie S_i de chaque oscillateur à anneau 11 provient donc de la phase relative $\varphi_i(\,)$.

[0107] Il est supposé que la phase relative $\varphi_i(T_0)$ à l'instant initial T_0 suit une loi uniforme de probabilité.

[0108] En outre, le modèle thermique inclut de considérer que chaque phase relative $\varphi_i(\,)$ suit un processus de Wiener de paramètres : la dérive μ_i du modèle thermique, et la volatilité du modèle thermique σ_i^2. Ainsi le signal S_i en sortie de chaque oscillateur à anneau 11 dépend des deux paramètres μ_i, σ_i^2 du processus de Wiener, du rapport cyclique a_i du signal créneau et de la période d'acquisition ΔT, i.e. de la fréquence d'acquisition f_{acq}.

[0109] Selon le modèle thermique, pour chaque oscillateur à anneau 11, la valeur du signal

de sortie S_i au j+1-ième tirage sachant la valeur de la phase $\varphi_i(\,)$ au j-ème tirage s'exprime par exemple selon l'équation suivante :

[0110] [Math.4]

$$S_i = S_i\left(j+1 \middle| \varphi_i(T_0 + j\Delta T) = x_i\right) = R\left[a_i\right]\left(\left(x_i^* + g_i\right) mod\ 1\right)$$

[0111] où x_i^* est la valeur moyenne de la phase relative $\varphi_i(T_0 + j\Delta T)$ à l'instant $T_0 + j\Delta T$, qui est égal à $S_i(j) + \mu_i \Delta T$, et

[0112] g_i est une variable aléatoire suivant la loi normale centrée et d'écart-type $\sigma_i\sqrt{\Delta T}$.

[0113] Ainsi, la valeur du signal de sortie S_i au j+1-ième tirage sachant la valeur de la phase $\varphi_i(\,)$ au j-ème tirage suit une loi de Bernoulli caractérisé par un biais ϵ_i qui dépend de la valeur de la phase $\varphi_i(\,)$ au j-ème tirage, par exemple selon l'équation suivante :

[0114] [Math.5]

$$\epsilon_i = P(S_i = 0) - P(S_i = 1) = E\left((-1)^{S_i}\right)$$

[0115] où $P(S_i = 0)$ est la probabilité que la valeur x_i du signal de sortie S_i au j+1-ième tirage soit égale à zéro, sachant la valeur de la phase $\varphi_i(\,)$, et

[0116] $P(S_i = 1)$ est la probabilité que la valeur x_i du signal de sortie S_i au j+1-ième tirage soit égale à un, sachant la valeur de la phase $\varphi_i(\,)$ au j-ème tirage.

[0117] On remarque alors que le biais ϵ_i de chaque oscillateur à anneau 11 dépend de la valeur x_i de la phase $\varphi_i(\,)$ au j-ème tirage.

[0118] Il existe donc une borne $|\epsilon_i|$ du biais ϵ_i en valeur absolue, indépendante de la valeur x_i de la phase $\varphi_i(\,)$. En effet, lorsque le rapport cyclique a_i est strictement supérieur à $\frac{1}{2}$, respectivement lorsque $1 - a_i > \frac{1}{2}$, la valeur x_i de la phase $\varphi_i(\,)$ qui maximise la valeur absolue du biais $|\epsilon(x_i)|$ est celle qui induit une valeur moyenne de la phase $x_i^* = x_i + \mu_i \Delta T$ au milieu de l'intervalle de phase sur [0,1] qui produit 0 (respectivement 1)✹

[0119] Initialement, lors d'une étape de réception 102, le module d'entrée 40 reçoit les informations du générateur 10, à savoir : le nombre L d'oscillateurs à anneau 11 compris dans le générateur 10, la fonction de composition F, la fréquence d'acquisition $f_{acq} = \frac{1}{\Delta T}$, des paramètres intrinsèques à chaque oscillateur à anneau 11 et le seuil de taux d'entropie H_{cible}, et optionnellement une marge M.

[0120] Dans ce premier mode de réalisation, les paramètres intrinsèques à chaque oscillateur à anneau 11 sont préférentiellement : le rapport cyclique a_i, et la volatilité de phase σ_i du modèle thermique définis précédemment.

[0121] La marge M est un nombre d'oscillateurs à anneau 11 ne contribuant pas à l'entropie

du générateur 10. Ainsi, la marge M permet de prendre en compte des oscillateurs à anneau défectueux ou faisant apparaître des phénomènes de métastabilité.

[0122] Puis, lors d'une étape de détermination 104, pour chaque oscillateur à anneau 11, le module de calcul 42 détermine un majorant Bi du biais ϵ_i,qui est indépendant de la valeur de la phase au j-ème tirage, à partir de la fréquence d'acquisition f_{acq} et des paramètres intrinsèques à l'oscillateur à anneau 11, à savoir le rapport cyclique α_i et de la volatilité σ_i. Il est clair que le biais Bi dépend alors du modèle thermique considéré dans ce premier mode de réalisation.

[0123] Le module de calcul 42 calcule par exemple chaque majorant B_i du biais ϵ_i selon les équations suivantes :

[0124] [Math.6]

$$\theta_0 = 0;$$

[0125] $$\theta_1 = \frac{\max(\alpha_i, 1-\alpha_i)}{2};$$

[0126] $$\theta_2 = 1 - \frac{\max(\alpha_i, 1-\alpha_i)}{2};$$

[0127] $$\theta_3 = 1$$

[0128] $$B_i = 2\sum_{j\geq 0}\left(D\left(\frac{\theta_3+j}{\sigma_i\sqrt{\frac{1}{f_{acq}}}}\right) - 2D\left(\frac{\theta_2+j}{\sigma_i\sqrt{\frac{1}{f_{acq}}}}\right) + 2D\left(\frac{\theta_1+j}{\sigma_i\sqrt{\frac{1}{f_{acq}}}}\right) - D\left(\frac{\theta_0+j}{\sigma_i\sqrt{\frac{1}{f_{acq}}}}\right)\right)$$

[0129] où $\sum_{j\geq 0}$ désigne la somme pour tous les entiers j positifs ou nuls, et

[0130] $D(\,)$ est la fonction de répartition de la loi normale centrée réduite.

[0131] De préférence, si les oscillateurs à anneau 11 sont tous similaires entre eux, les majorant $B_i$des biais ϵ_i de chaque oscillateur à anneau 11 sont égaux.

[0132] Puis, lors d'une étape d'estimation 106, le module de calcul 42 estime un minorant H_{min} du taux d'entropie τ du générateur 10, à partir de chaque bais B_i calculé, du nombre L d'oscillateurs à anneau 11 dans le générateur 10, et de la fonction de composition F.

