RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 486 680**
(A n'utiliser que pour les commandes de reproduction).

A1

DEMANDE DE BREVET D'INVENTION

(21) **N° 80 15506**

(54) **Procédé et dispositif de permutation des éléments d'un ensemble.**

(51) Classification internationale (Int. Cl.³). **G 06 F 7/00; G 11 C 7/00.**

(22) Date de dépôt ..... 11 juillet 1980.

(33) (32) (31) Priorité revendiquée :

(41) Date de la mise à la disposition du public de la demande ..... B.O.P.I. — « Listes » n° 2 du 15-1-1982.

(71) Déposant : TELECOMMUNICATIONS RADIOELECTRIQUES & TELEPHONIQUES T.R.T., SA, résidant en France.

(72) Invention de : Pierre Louis Vincent Bréant.

(73) Titulaire : *Idem* (71)

(74) Mandataire : Cabinet Martinet,
62, rue des Mathurins, 75008 Paris.

PROCEDE ET DISPOSITIF DE PERMUTATION DES ELEMENTS D'UN ENSEMBLE

La présente invention concerne un procédé de permutation des N éléments ordonnés d'un ensemble selon lequel les éléments sont permutés selon un plan de permutation défini par un ordre prédéterminé de N éléments prédéterminés qui sont liés à la désignation des éléments de l'ensemble et qui sont préalablement mémorisés selon un ordre initial dans N cellules d'une mémoire . Elle a trait également à un dispositif mettant en oeuvre ce procédé.

Dans la suite, la nature et la signification des éléments de l'ensemble ne seront pas considérées. On n'admettra qu'une source d'éléments transmet chaque ensemble de sorte qu'il est composé de N éléments choisis parmi ceux d'un alphabet déterminé. Par exemple, lorsque l'ensemble est un message sous forme numérique ou analogique, chaque élément est un mot ayant un nombre prédéterminé de bits ou d'échantillons égal à 1 ou plus. Par "ensemble", on désigne indifféremment une suite de N éléments d'un ensemble donné, ou de N sous-ensembles d'un ensemble donné, chaque sous-ensemble jouant alors le rôle d'un élément. De ce qui précède, il apparaît que la mémoire stockant les éléments de l'ensemble en vue de leurs permutations sera de nature correspondante à celle des éléments de l'ensemble.

Les dispositifs connus destinés à la permutation d'éléments d'un ensemble peuvent être classés en deux catégories.

La première catégorie est relative à une suite de plans de permutation distribués pseudo-aléatoirement. Au fur et à mesure de l'entrée des ensembles dans le dispositif, chacun est soumis à des permutations selon un plan de permutation adressé. Il est alors nécessaire de mémoriser les plans de permutation dans une mémoire morte qui sont sélectionnés par adressage, tous les N éléments, par un générateur pseudo-aléatoire. Cette mémoire a une capacité d'autant plus grande que le nombre N d'éléments des ensembles est élevé, c'est-à-dire que la fonction factorielle N! est élevée.

Néanmoins, pour éviter la mise en œuvre d'une telle mémoire de coût très élevé, il est toujours possible de découper l'ensemble long en segments courts et d'appliquer aux éléments des segments un plan de permutation choisi de façon pseudo-aléatoire. Dans ce cas, l'ensemble sortant du dispositif est nettement moins désordonné et résulte d'un processus faiblement aléatoire, contrairement au but recherché.

Afin de résoudre le premier problème posé, on a proposé une seconde catégorie de dispositifs de permutation dans lesquels la permutation s'effectue selon un plan de permutation unique sur un nombre élevé d'éléments, mais est cependant répétée après N éléments consécutifs. Le plan de permutation est obtenu à partir d'une "clé" à partir de laquelle est calculé l'unique plan de permutation selon un algorithme plus ou moins complexe. Ces dispositifs servent généralement au chiffrement de messages radiophoniques télévisuels et, par nature, ne nécessitent pas un chiffrement très élaboré qui peut être reconnu par des spécialistes. En effet, la répétition du plan de permutation peut donner une telle possibilité, car dans ces derniers dispositifs, aucune sélection aléatoire ou pseudo-aléatoire d'une pluralité de plans de permutation n'a lieu.

