RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 505 585**
(A n'utiliser que pour les commandes de reproduction).

A1

DEMANDE DE BREVET D'INVENTION

(21) **N° 81 09222**

(54) **Procédé et dispositif de génération de suites d'éléments suivant des lois aléatoires et orthogonales, notamment pour transmission radio par sauts de fréquence.**

(51) Classification internationale (Int. Cl. ³). **H 04 L 9/00; H 04 B 7/12; H 04 K 1/00.**

(22) Date de dépôt ..... 8 mai 1981.
(33) (32) (31) Priorité revendiquée :

(41) Date de la mise à la disposition du public de la demande ..... B.O.P.I. — « Listes » n° 45 du 12-11-1982.

(71) Déposant : THOMSON-CSF, société anonyme, résidant en France.

(72) Invention de : Philippe Sidin.

(73) Titulaire : *Idem* (71)

(74) Mandataire : P. Guilguet, Thomson-CSF, SCPI,
173, bd Haussmann, 75360 Paris Cedex 08.

PROCEDE ET DISPOSITIF DE GENERATION DE SUITES D'ELEMENTS SUIVANT DES LOIS ALEATOIRES ET ORTHOGONALES, NOTAMMENT POUR TRANSMISSION RADIO PAR SAUTS DE FREQUENCE

La présente invention concerne un procédé et un dispositif de génération de suites d'éléments suivant des lois aléatoires et orthogonales.

Si l'on appelle N le nombre de lois distinctes cherchées, ces N lois sont construites au niveau de N entités.

L'invention s'applique notamment aux transmissions radio militaires utilisant des sauts de fréquence pour se protéger contre l'interception et le brouillage. Lesdits éléments sont alors constitués par des valeurs de fréquence, et les entités génératrices par les divers postes radio appartenant aux différents réseaux, (par réseau, on entend un ensemble de quelques postes devant être en liaison permanente entre eux pour des raisons opérationnelles). Tous les postes appartenant à un réseau donné font strictement les mêmes opérations et ne constituent donc conceptuellement qu'une seule entité.

Dans cette application, lorsqu'un certain nombre de postes groupés en N réseaux distincts opérent simultanément sur un même terrain, il faut que tous les postes appartenant à un réseau donné disposent de la même succession de fréquences (appelée loi de fréquence), mais que les postes appartenant à des réseaux différents aient des lois différentes. Si les divers réseaux utilisent le même ensemble de fréquences, il peut se faire, si l'on ne prend aucune précaution, qu'une même fréquence soit choisie, à un instant donné, par les postes appartenant à des réseaux différents. Il en résulte alors un brouillage mutuel entre les réseaux, défavorable à la transmission.

Pour éviter ce brouillage intrinsèque, il est nécessaire de générer les fréquences des différents réseaux suivant des lois orthogonales, c'est-à-dire telles qu'à un instant donné, les fréquences générées suivant ces diverses lois soient toutes différentes.

Pour se protéger contre l'interception on impose de plus que chacune des lois utilisées soit aléatoire, ou à tout le moins pseudo-aléatoire, c'est-

à-dire que la succession des éléments apparaisse à qui ne connaît pas la loi, comme aléatoire.

Dans le cas de ces applications militaires on souhaite également que la coordination des lois de fréquence se fasse en recherchant le minimum de compromission du système. On entend par là qu'il faut viser à ce que la capture d'un poste appartenant à un réseau donné et l'examen des informations disponibles à ce niveau n'entraînent pas la connaissance des lois relatives aux autres réseaux.

Il faut souligner que l'application de la génération d'éléments suivant des lois aléatoires et orthogonales aux réseaux radio militaires n'est donnée qu'à titre illustratif. De telles lois sont utiles dans d'autres domaines présentant des exigences similaires, et la présente invention y est également applicable.

Les problèmes de génération d'éléments suivant des lois aléatoires ou orthogonales sont résolus de la manière suivante dans l'état de la technique.

On sait réaliser des générateurs, dits générateurs pseudo-aléatoires, qui sont capables de générer des éléments suivant des lois pseudo-aléatoires. Et pour résoudre le problème posé par l'orthogonalité des lois, on utilise classiquement une technique connue sous le nom de "tirage alphabet" ou de "tirage exhaustif". Cette méthode consiste à effectuer des tirages successifs dans un ensemble fini d'éléments, soit jusqu'à l'épuisement des éléments, auquels cas la méthode porte le nom de tirage exhausif, soit jusqu'à toute autre condition d'arrêt (nombre suffisant d'éléments ...), auquel cas la méthode porte le nom de tirage alphabet. Si les éléments ne sont pas tous différents, il faut de plus vérifier à chaque tirage que l'élément que l'on vient de tirer est différent de tous ceux déjà tirés.