[0133] A cet effet, le module de calcul 42 détermine pour chaque combinaison linéaire de bits de sortie de F (i.e. a.F(x) = <a | F(x)>), premièrement un majorant $B_{a.F}$du biais en cette composante en sortie de la fonction de composition F du générateur 10, par exemple selon l'équation suivante :

[0134] [Math.7]

$$B_{aF} = \frac{1}{2^L}\sum_{w=(w_1,\ldots,w_L)\in\{0,1\}^L}\left(|\hat{F}(a,w)|\prod_{i=1}^{L}B_i^{w_i}\right)$$

[0135] où $\sum_{w=(w_1,\ldots,w_L)\in\{0,1\}^L}$ est la somme sur tous les vecteurs w de L bits,

[0136] $\hat{F}(a,w)$ désigne la transformée de Walsh de $(-1)^{a.F}$ au point w évaluée suivant l'équation :

[0137] [Math.8]

$$\forall\ a \in \{0,1\}^k,\ \forall\ w \in \{0,1\}^L\quad \hat{F}(a,w) = \sum_{x\in\{0,1\}^L} (-1)^{aF(x)+w.x}$$

[0138] $||$ est la fonction valeur absolue,

[0139] $\prod_{i=1}^{L}$ est le produit pour un indice i allant de 1 à L, et

[0140] $B_i^{w_i}$ est égal à B_i si le bit w_i vaut 1 ou est égal à 1 si le bit w_i vaut 0.

[0141] Le module de calcul 42 détermine alors à l'aide des quantités $B_{a.F}$, un majorant B_F des biais en sortie de F, valable pour toute composante a, suivant le calcul :

[0142] [Math.9]

$$B_F = Max(B_{aF})_{a\in\{0,1\}^k\setminus\{0\}}$$

[0143] Toujours lors de l'étape d'estimation 106, pour chaque oscillateur à anneau 11, le module de calcul 42 calcule des coefficients, de préférence trois coefficients notés $A_i(0)$, $A_i(1)$, $A_i(2)$, à partir des équations suivantes :

[0144] [Math.10]

$$A_i(0) = 1$$

[0145] $A_i(1) = 2a_i - 1$

[0146] $A_i(2) = \int_0^1 \gamma_i(y)^2 dy$

[0147] où pour tout y, $\gamma_i(y) = \int_0^1 G_i(x)\,(-1)^{R[a_i](x-y) \bmod 1)} dx$, avec $G_i(x) = \sum_{j\in Z} g[\sigma_i^2 \Delta T](x+y)$ dans lequel $g[\sigma_i^2\Delta T]()$ est une distribution Gaussienne centrée d'écart type $\sigma_i\sqrt{\Delta T}$.

[0148] $\varepsilon_{aF}(x_1, x_2, \ldots, x_L)$ désigne le biais de la variable aléatoire correspondant à la combinaison linéaire $a.F$ des bits en sortie de F, sachant les phases $\varphi_i(t_0 + jT) = x_i,\ 1 \le i \le L$

[0149] $A(x_1, x_2, \ldots, x_L) = \sum_{a\in\{0,1\}^k\setminus\{0\}} \varepsilon_{aF}(x_1, x_2, \ldots, x_L)^2$, et

[0150] A^{moy} est la moyenne de $A(x_1, x_2, \ldots, x_L)$ sur le domaine des états $[0,1]^L$.

[0151] Le module de calcul 42 calcule ensuite cette valeur moyenne A^{moy} par exemple selon l'équation suivante :

[0152] [Math.11]

$$A^{moy} = \frac{1}{2^{2L}} \sum_{\substack{u=(u_1,\ldots,u_L)\in\{0,1\}^L \\ v=(v_1,\ldots,v_L)\in\{0,1\}^L \\ a\in\{0,1\}^k\setminus\{0\}}} \left(\hat{Q}(a,u)\hat{Q}(a,v) \prod_{i=1}^{L} (A_i(u_i+v_i)) \right)$$

[0153] où $\sum_{\substack{u=(u_1,\ldots,u_L)\in\{0,1\}^L \\ v=(v_1,\ldots,v_L)\in\{0,1\}^L \\ a\in\{0,1\}^k\setminus\{0\}}}$ est la somme sur tous les vecteurs u de L bits, sur tous les

vecteurs v de L bits, et sur tous les vecteurs a de k bits différent du vecteur nul,

[0154] $\hat{Q}(a,u)$ est la transformée de Walsh de la fonction $(-1)^{a.F}$ évaluée pour le vecteur u,

[0155] $\hat{Q}(a,v)$ est la transformée de Walsh de la fonction $(-1)^{a.F}$ évaluée pour le vecteur v,

[0156] u_i est la i-ème composante du vecteur u, et

[0157] v_i est la i-ème composante du vecteur v.

[0158] Toujours lors de l'étape d'estimation 106, le module de calcul 42 estime ensuite le minorant de taux d'entropie H_{min} à partir du majorant B_F du biais en sortie de la fonction de composition F, du nombre k de bits dans le vecteur de bits V en sortie du module de composition 18 et de la valeur A^{moy}, par exemple selon l'équation suivante :

[0159] [Math.12]

$$H_{min} = \frac{1}{k}\left(k - \frac{1}{2\ln(2)}A^{moy} - \Delta\left(\left(2^k - 1\right)B_F\right)\right)$$

[0160] Puis lors d'une étape de comparaison 108, le module de comparaison 44 compare le minorant H_{min} estimé lors de l'étape d'estimation 106 avec le seuil de taux d'entropie H_{cible}.

[0161] Si le minorant estimé H_{min} est supérieur au seuil H_{cible} de taux d'entropie τ, alors lors d'une étape de qualification 110, le générateur 10 est qualifié. Par exemple le module de sortie 46 envoie, à destination de l'utilisateur du dispositif 20 et via l'unité d'affichage 22, un premier message indiquant que le taux d'entropie τ du générateur 10 est supérieur au seuil du taux d'entropie H_{cible}.

[0162] Sinon, lors d'une étape d'affichage 112, le module de sortie 46 envoie, à destination de l'utilisateur du dispositif 20 et via l'unité d'affichage 22, un deuxième message indiquant un échec de la qualification du générateur 10. L'utilisateur sait alors que le taux d'entropie τ du générateur 10 n'est pas garanti d'être supérieur au seuil de taux d'entropie H_{cible}.

[0163] Des variantes du procédé 100 de qualification vont maintenant être décrites.

[0164] Premièrement, des variantes du calcul du majorant B_F du biais en sortie de la fonction de composition F, vont être décrites. Dans chaque variante, sauf mention contraire explicite, l'estimation du minorant H_{min} est effectuée tel que décrit précédemment à partir du majorant B_F du biais en sortie de la fonction de composition F nouvellement décrit plutôt que de celui précédemment décrit.