La présente invention a pour but de fournir un procédé de permutation selon lequel les éléments de chaque ensemble sont permutés de manière aléatoire ou pseudo-aléatoire, mais cependant selon lequel, chaque permutation de deux éléments est définie et calculée au fur et à mesure de l'entrée de l'ensemble dans le dispositif, c'est-à-dire ne nécessite pas de mémoires d'une pluralité de plans de permutation. De ce fait, le procédé est pratiquement indépendant du nombre N d'éléments composant chaque ensemble, qui peut être très élevé. En outre, non seulement les plans de permutation sont distribués aléatoirement relativement aux ensembles, mais également les permutations internes à un plan sont choisies très aléatoirement, tout en conservant entre elles l'équiprobabilité.

A cette fin, le procédé de permutation, tel que défini dans l'entrée en matière, est caractérisé en ce que, pour chaque permutation de

rang n parmi N-1 permutations consécutives, les éléments prédéterminés contenus dans les cellules ayant les adresses $r_n + n-1$ et n-1 sont échangés, r_n étant un entier aléatoire ou pseudo-aléatoire compris entre 0 et N-n.

Afin de rendre encore plus aléatoire les permutations, l'entier r_n résulte de l'opération k_n modulo N-n+1, où k_n est un entier aléatoire ou pseudo-aléatoire compris entre 0 et un entier K supérieur ou égal à N. Les éléments prédéterminés liés à la désignation des éléments de l'ensemble et soumis aux permutations peuvent être, selon l'invention, soit les adresses de la mémoire d'ensemble, soit les éléments de l'ensemble, de préférence lorsque la mémorisation des adresses nécessite une capacité mémoire plus grande que celle pour la mémorisation de l'ensemble.

Le dispositif pour la mise en oeuvre du procédé par permutation d'adresses, comprend une mémoire d'ensemble à N éléments, des moyens comprenant un générateur d'entiers aléatoires ou pseudo-aléatoires pour produire les N adresses de la mémoire d'ensemble suivant l'ordre prédéterminé, des moyens pour écrire (ou lire) les éléments d'ensemble selon leur ordre naturel dans la mémoire d'ensemble et des moyens pour lire (ou écrire) les éléments d'ensemble dans la mémoire d'ensemble selon l'ordre prédéterminé des adresses, et est caractérisé en ce que les moyens de production d'adresses comprennent une mémoire des N adresses, des moyens pour produire les entiers r_n, des moyens pour calculer les entiers $r_n + n-1$ et n-1 pour chaque permutation de rang n, et des moyens pour adresser les cellules de la mémoire d'adresses ayant les adresses $r_n + n-1$ et n-1 afin d'écrire le contenu de l'une de ces cellules dans l'autre cellule et inversement.

Pour la mise en oeuvre du procédé par permutation directe sur les éléments d'ensemble, le dispositif ne contient donc pas de mémoires d'adresses, et les moyens d'adressage opèrent directement sur la mémoire d'ensemble en vue d'échanger les éléments de l'ensemble contenus dans les cellules ayant les adresses $r_n + n-1$ et n-1 pour chaque permutation de rang n.

D'autres avantages de l'invention apparaîtront plus clairement à la lecture de la description qui suit de plusieurs exemples de réalisation et des dessins annexés correspondants, dans lesquels :

- la Fig. 1 est un bloc - diagramme schématique du dispositif de permutation dans lequel est détaillée l'unité de commande en écriture et lecture de la mémoire d'ensemble ;

- la Fig. 2 est un bloc-diagramme détaillé du circuit d'élaboration de nombres aléatoires ou pseudo-aléatoires r_n ;

- la Fig. 3 est un bloc-diagramme détaillé du circuit de chargement de la mémoire du plan de permutation ;

- la Fig. 4 est un diagramme des signaux inhérents au chargement et à une permutation élémentaire d'adresses dans la mémoire du plan de permutation ; et

- la Fig. 5 est une autre variante du circuit d'élaboration de nombres aléatoires ou pseudo-aléatoires.