Cette méthode a pour inconvénient majeur d'impliquer, là où elle est mise en oeuvre la connaissance de ce que font les postes. Il paraît en effet évident que pour ne pas se mettre sur la fréquence des autres postes, il est nécessaire de savoir quelles fréquences ces autres postes utilisent.

Par voie de conséquence, si elle est mise en oeuvre au niveau des postes, la contrainte de non compromission n'est pas respectée. Si elle l'est au niveau d'un "service central", il s'avère impossible de mémoriser au niveau des postes l'ensemble des informations utiles.

La présente invention a pour objet un procédé et un dispositif de génération d'éléments suivant des lois aléatoires et orthogonales évitant la connaissance au niveau de chaque poste des éléments générés par tous les autres postes et présentant donc un très faible risque de compromission.

Selon l'invention le procédé de génération d'éléments suivant des lois aléatoires et orthogonales, ces éléments étant au nombre de Y et étant générés par N entités distintes sous la forme de N suites infinies d'éléments s_{nj} (Y et N étant des nombres entiers, j un nombre entier croissant de 1 à l'infini et n un nombre entier variable de 1 à N), comporte :

- une première étape consistant à effectuer M tirages alphabet successifs de N nombres entier chacun, parmi un ensemble de X nombres entiers tous différents (M étant un nombre entier et X un nombre entier supérieur ou égal à N), le $n^{ième}$ tirage à l'intérieur du $m^{ième}$ tirage alphabet (m étant un nombre entier variable de 1 à M) fournissant un nombre x_{mn},

- une deuxième étape consistant à affectuer les nombres x_{mn} (avec n fixé) à la $n^{ième}$ entité en vue de la génération des éléments de la $n^{ième}$ suite,

- une troisième étape consistant à générer l'éléments s_{nj} sous la forme du $x_{mn}^{ième}$ élément obtenu au cours d'un tirage alphabet effectué parmi les Y éléments au niveau de la $n^{ième}$ entité, N tirages alphabet identiques étant effectués simultanément au niveau des N entités.

Les objets et caractéristiques de la présente invention apparaîtront plus clairement à la lecture de la description d'un exemple de réalisation, ladite description étant faite en relation avec le dessin ci-annexé représentant un schéma synoptique d'un dispositif pour la mise en oeuvre d'un procédé de génération conforme à l'invention.

Le procédé conforme à l'invention est destiné à générer N suites

comportant chacune un nombre infini d'éléments, chacune des suites étant générée suivant une loi pseudo-aléatoire et les N lois étant orthogonales entre elles (N étant un nombre entier). On appellera dans ce qui suit s_{nj} le $j^{ième}$ élément de la $n^{ième}$ suite ainsi générée (j étant un nombre entier variable de 1 à l'infini et n étant un nombre entier variable de 1 à N).

Le procédé de génération selon l'invention comporte une première étape qui consiste à effectuer M tirages alphabet successifs, de N nombres entiers chacun, parmi un même ensemble de X nombres entiers tous différents, M étant un nombre entier et X un nombre entier supérieur ou égal à N (et généralement inférieur ou égal à Y). On désigne par x_{mn} le nombre obtenu lors du $n^{ième}$ tirage à l'intérieur du $m^{ième}$ tirage alphabet (n étant un nombre entier variable de 1 à N et m un nombre entier variable de 1 à M). Le premier tirage alphabet fournit dans l'ordre les nombres x_{11} x_{12} ... X_{1N}. De même le $m^{ième}$ tirage alphabet fournit dans l'ordre les nombres x_{m1} x_{m2} ...x_{m2} ...x_{mN} et le $M^{ième}$ tirage alphabet fournit dans l'ordre les nombres x_{M1} x_{M2} ... x_{MN}.

Le procédé de génération selon l'invention comporte une deuxième étape au cours de laquelle on affecte les nombres x_{mn} résultant du $n^{ième}$ tirage à l'intérieur des M tirages alphabet successifs (m = 1,2 ...M et n fixé) à l'entité n (n = 1,2, ... N).