[0165] Selon une première variante, lors de l'étape d'estimation 106, le module de calcul 42 détermine un majorant moins fin du biais sur une composante a.F en sortie de la fonction de composition F, par exemple selon l'équation suivante :

[0166] [Math.13]

$$B_{a.F} = \sqrt{\sum_{w=(w_1,\ldots,w_L)\in Spectre(a.F)}\left(\prod_{i=1}^{L} B_i^{2w_i}\right)}$$

[0167] où $\sum_{w=(w_1,\ldots,w_L)\in Spectre(a.F)}$ est la somme sur tous les vecteurs w dans le spectre de la fonction booléenne a.F.

[0168] Le spectre de la fonction booléenne a.F est l'ensemble des vecteur w tel que $\hat{F}(a,w)\neq 0$.

[0169] Toujours selon la première variante, si le vecteur nul appartient au spectre de la fonction a.F de la fonction de composition F, alors lors l'étape d'estimation 106, le majorant $B_{a.F}$ du biais est déterminé par exemple selon l'équation suivante plutôt que selon l'équation (13) :

[0170] [Math.14]

$$B_{a.F}=\sqrt{\left(1+B_1^2\right)\left(1+B_2^2\right)\ldots\left(1+B_L^2\right)-1}=\sqrt{-1+\sum_{i=1}^{L}\left(1+B_i^2\right)}$$

[0171] Il est clair que la détermination du majorant $B_{a.F}$ selon l'une des équations (13) et (14) est plus simple que selon l'équation (7). L'homme du métier remarquera tout de même que le majorant $B_{a.F}$ obtenu selon l'équation (13) ou (14) est plus grand que celui déterminé selon l'équation (7).

[0172] Selon une deuxième variante, si la fonction de composition F est une fonction linéaire, lors de l'étape d'estimation 106, le majorant B_F du biais en sortie de la fonction de composition F est déterminé selon l'équation suivante plutôt que selon l'équation (7) :

[0173] [Math.15]

$$B_F=\max_{\substack{a\in\{0,1\}^k\setminus\{0\}\\ u={}^tF(a)}}\left(B_1^{u_1}B_2^{u_2}\ldots B_L^{u_L}\right)=\max_{\substack{a\in\{0,1\}^k\setminus\{0\}\\ u={}^tF(a)}}\left(\prod_{i=1}^{L}B_i^{u_i}\right)$$

[0174] où $\max_{\substack{a\in\{0,1\}^k\setminus\{0\}\\ u={}^tF(a)}}()$ est la fonction maximum sur tous les vecteurs u tels que, pour tous vecteurs x de L coefficients et pour tout vecteur a non nul de k coefficients,

[0175] $u=(u_1,\ldots,u_L)\in\{0,1\}^L={}^tF(a)$ désigne les L coefficients de la forme linéaire des k bits de sortie de F, $a.F(x)$ écrite comme combinaison linéaire des L bits d'entrée de F, ie tel que $<a.\,|\,F(x)>=<u|x>$.

[0176] Selon une troisième variante, si la fonction de composition F est un code linéaire, lors de l'étape d'estimation 106, le module de calcul 42 détermine le majorant B_F du biais en sortie de la fonction de composition F selon l'équation suivante plutôt que selon l'équation (7) :

[0177] [Math.16]

$$B_F=\widetilde{B_1}\widetilde{B_2}\ldots\widetilde{B_d}=\prod_{i=1}^{d}\widetilde{B_i}$$

[0178] où, pour rappel, d est la distance minimale du code linaire, et

[0179] les $\widetilde{B_1}$, $\widetilde{B_2}$, ..., $\widetilde{B_d}$ sont les d majorants B_i de biais les plus grands parmi les L majorants de biais B_i.

[0180] Selon une quatrième variante combinable avec les première, deuxième et troisième variantes, si lors de l'étape d'acquisition 102, la marge M est acquise, alors lors de l'étape d'estimation 106, la détermination du majorant B_F du biais en sortie de la fonction de composition F selon l'une des équations (13) et (15), ne comprend le produit que des L-M majorants de biais B_i les plus élevés.

[0181] Selon la quatrième variante, si la fonction de composition est un code linéaire, la détermination du majorant B_F du biais en sortie de la fonction de composition F selon l'équation (16) ne comprend le produit que des d-M majorants de biais B_i les plus élevés.

[0182] Des variantes de l'estimation du minorant H_{min} et/ou de la valeur moyenne des coefficients d'aléa A^{moy} vont maintenant être décrites.

[0183] Selon une cinquième variante, si la fonction de composition F est linéaire, la valeur moyenne A^{moy} est calculée selon l'équation suivante :

[0184] [Math.17]

$$A^{moy} = \sum_{u=F^t(a)} a \in \{0,1\}^k \setminus \{0\} A_1(2)^{u_1} A_2(2)^{u_2} \ldots A_L(2)^{u_L}$$

[0185] plutôt que selon l'équation (11). Il est clair que selon cette cinquième variante, lors de l'étape d'estimation 106, les coefficients $A_i(0)$ et $A_i(1)$ ne sont pas calculés.

[0186] Préférentiellement, cette cinquième variante est combinée avec la troisième variante.

[0187] Selon une sixième variante, lors de l'étape d'estimation 106, le calcul de la valeur moyenne A^{moy} est remplacé par le calcul d'une valeur maximale A^{max} qui est toujours supérieure à la valeur moyenne A^{moy}.

[0188] Selon cette sixième variante, la valeur maximale A^{max} est calculée selon l'équation suivante :

[0189] [Math.18]

$$A^{max} = \sum_{a \in \{0,1\}^k \setminus \{0\}} B_{a,F}^2$$

[0190] Selon cette sixième variante, lors de l'étape d'estimation 106, les coefficients A_i ne sont pas calculés.

[0191] Selon une première sous-variante de cette sixième variante, si la fonction de composition F est linéaire, la valeur maximale A^{max} est calculée selon l'équation suivante :

[0192] [Math.19]

$$A^{max} = \sum_{u=F^t(a)} a \in \{0,1\}^k \setminus \{0\} \left(\prod_{i=1}^{L} B_i^{2u_i} \right)$$

[0193] plutôt que selon l'équation (18)

[0194] Selon une deuxième sous-variante de la sixième variante, si la fonction de com-

position F est un code linéaire, lors de l'étape d'estimation 106, aucun des coefficients A_i, de la valeur moyenne A^{moy}, ou de la valeur maximale A^{max} ne sont calculés. A la place, lors de l'étape d'estimation 106, le minorant H_{min} du taux d'entropie τ est directement calculé à partir du majorant B_F du biais en sortie de la fonction de composition F, et du nombre k de bits dans le vecteur de bits V en sortie du module de composition 18, par exemple selon l'équation suivante :

[0195] [Math.20]

$$H_{min} = \frac{1}{k}\left(k - \frac{(2^k-1)B_F^2}{2\ln(2)} - \Delta\left((2^k-1)B_F\right)\right)$$

[0196] Où $\Delta(B) = \frac{1}{ln(2)}\left((1-B)ln(1-B) + B - \frac{B^2}{2}\right)$

[0197] Un procédé 200 de conception du générateur 10 va maintenant être décrit en référence à la [Fig.4] représentant un organigramme de ce procédé 200.