Selon une réalisation préférée, on considère dans la suite, en tant qu'ensemble, un message qui est transmis sous la forme d'un signal numérique. Ce message peut être partagé en un nombre entier N de mots m_0 à m_{N-1}, en tant qu'éléments d'ensemble, ayant chacun un nombre de bits prédéterminés qui peut être différent de celui des mots proprement informatifs, tel que des octets pour un message en code MIC. Le message reçu dans la mémoire d'ensemble, dite mémoire de message, peut par exemple résulter d'échantillonnage, codage et multiplexage de plusieurs messages. Le traitement du message en amont de la mémoire de message n'appartient pas au cadre de l'invention.

Le dispositif de permutation comprend une base de temps dont la structure n'est pas détaillée et dont les différents signaux de commande des organes du dispositif ne seront pas indiqués, à l'exception de ceux utiles à la compréhension du procédé de permutation. Cette base de temps comprend, en outre, de manière connue, des moyens de synchronisation afin de synchroniser tous les signaux d'horloge sur la fréquence des mots du message et de retransmettre, si nécessaire, un signal de synchronisation en vue de synchroniser le dispositif de reconstitution du message initial à partir du message résultant

de la permutation. La base de temps 1 du dispositif de permutation montré à la Fig. 1, reçoit par conséquent le message initial présenté à l'entrée 2 du dispositif et produit, en outre, un signal d'horloge H_m à la fréquence des mots m, un signal d'horloge rapide H_r à une fréquence au moins supérieure à K fois celle du signal H_m, et trois ensembles de signaux P_1, P_2 et P_3 propres au déclenchement des trois phases principales composant le processus d'obtention du message résultant.

En se référant à la Fig. 1, le dispositif comprend également une première mémoire vive 3 qui mémorise le message initial reçu à l'entrée 2 pour retransmettre le message résultant à la sortie 4 du dispositif, un circuit d'élaboration de nombres aléatoires ou pseudo-aléatoires 5, une seconde mémoire vive 6 qui mémorise les éléments du plan de permutation, un circuit de chargement 7 qui calcule les paires d'adresses de la mémoire 6 en fonction des nombres aléatoires r_n transmis par le circuit 5, et une unité de commande 8 qui commande l'écriture des mots du message selon leur ordre initial et la lecture des mots selon le plan de permutation dans la mémoire 6. Selon la réalisation illustrée à la Fig. 1, la permutation est effectuée sur les adresses de la mémoire de message 3, c'est-à-dire la mémoire 6 contient les N adresses des cellules de la mémoire 3 selon un ordre différent de celui de l'ordre natural 0 à N-1, pour lequel les mots du message initial sont écrits.

L'algorithme du processus d'obtention du signal résultant sortant comprend, comme déjà dit, trois phases P_1, P_2 et P_3.

La première phase dite d'initialisation P_1 concerne la mise en mémoire du message initial dans la mémoire 3 et le chargement de la mémoire 6 par les adresses 0 à N-1, selon leur ordre initial. Pour ce faire, le circuit de chargement 7 montré à la Fig. 3 comprend un compteur 70 et l'unité de commande 8 montrée à la Fig. 1 comprend un compteur-décompteur 80.

Les signaux d'initialisation P_1 délivrés par la base de temps 1, en réponse au début du message, mettent à zéro (RZ) et ordonnent le comptage des impulsions d'horloge H_m par le compteur 70 et le

compteur-décompteur 80. Les signaux P_1 sont également transmis aux entrées de commande en écriture 3e et 6e des mémoires 5, 6 qui passent en phase d'écriture. Le bus de sortie 70S du compteur 70 est relié au bus d'entrée informatif 6E et au bus d'adressage 6a de la mémoire 6 à travers deux jeux de portes ET 71E et 71a qui sont ouvertes pendant la phase d'initialisation et d'écriture P_1. Le bus de sortie 80 S du compteur-décompteur 80 est relié au bus d'adressage 3 a de la mémoire 3 à travers un jeu de portes ET 30e ouvertes pendant la phase P_1. Les nombres 0 à N-1 sont ainsi respectivement mémorisés dans les cellules d'adresses 0 à N-1 dans la mémoire 6, tandis que les mots m_0 à m_{N-1} sont respectivement mémorisés dans les cellules d'adresses 0 à N-1 de la mémoire de message 3.