Cette deuxième étape se fait notamment en inscrivant les nombres x_{mn} dans une mémoire qui sera ensuite adressée en lecture de manière que la lecture du nombre x_{mn} soit utilisée pour la génération du $j^{ième}$ élément de la $n^{ième}$ suite, en imposant entre les éléments m et j la relation m = j modulo M. Dans l'application citée une mémoire se trouve ainsi localisée au niveau de chacun des postes. La mémoire localisée au niveau du poste générant la suite de numéro n fixé contient les nombres x_{mn} (avec n fixé et égal au numéro du réseau auquel appartient le poste et m variant de 1 à M).

Le procédé de génération selon l'invention comporte une troisième étape qui se déroule de la façon suivante. Pour cette troisième étape les instants t_j correspondant à la génération des éléments s_{nj} des N suites sont comptés modulo M à partir d'une origine de temps t_0 commune aux N suites. A chacun de ces instants de génération tj, un tirage alphabet

identique est fait au niveau de chacune des N entités parmi un même ensemble de Y éléments correspondant aux différents éléments qu'il est possible d'utiliser pour obtenir X nombres tous différents (avec la condition $Y \geqslant X$). On appelle y_{ij} ces éléments, avec i variant de 1 à X et j correspondant à l'instant d'émission considéré. Dans l'application décrite les Y éléments sont les fréquences allouées à l'ensemble des réseaux.

Au niveau de la $n^{ième}$ suite, et au temps considéré t_j, on prend comme j^e élément de cette suite : s_{nj}, le $x_{mn}^{ième}$ nombre obtenu au cours du tirage parmi les Y éléments effectué au temps t_j, j étant égal à m modulo M. En d'autres termes, la condition d'arrêt du tirage alphabet effectué au niveau du poste numéro 1 est que l'on ait atteint le tirage du $x_{m1}^{ième}$ élément, la condition d'arrêt du tirage alphabet effectué au niveau du poste numéro n est que l'on ait atteint le tirage du $x_{mn}^{ième}$ élément, et la condition d'arrêt du tirage alphabet effectué au niveau du $N^{ième}$ poste est que l'on ait atteint le tirage du $x_{mN}^{ième}$ élément. Les N suites recherchées sont formées des éléments s_{nj} ainsi définis.

L'orthogonalité des lois se trouve ainsi assurée sans qu'il soit besoin de se placer au niveau d'un service central à chaque instant de génération.

En effet pour chaque instant de génération t_j l'élément s_{nj} choisi pour être utilisé au niveau de l'entité numéro n est différent des éléments choisis pour être utilisés au niveau de toutes les autres entités car les éléments y_{ij} sont issus d'un tirage alphabet et de plus le rang x_{mn} de l'élément s_{nj} choisi parmi les éléments y_{ij} est lui-même issu d'un tirage alphabet.

On a supposé que les nombres ou éléments servant de base aux tirages étaient tous différents. Or dans la pratique les tirages se font au moyen d'un générateur pseudo-aléatoire, le caractère imprévisible des nombres ou éléments générés par ce générateur pseudo-aléatoire étant mis à profit pour simuler un tirage au sort. Il faut alors faire un traitement supplémentaire pour vérifier que le nombre ou l'élément tiré à chaque nouveau tirage est différent de tous ceux déjà tirés.

Le caractère aléatoire de chacune des lois est alors assuré par le fait que c'est un générateur pseudo-aléatoire qui génère les éléments des différentes suites.

Les générateurs pseudo-aléatoires situés dans les différentes entités sont conçus de manière à effectuer des tirages identiques lorsqu'ils sont commandés simultanément (générateurs synchrones) et lorsqu'ils disposent des mêmes éléments d'initialisation.

De plus, le risque de compromission du système conforme à l'invention est très faible puisque la connaissance de la loi relative à une entité donnée ne donne à l'ennemi que la connaissance des M nombres relatifs cette entité et qui seront à lire dans une mémoire. Elle ne donne qu'une information sur les lois des autres entités que l'on peut rendre extrêmement limitée puisque la probabilité d'en tirer une autre loi est sensiblement 1/M!

On se réfère maintenant au dessin montrant un schéma synoptique d'un dispositif pour la mise en oeuvre du procédé de génération selon l'invention.