[0198] Le procédé de conception 200 met en œuvre le dispositif électronique de qualification 20 de la [Fig.2].

[0199] Lors d'une étape de réception 202, le module d'entrée 40 reçoit, depuis l'utilisateur, la fonction de composition F comprenant le cas échéant les coefficients réglables C, les paramètre intrinsèques à chaque oscillateur à anneau 11, à savoir : le rapport cyclique α_i et la volatilité σ_i, le nombre L d'oscillateurs à anneau 11 dans le générateur 10 et optionnellement la marge M. Ces éléments reçus depuis l'utilisateur forment par exemple un cahier des charges de générateur 10.

[0200] Lors d'une étape d'initialisation 204, la fréquence d'acquisition f_{acq} et les coefficients réglables C de la fonction de composition F si ladite fonction F est une fonction linéaire qui n'est pas un code linéaire, sont initialisés à des valeurs initiales respective par l'utilisateur, via le périphérique 24.

[0201] Lors d'une étape de qualification 206, le dispositif de qualification 20 met en œuvre le procédé de qualification 100 décrit précédemment à partir des paramètres reçues et initialisés.

[0202] Puis, si suite à l'étape de qualification 206, le générateur 10 n'est pas qualifié, c'est-à-dire si le minorant H_{min} du taux d'entropie τ est inférieur au seuil H_{cible} de taux de d'entropie, alors, le procédé comprend une étape de modification 208. Lors de l'étape de modification 208, les paramètres réglables du générateur 10 sont modifiés.

[0203] Par exemple, le module d'entrée 40 reçoit depuis l'utilisateur et via le périphérique 24, de nouvelles valeurs de la fréquence d'acquisition f_{acq}, et le cas échéant des nouvelles valeurs des coefficients réglables C de la fonction de composition F.

[0204] Par exemple, si la fréquence d'acquisition f_{acq}diminue, une durée plus grande s'écoule entre deux tirages. Ainsi, le taux d'entropie τ du générateur 10 augmente et le minorant estimé H_{min} augmente également. Par exemple, une modification de la

fréquence d'acquisition f_{acq} est réalisée en modifiant la valeur de compteur prédéfinie N pour laquelle le compteur 17 envoie le signal d'horloge CLK avec un front montant. Une augmentation de cette valeur de compteur prédéfinie N induirait une augmentation de la période d'acquisition ΔT et donc une diminution de la fréquence d'acquisition f_{acq}.

[0205] Puis, l'étape de qualification 206 est réitérée.

[0206] Tant que le générateur 10 n'est pas qualifié lors de l'étape de qualification 206, les étapes de modifications 208 et de qualification 206 sont réitérées.

[0207] Si, suite à l'étape de qualification 206, le générateur 10 est qualifié, c'est-à-dire si le minorant estimé H_{min} est supérieur au seuil de taux d'entropie H_{cible}, alors le procédé de conception comprend une étape de validation 212.

[0208] Lors de l'étape de validation 212, le module de sortie 46 envoie préférentiellement, à l'unité d'affichage 22 et à destination de l'utilisateur, un message indiquant les valeurs des paramètres du générateurs 10 pour lesquels le générateur 10 a été qualifié lors de l'étape de qualification 206.

[0209] Avec le procédé de qualification 100 selon l'invention, le taux d'entropie τ du générateur est garanti d'être supérieur au seuil H_{cible} de taux d'entropie τ même si la fonction de composition F est complexe.

[0210] Ainsi, le procédé de qualification 100 permet de qualifier un générateur 10 plus complexe à qualifier que celui qualifié par l'état de l'art.

[0211] En outre, le recours à un code linéaire pour la fonction de composition F simplifie l'estimation du minorant H_{min} tout en permettant de générer à chaque tirage une pluralité de bits V_i dans le vecteur de bits V_i.

Revendications

[Revendication 1] Procédé (100) de qualification d'un générateur de nombre(s) aléatoire(s) (10) pour le respect d'un seuil prédéfini (H_{cible}) de taux d'entropie (τ), le générateur de nombre(s) aléatoire(s) (10) comprenant :

- un nombre (L) d'oscillateurs à anneau (11), chacun générant un signal créneau,
- un module d'acquisition (12) d'une valeur du signal créneau (S_i) de chaque oscillateur à anneau (11) suivant une fréquence d'acquisition (f_{acq}), et
- un module de composition (13) connecté au module d'acquisition (12) et propre à fournir, depuis les valeurs acquises des signaux créneaux (S_i), un vecteur de bits (V) formant le nombre aléatoire, par application auxdites valeurs (S_i) d'une fonction de composition (F),

le taux d'entropie (τ) du générateur de nombre(s) aléatoire(s) (10) étant la limite, quand un nombre de générations (D) de vecteurs de bits (V) tend vers l'infini, d'un rapport entre l'entropie de Shannon par bit d'une suite des vecteurs de bits (V) successivement généré, et le nombre de générations successives (D),
le procédé (100) étant mis en œuvre par un dispositif électronique de qualification (20) et comprenant les étapes suivantes :

- réception (102) du nombre (L) d'oscillateurs à anneau (11) compris dans le générateur de nombre(s) aléatoire(s) (10), de la fonction de composition (F), de la fréquence d'acquisition (f_{acq}) de la valeur du signal créneau (S_i) de chaque oscillateur à anneau (11), d'au moins un paramètre intrinsèque (a_i, σ_i) à chaque oscillateur à anneau (11) et du seuil prédéfini (H_{cible}) de taux d'entropie (τ),
- pour chaque oscillateur à anneau (11), détermination (104) d'un majorant (B_i) d'un biais (ϵ_i) à partir du ou des paramètres intrinsèques (a_i, σ_i) à l'oscillateur à anneau (11) et de la fréquence d'acquisition (f_{acq}),
- estimation (106) d'un minorant (H_{min}) du taux d'entropie (τ) du générateur de nombre(s) aléatoire(s) (10) à partir du nombre (L) d'oscillateurs à anneau reçu (11), de la fonction de

composition reçue (F) et de chaque majorant de biais déterminé (B_i),

- comparaison (108) du minorant estimé (H_{min}) au seuil prédéfini (H_{cible}) de taux d'entropie (τ), et
- qualification (110) du générateur de nombre(s) aléatoire(s) (10) uniquement si le minorant estimé (H_{min}) est supérieur au seuil prédéfini (H_{cible}) de taux d'entropie (τ).