Un détecteur de N-1 et de zéro 81 est relié au bus de sortie 80S du compteur-décompteur 80 et transmet un signal de détection de N-1 vers la base de temps 1 qui signifie la fin de la phase d'initialisation et d'écriture P_1. La base de temps stoppe l'émission des signaux d'horloge H_m vers le compteur 70 et le compteur-décompteur 80 et déclenche la seconde phase P_2.

Cette seconde phase P_2 est relative à l'élaboration du plan de permutation, c'est-à-dire des adresses d'écriture de la mémoire de message 3 qui sont à mémoriser dans la mémoire 6, préalablement à la phase proprement dite d'obtention du message sortant P_3. L'élaboration du plan de permutation est réalisée au moyen des circuits 5 et 7 qui sont représentés sur les Figs. 2 et 3, selon une réalisation préférée.

Le circuit d'élaboration de nombres aléatoires ou pseudo-aléatoires 5, montré à la Fig. 2, comprend un générateur de nombres aléatoires ou pseudo-aléatoires 50, un décompteur 51 à partir de N+1, des premier et second compteurs à compte maximal ou module variable 52 et 53, ainsi que d'autres éléments logiques 54 à 58. Le générateur 50 fournit des nombres entiers k compris entre 0 et K. L'entier K est très grand devant N afin de rendre plus aléatoires les nombres entiers r_n délivrés par le circuit 5. Les compteurs 52, 53 se

remettent automatiquement à zéro dès que leurs comptes ont atteint respectivement leurs modules variables k_n, N+1-n.

Au début de la seconde phase, les signaux P_2 émis par la base de temps 1 commandent la mise à zéro des compteurs 52 et 53 et la mise à N+1 du décompteur 51. La base de temps déclenche l'émission du signal d'horloge H_m vers les entrées d'horloge 50 H, 51 H du générateur et du décompteur 50, 51 et l'émission du signal d'horloge rapide H_r vers les entrées d'horloge 52 H, 53 H des compteurs 52, 53 à travers une porte ET 54 initialement ouverte.

En réponse à chaque $n^{ième}$ impulsion H_m, le bus de sortie 50S du générateur fournit à l'entrée de compte maximal 52 CM du premier compteur 52 un entier k_n compris entre 0 et K. Le bus de sortie 51S du décompteur 51 dont le compte a été décrémenté de n, fournit simultanément à l'entrée de compte maximal 53 CM du second compteur 53 l'entier N+1-n. Par conséquent, pendant la $n^{ième}$ opération, en réponse à la $n^{ième}$ impulsion H_m, le compteur 52 compte k_n impulsions H_r et le compteur 53 compte $k_n = r_n$ ou une ou plusieurs fois (N-n-1) plus r_n impulsions H_r selon que le nombre k_n est inférieur ou supérieur à N+1-n. Le compte r_n du compteur 53 est donc le résidu de l'opération $k_n = r_n$ modulo (N-n-1) lorsque le compte du compteur 52 se remet automatiquement à zéro. Ceci est détecté par un détecteur de zéro 55, relié au bus de sortie 52S du compteur 52, dont la sortie émet un signal pour fermer momentanément la porte ET 54 et pour ouvrir momentanément un jeu de portes ET 56 permettant le transfert du résidu r_n du bus de sortie 53S du second compteur 53 vers un bus d'entrée 72 du circuit de chargement 7. Le signal de sortie du détecteur de zéro 55 remet également à zéro (RZ) le second compteur 53 en vue de préparer celui-ci pour la prochaine opération de rang n+1. Simultanément le nombre N+1-n est également transmis à un second bus d'entrée 73 du circuit de chargement 7 à travers un jeu de portes ET 57 qui sont ouvertes momentanément.

Le circuit 5 comprend également un détecteur du nombre 2, 58, relié au bus de sortie des portes ET 57 qui émet un signal vers la base de temps afin de lui signifier la fin de la phase de calcul du plan de permutation P_2, qui correspond à la $(n-1)^{ième}$ impulsion H_m reçue

par le décompteur 51.