Un tel dispositif est situé au niveau de chacune des entités (ou de chacun des postes dans l'application citée) et comporte un module d'initialisation 1, dont la sortie est reliée à l'entrée de commande d'un compteur 2, modulo M. Le compteur 2 a son entrée d'horloge reliée à la sortie d'une horloge 3. Ce dispositif comporte également une mémoire morte 4, dont les entrées d'adresse sont reliées aux sorties du compteur 2. Ce dispositif comporte également un générateur pseudo-aléatoire 5, muni d'entrées de commande reliées aux sorties du compteur 2 et un module de sélection d'élément 6 muni d'entrées de données reliées aux sorties du générateur pseudo-aléatoire 5 et d'entrées de commande reliées aux sorties de la mémoire morte 4. Les sorties du module de sélection d'élément 6 fournissent les éléments de la suite associée à l'entité considérée.

Ce dispositif fonctionne de la façon suivante.

Le module d'initialisation 1 fournit l'instant t_0 au compteur 2. Le compteur 2 incrémenté par le signal d'horloge fourni par l'horloge 3, de fréquence égale à la fréquence de génération des éléments de la suite, fournit à son tour les différents instants t_j, avec m = j modulo M.

Dans la mémoire morte 4 sont stockés les nombres x_{mn} correspondant au poste numéro n (avec n fixé et m variant de 1 à M). Ainsi,

lorsque le compteur 2 atteint la valeur m, on lit en sortie de la mémoire morte 4 le nombre x_{mn} correspondant.

Pour chaque valeur de m, c'est-à-dire aussi pour chaque valeur de j, le générateur pseudo-aléatoire 5 fournit des éléments y_{ij} (i étant variable de 1 à X). Le module de sélection 6, en relation avec la mémoire morte 4, sélectionne le $x_{mn}^{ième}$ élément fourni par le générateur pseudo-aléatoire pour la valeur de m considérée. Cet élément constitue l'élément s_{nj} recherché.

Ce processus se répète pour chaque instant de génération, c'est-à-dire pour chaque valeur de m.

La capacité mémoire nécessaire à la mémorisation des M éléments x_{mn} dépend évidemment des valeurs de M, N et X. Dans l'hypothèse X = M = N = 100, une mémoire de 1 kilobit suffit à cette fonction.

Les différents organes constituant le dispositif pour la mise en oeuvre du procédé de génération peuvent être réalisés suivant l'art connu, soit sous forme de circuits logique et/ou analogiques, soit sous forme de logiciel implanté sur un micro-ordinateur.

REVENDICATIONS

1. Procédé de génération de suites d'éléments suivant des lois aléatoires et orthogonales, ces éléments étant au nombre de Y et étant générés par N entités distinctes sous la forme de N suites infinies d'éléments s_{nj} (Y et N étant des nombres entiers, j un nombre entier variable de 1 à l'infini et n un nombre entier variable de 1 à N), caractérisé en ce qu'il comporte :

- une première étape consistant à effectuer M tirages alphabet successifs de N nombres entiers chacun, parmi un ensemble de X nombres entier tous différents (M et X étant des nombres entiers avec $X \geqslant N$), le $n^{ième}$ tirage à l'intérieur du $m^{ième}$ tirage alphabet (m étant un nombre entier variable de 1 à M) fournissant un nombre x_{mn},

- une deuxième étape consistant à affecter les nombres x_{mn} (avec n fixé) à la $n^{ième}$ entité en vue de la génération des éléments de la $n^{ième}$ suite,