[Revendication 2] Procédé (100) selon la revendication 1, dans lequel, pour chaque oscillateur à anneau (11), les paramètres intrinsèques (α_i, σ_i) sont représentatifs d'un modèle stochastique thermique dans chaque oscillateur à anneau (11) et comprennent : un rapport cyclique (α_i) du signal créneau de chaque oscillateur à anneau (11) et une volatilité (σ_i) du modèle thermique de l'oscillateur à anneau (11).

[Revendication 3] Procédé (100) selon la revendication 1 ou 2, dans lequel la fonction de composition (F) est une fonction linéaire des valeurs acquises des signaux créneaux (S_i).

[Revendication 4] Procédé (100) selon la revendication précédente, dans lequel la fonction de composition (F) est un code correcteur linéaire caractérisé par une longueur égale au nombre (L) d'oscillateurs à anneau (11), une dimension égale au nombre de bits dans le vecteur de bits (V) et une distance minimale prédéfinie (d).

[Revendication 5] Procédé (100) selon la revendication précédente, dans lequel l'étape d'estimation (106) comprend :
une détermination d'un majorant (B_F) d'un biais en sortie de la fonction de composition (F) du générateur de nombre(s) aléatoire(s) (10) à partir des majorants (B_i) du biais (ϵ_i) de chaque oscillateur à anneau (11), et une estimation du minorant (H_{min}) du taux d'entropie (τ) du générateur de nombre(s) aléatoire(s) (10) selon l'équation suivante :

$$H_{min} = \frac{1}{k}\left(k - \frac{(2^k-1)B_F^2}{2\ln(2)} - \Delta\left(\left(2^k-1\right)B_F\right)\right)$$

où $\ln(\,)$ est le logarithme népérien, et

$$\Delta(B_F) = \frac{1}{\ln(2)}\left((1-B_F)\ln(1-B_F) + B_F - \frac{B_F^2}{2}\right).$$

[Revendication 6] Procédé (100) selon la revendication précédente, dans lequel lors l'étape d'estimation (106), le majorant (B_F) du biais en sortie de la fonction de composition (F) est égal au produit des majorants (B_i) des biais (ϵ_i) de chaque oscillateur à anneau (11).

[Revendication 7] Procédé (100) selon l'une quelconque des revendications précédentes, dans lequel l'étape de réception (102) comprend la réception d'une marge (M) quantifiant un nombre d'oscillateur(s) à anneau (11) dont une contribution au minorant estimé (H_{min}) est nulle,
lors de l'étape d'estimation (104), le minorant (H_{min}) de taux d'entropie (τ) est estimé en outre à partir de la marge (M).

[Revendication 8] Produit programme d'ordinateur comprenant des instructions logicielles qui, lorsqu'elles sont exécutées par un ordinateur, mettent en œuvre un procédé de qualification (100) selon l'une quelconque des revendications précédentes.

[Revendication 9] Procédé (200) de conception d'un générateur de nombre(s) aléatoire(s) (10) comprenant :

- un nombre (L) d'oscillateurs à anneau (11), chacun générant un signal créneau,
- un module d'acquisition (12) d'une valeur du signal créneau (S_i) de chaque oscillateur à anneau (11) suivant une fréquence d'acquisition (f_{acq}), et
- un module de composition (13) connecté au module d'acquisition (12) et propre à fournir, depuis les valeurs acquises des signaux créneaux (S_i), un vecteur de bits (V) formant le nombre aléatoire, par application auxdites valeurs (S_i) d'une fonction de composition (F),

le taux d'entropie (τ) du générateur de nombre(s) aléatoire(s) (10) étant la limite, quand un nombre de générations (D) de vecteurs de bits (V) tend vers l'infini, d'un rapport entre l'entropie de Shannon par bit d'une suite des vecteurs de bits (V) successivement généré, et le nombre de générations successives (D),
le procédé (200) comprenant les étapes suivantes :

- réception (202) du nombre (L) d'oscillateurs à anneau (11), de la fonction de composition (F) et d'au moins un paramètre intrinsèque (α_i, σ_i) à chaque oscillateur à anneau (11),
- initialisation (204) d'une valeur de la fréquence d'acquisition (f_{acq}),
- qualification (206) du générateur de nombre(s) aléatoire(s) (10) par un procédé de qualification (100) selon l'une quelconque des revendications 1 à 7, à partir du nombre (L)

d'oscillateurs à anneau (11), de la fonction composition (F) comprenant les coefficients réglables (C), le(s) paramètre(s) intrinsèque(s) (α_i, σ_i), et de la valeur de la fréquence d'acquisition (f_{acq}),

tant que le générateur de nombre(s) aléatoire(s) (10) n'est pas qualifié lors de l'étape de qualification (206), le procédé (200) comprend en outre les étapes suivantes :

- modification (208) de la fréquence d'acquisition (f_{acq}) et de préférence de la fonction de composition (F), et réitération de l'étape de qualification (206).

[Revendication 10] Dispositif (20) électronique de qualification d'un générateur de nombre(s) aléatoire(s) (10) pour le respect d'un seuil prédéfini (H_{cible}) de taux d'entropie (τ), le générateur de nombre(s) aléatoire(s) (10) comprenant :

- un nombre (L) d'oscillateurs à anneau (11), chacun générant un signal créneau,
- un module d'acquisition (12) d'une valeur du signal créneau (S_i) de chaque oscillateur à anneau (11) suivant une fréquence d'acquisition (f_{acq}), et
- un module de composition (13) connecté au module d'acquisition (12) et propre à fournir, depuis les valeurs acquises des signaux créneaux (S_i), un vecteur de bits (V) formant le nombre aléatoire, par application auxdites valeurs (S_i) d'une fonction de composition (F),

le taux d'entropie (τ) du générateur de nombre(s) aléatoire(s) (10) étant la limite, quand un nombre de générations (D) de vecteurs de bits (V) tend vers l'infini, d'un rapport entre l'entropie de Shannon par bit d'une suite des vecteurs de bits (V) successivement généré, et le nombre de générations successives (D),
le dispositif électronique de qualification (20) comprenant :

- un module d'entrée (40) propre à recevoir le nombre (L) d'oscillateurs à anneau (11) compris dans le générateur de nombre(s) aléatoire(s) (10), la fonction de composition (F), la

fréquence d'acquisition (f_{acq}) de la valeur du signal créneau (S_i) de chaque oscillateur à anneau (11), au moins un paramètre intrinsèque (a_i, σ_i) à chaque oscillateur à anneau (11), et le seuil prédéfini (H_{cible}) de taux d'entropie (τ),