Chaque résidu r_n délivré par le circuit 5 permet de calculer les deux adresses de la mémoire 6 dont les contenus sont à permuter à la $n^{ième}$ opération. Cette permutation résulte du procédé suivant.

Comme on l'a vu, la phase d'initialisation P_1 affecte un numéro d'ordre A_n ou adresse d'écriture dans la mémoire 3 à chaque mot m_n du message initial. Ce numéro d'ordre est compris entre 0 et N-1, limites incluses, et est égal dans le cas présent à n-1. Selon d'autres variantes, à la place du compteur 70 du circuit de chargement 7, une mémoire morte peut être lue pendant la phase d'initialisation afin de transférer un plan de permutation A_0 à A_{N-1} dans la mémoire 6.

L'algorithme du processus de permutation mis en oeuvre par le circuit 7 consiste en ce qu'à la $n^{ième}$ opération du circuit 5, le contenu de la cellule de la mémoire 6 ayant l'adresse $r_n + n-1$ est échangé avec le contenu de la cellule ayant l'adresse n-1. Comme le nombre r_n est issu du résidu d'une opération modulo (N-n+1), c'est-à-dire est compris entre 0 et N-n, les contenus des cellules de la mémoire 6 ayant les adresses 0 à n-1 sont fixés définitivement après la $n^{ième}$ opération parmi N-1 opérations. A la dernière opération de rang N-1, le circuit 5 fournit un entier r_{N-1} qui est égal à 0 ou 1. Le contenu de la cellule ayant l'adresse $r_{N-1} + N-2$, c'est-à-dire ayant l'adresse N-2 ou N-1, est échangé avec celui de la cellule d'adresse N-2. Ainsi, à la fin de la phase P_2, non seulement le contenu de la cellule d'adresse N-2, mais également celui de la cellule d'adresse N-1 ont pris leur place définitive dans la mémoire 6.

On notera que cet algorithme donne bien aux plans de permutation la même probabilité puisque, avant la $n^{ième}$ opération, les n-1 premières cellules de la mémoire 6, d'adresses 0 à n-2, ont reçu leurs contenus définitifs et puisque l'adresse à placer dans la cellule d'adresse n-1 est tirée au sort parmi les adresses contenues dans les cellules ayant des adresses comprises entre n-1 et N-1, limites incluses.

Ce calcul d'adresses des cellules de la mémoire 6 et la permutation des contenus de celles-ci sont effectués par le circuit de

chargement 7 montré à la Fig. 3.

Pour le calcul des adresses, le circuit 7 comprend un circuit de complémentation à N, 74 et un circuit d'addition 75. Le bus d'entrée du circuit 74 et l'un des deux bus d'entrée du circuit 75 sont les bus déjà cités 73 et 72 qui transmettent les entiers N-n+1 et r_n, pour chaque $n^{ième}$ opération. Le circuit 74 effectue l'opération N - (N-n+1) dont le résultat n-1 est transmis vers l'autre bus d'entrée du circuit 75 et vers un jeu de portes ET 760. Le résultat de l'addition r_n + n-1 effectuée par le circuit d'addition 75 est transmis vers un autre jeu de portes ET 761.

Le circuit de chargement 7 comporte également une mémoire auxiliaire 77 à deux cellules qui est destinée à échanger les contenus des cellules de la mémoire 6 ayant pour adresses r_n + n-1 et n-1, et un compteur auxiliaire 78 qui commande les adressage, lecture et écriture des mémoires 6 et 77 pendant la phase P_2. On notera qu'à chaque opération, le calcul de r_n par le circuit 5 et la permutation de deux adresses par le circuit 7 sont consécutifs.

Au début de la seconde phase P_2, des signaux P_2 de la base de temps 1 remettent à zéro le compteur 78. Pendant la phase P_2, ils maintiennent ouverts des jeux de portes ET 762, 763 qui relient respectivement le bus de sortie 6S de la mémoire 6 au bus d'entrée 77E de la mémoire 77 et le bus de sortie 77S de la mémoire 77 au bus d'entrée 6E de la mémoire 6. Le compteur 78 est rythmé par les impulsions d'horloge rapides H_r qu'il reçoit sur son entrée d'horloge 78H. Par ailleurs, à la fin de chaque opération, il est remis à zéro sous la commande du signal émis par le détecteur de zéro 55 du circuit 5 (Fig. 2).