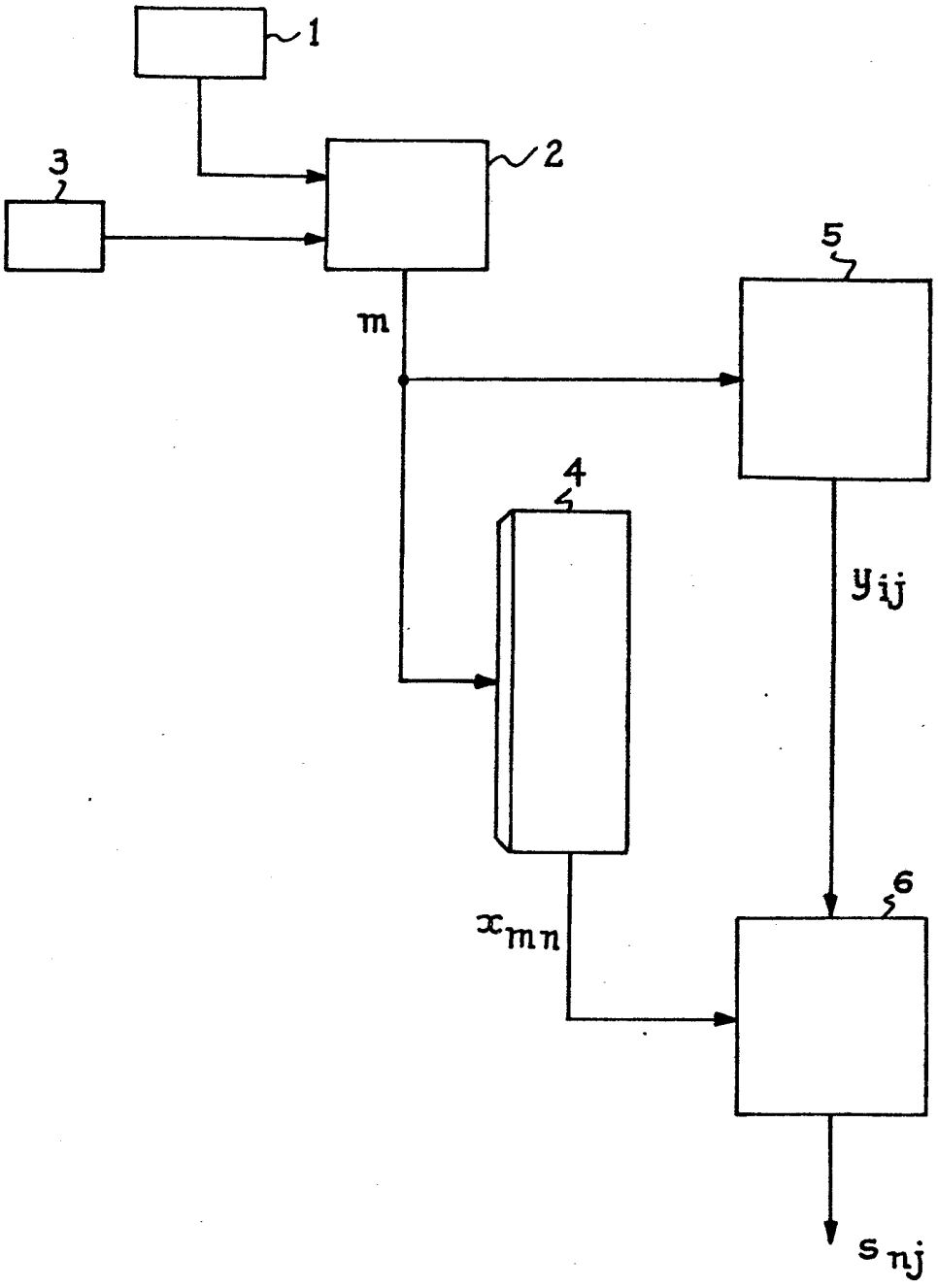
- une troisième étape consistant à générer le $j^{ième}$ élément s_{nj} de la $n^{ième}$ suite, sous la forme du $x_{mn}^{ième}$ élément obtenu au cours d'un tirage alphabet effectué parmi les Y éléments au niveau de la $n^{ième}$ entité, N tirages alphabet identiques étant effectués simultanément au niveau des N entités.

2. Dispositif pour la mise en oeuvre du procédé selon la revendication 1, caractérisé en ce que les entités comportent une mémoire morte (4), contenant les nombres x_{mn} obtenus à l'issue de la première étape (avec m variable de 1 à M), adressée par un compteur (2) modulo M lui-même incrémenté par un signal d'horloge fourni par une horloge (3) de fréquence égale à la fréquence de génération des éléments s_{nj}, un générateur pseudo-aléatoire (5) apte à effectuer un tirage alphabet parmi les Y éléments à chaque instant de génération d'un nouvel élément s_{nj}, et un module de sélection d'élément (6) apte à sélectionner le $x_{mn}^{ième}$ élément obtenu au cours de ce tirage alphabet, cet élément constituant l'élément s_{nj}.

3. Dispositif selon la revendication 2, caractérisé en ce que les N

générateurs pseudo-aléatoires localisés au niveau des N entités effectuent des tirages identiques.

4. Dispositif selon l'une des revendications 2 et 3, caractérisé en ce que les N générateurs pseudo-aléatoires localisés au niveau des N entités sont synchrones.


1
2
3
5
m
4
y_{ij}
x_{mn}
6
s_{nj}