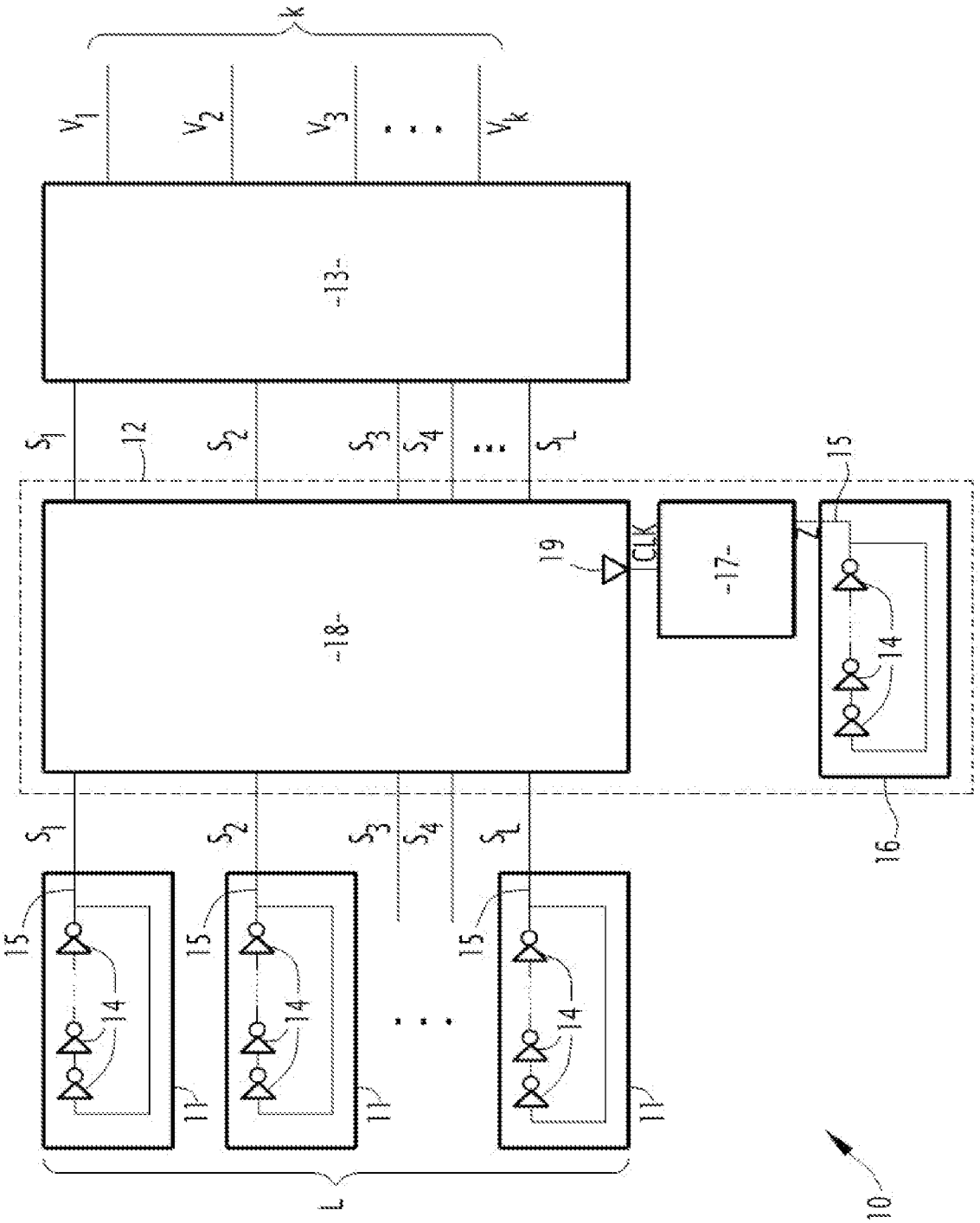
– un module de calcul (42) propre à déterminer, pour chaque oscillateur à anneau (11), un majorant (B_i) d'un biais (ϵ_i) à partir du ou des paramètres intrinsèques (a_i, σ_i) à l'oscillateur à anneau (11) et à partir de la fréquence d'acquisition (f_{acq}),

le module de calcul (42) étant en outre propre à estimer le minorant (H_{min}) du taux d'entropie (τ) du générateur de nombre(s) aléatoire(s) (10) à partir du nombre acquis (L) d'oscillateurs à anneau (11), de la fonction de composition acquise (F) et de chaque majorant (B_i) de biais (ϵ_i) déterminé,

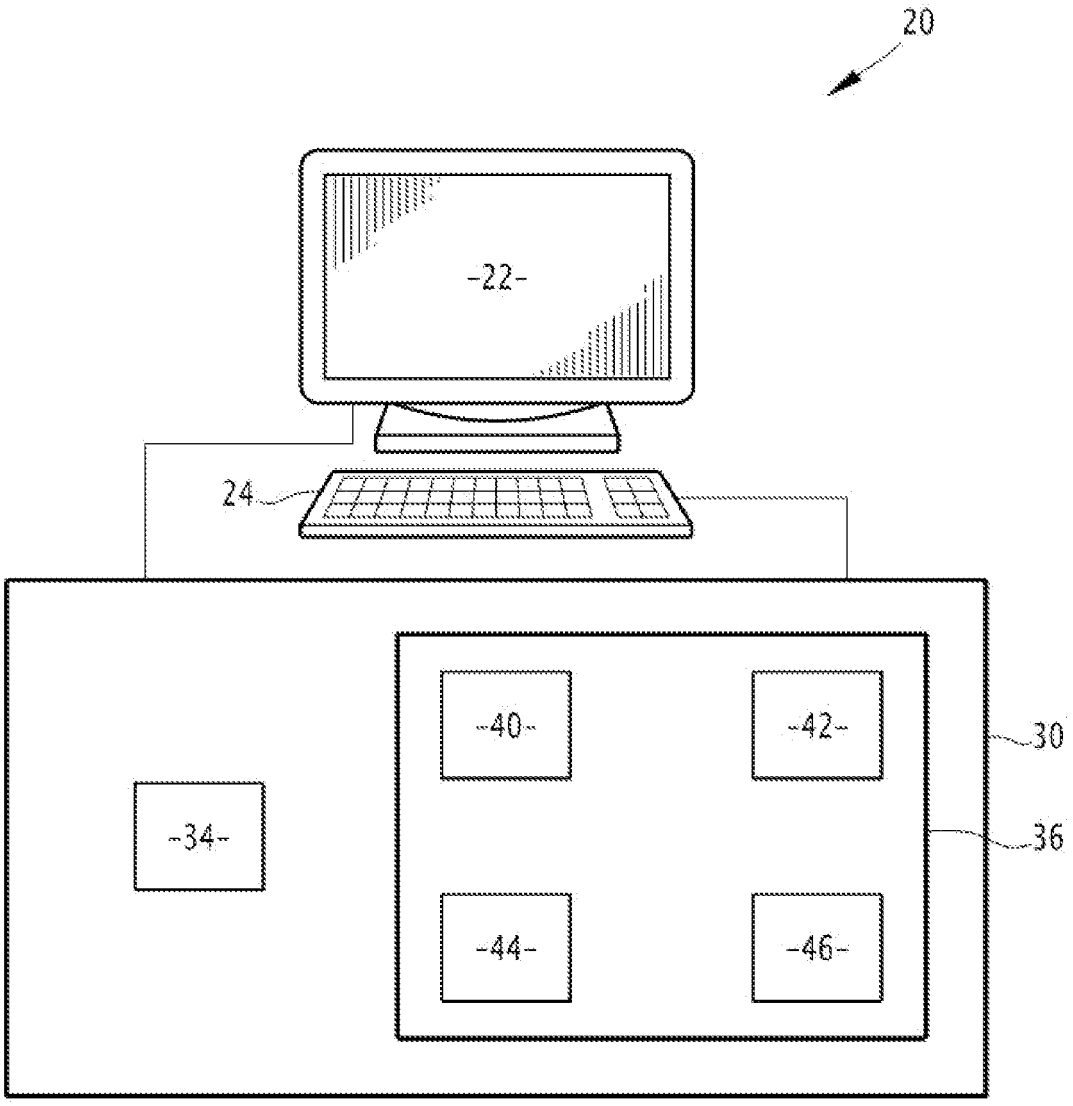
– un module de comparaison (44) du minorant estimé (H_{min}) au seuil prédéfini (H_{cible}) de taux d'entropie (τ), et

– un module de sortie (46) propre à qualifier le générateur de nombre(s) aléatoire(s) (10) uniquement si le minorant estimé (H_{min}) est supérieur au seuil prédéfini (H_{cible}) de taux d'entropie (τ).

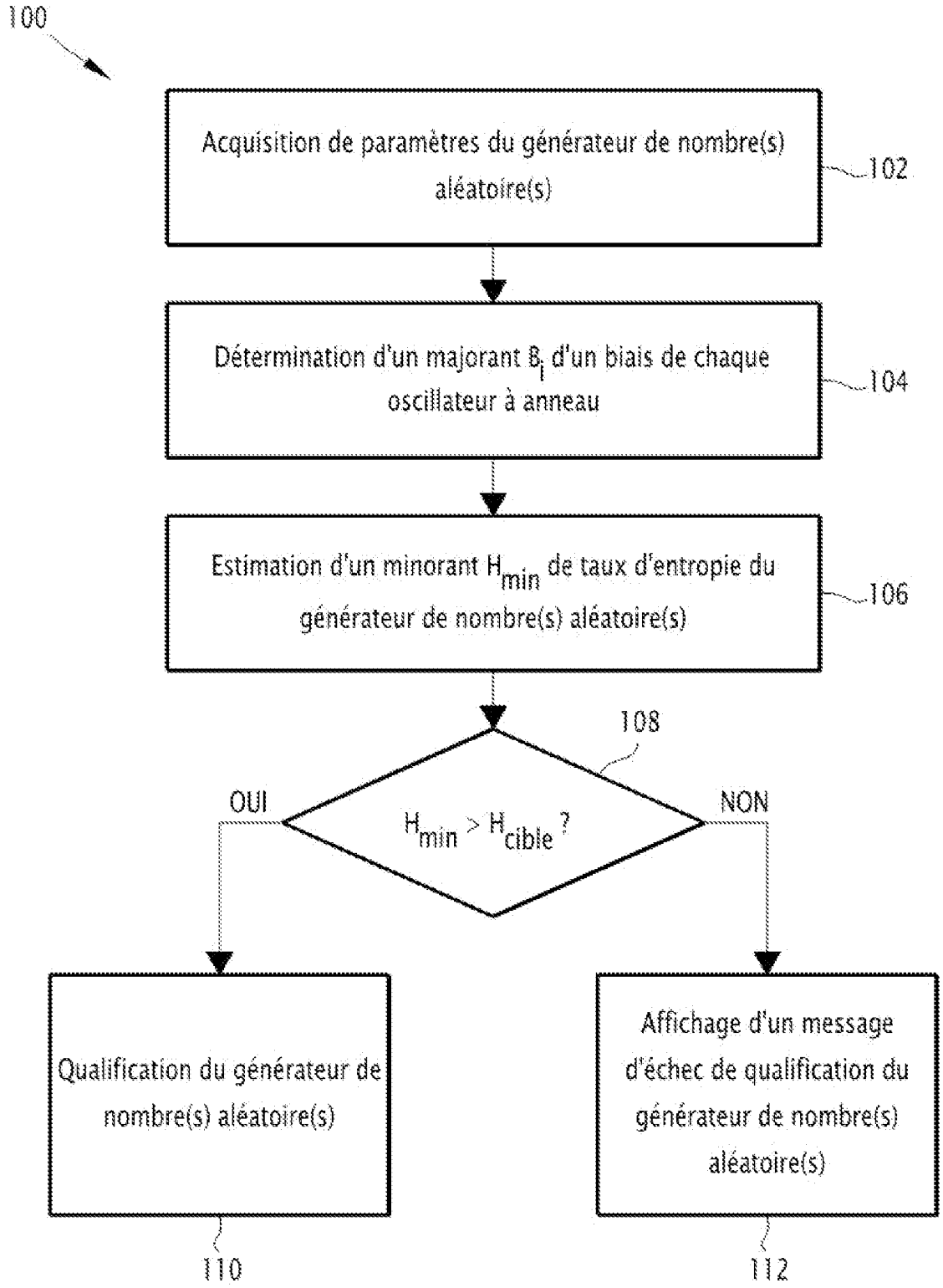
[Fig. 1]



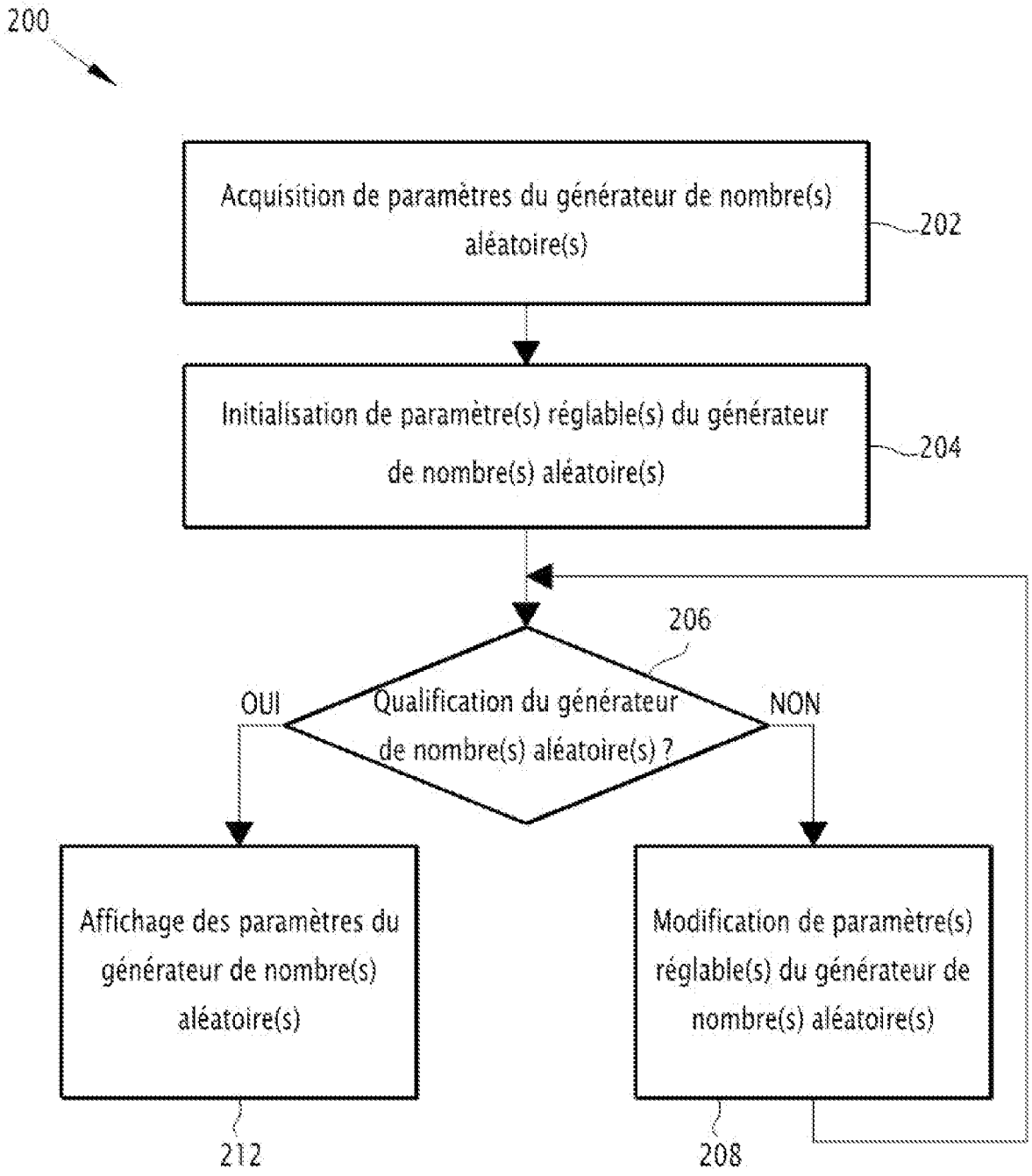
[Fig. 2]



[Fig. 3]


100
Acquisition de paramètres du générateur de nombre(s) aléatoire(s)
102
Détermination d'un majorant B_i d'un biais de chaque oscillateur à anneau
104
Estimation d'un minorant H_{min} de taux d'entropie du générateur de nombre(s) aléatoire(s)
106
108
$H_{min} > H_{cible}$?
OUI
NON
Qualification du générateur de nombre(s) aléatoire(s)
110
Affichage d'un message d'échec de qualification du générateur de nombre(s) aléatoire(s)
112

[Fig. 4]


200
Acquisition de paramètres du générateur de nombre(s) aléatoire(s)
202
Initialisation de paramètre(s) réglable(s) du générateur de nombre(s) aléatoire(s)
204
206
Qualification du générateur de nombre(s) aléatoire(s) ?
OUI
NON
Affichage des paramètres du générateur de nombre(s) aléatoire(s)
212
Modification de paramètre(s) réglable(s) du générateur de nombre(s) aléatoire(s)
208

RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

☐ Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

[x] Le demandeur a maintenu les revendications.

☐ Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

☐ Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

[x] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION

NEANT

2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL

YANG BOHAN ET AL: "On-chip jitter measurement for true random number generators",
2017 ASIAN HARDWARE ORIENTED SECURITY AND TRUST SYMPOSIUM (ASIANHOST), IEEE,
19 octobre 2017 (2017-10-19), pages 91-96, XP033338280,
DOI: 10.1109/ASIANHOST.2017.8354001
[extrait le 2018-05-03]

MA YUAN ET AL: "On the Entropy of Oscillator-Based True Random Number Generators",
10 janvier 2017 (2017-01-10), SAT 2015 18TH INTERNATIONAL CONFERENCE, AUSTIN, TX, USA, SEPTEMBER 24-27, 2015; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER, BERLIN, HEIDELBERG, PAGE(S) 165 - 180, XP047404289,
ISBN: 978-3-540-74549-5
[extrait le 2017-01-10]

BAUDET MATHIEU ET AL: "On the Security of Oscillator-Based Random Number Generators",
JOURNAL OF CRYPTOLOGY, SPRINGER US, NEW YORK,
vol. 24, no. 2,
20 octobre 2010 (2010-10-20), pages 398-425, XP037087985,
ISSN: 0933-2790, DOI: 10.1007/S00145-010-9089-3
[extrait le 2010-10-20]

Marek Laban ET AL: "HECTOR : D4.1 Demonstrator Specification",
,
3 mai 2017 (2017-05-03), XP055531437,
Extrait de l'Internet:
URL:https://hector-project.eu/downloads/HECTOR-D4.1-PU-M26.pdf
[extrait le 2018-12-07]

MARKKU-JUHANI O SAARINEN: "On Entropy and Bit Patterns of Ring Oscillator Jitter", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 3 février 2021 (2021-02-03), XP081873622,

BERNARD FLORENT ET AL: "From Physical to Stochastic Modeling of a TERO-Based TRNG", JOURNAL OF CRYPTOLOGY, SPRINGER US, NEW YORK, vol. 32, no. 2, 29 mars 2018 (2018-03-29), pages 435-458, XP036739175, ISSN: 0933-2790, DOI: 10.1007/S00145-018-9291-2 [extrait le 2018-03-29]

3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES

NEANT