Pour chaque $n^{ième}$ opération, le compteur 78 commande successivement les sous-opérations suivantes par production d'un signal de permutation, d'un signal de commande de lecture et d'écriture et d'un signal d'adressage sur ses sorties respectives 77P, 77le et 77a. Les formes d'onde de ces signaux sont représentées respectivement à la Fig. 4 pour une opération de permutation.

Le signal en sortie 78 P commande directement et à travers un

inverseur 764, les ouvertures successives des portes ET 761 et 760 qui transfèrent l'adresse $r_n + n-1$ puis l'adresse n-1 au bus d'adressage 6a de la mémoire 6. En synchronisme à l'adressage précédent, les cellules 0 et 1 de la mémoire axiliaire 77 sont adressées par le signal en sortie 78a. Simultanément le signal en sortie 78 le commande, à travers un inverseur 765, la lecture de la mémoire 6 et l'écriture de la mémoire 77 afin que les contenus des cellules de la mémoire 6 ayant les adresses $r_n + n-1$ et n-1 soient transférés dans les cellules 0 et 1 de la mémoire auxiliaire 77.

Puis est réalisée la permutation proprement dite, par inversion de l'ordre d'adressage de deux cellules de la mémoire auxiliaire 77 (ou des cellules précitées de la mémoire 6 ; diagramme de droite de la Fig. 4). L'entrée d'adressage 6a reçoit toujours successivement les adresses $r_n + n-1$ et n-1, cependant que l'entrée d'adressage 77a reçoit successivement les adresses 1 et 0. Le signal en sortie 78 le du compteur 78 est inversé et est délivré directement aux entrées 6e, 771 des mémoires 6 et 77 qui passent respectivement en phase d'écriture et en phase de lecture. Le contenu de la cellule d'adresse 1 de la mémoire auxiliaire 77 est rangé dans celle d'adresse $r_n + n-1$ de la mémoire 6 et le contenu de la cellule d'adresse 0 de la mémoire 77 est rangé dans celle d'adresse n-1 de la mémoire 6.

A la fin de la $(n-1)^{ième}$ opération, le plan de permutation est complètement mémorisé dans la mémoire 6. La phase P_2 est terminée, ce qui est signalé à la base de temps 1 par le signal émis par le détecteur du nombre 2, 58 (Fig. 2). La transmission des signaux d'horloge H_m, H_r vers les éléments correspondants 50, 51, 54, 78 des circuits 5 et 7 (Figs. 2 et 3) est arrêtée. Le jeu de portes dites d'écriture 30e a été fermé à la fin de la première phase P_1 et les jeux des portes 762, 763 du transfert d'adresses entre les mémoires 6 et 77 (Fig. 3) ont été fermés à la fin de la seconde phase P_2.

Suite à la seconde phase P_2, la dernière phase P_3 a trait à la lecture des mots de message m_0 à m_{N-1} mémorisés dans la mémoire 3, selon l'ordre d'adressage du plan de permutation mémorisé dans

la mémoire 6.

En se reportant à la Fig. 1, des signaux P_3 ouvrent un jeu de porte ET dites de lecture 301 qui sont propres aux transferts successifs des adresses contenues dans la mémoire du plan de permutation 6, du bus de sortie 6S de la mémoire 6 vers le bus d'adressage 3a de la mémoire 3. La troisième phase P_3 est accomplie sous la commande d'un compteur 82 qui est inclus dans l'unité de commande 8 et qui est remis à zéro à la fin de la phase P_3 d'un message précédent -comme on le verra dans la suite-. Au début de la troisième phase, des signaux P_3 mettent en état de décomptage (D) le compteur-décompteur 80 dont le compte a été bloqué à N-1 à la fin de la première phase précédente, et N impulsions d'horloge H_m sont délivrées par la base de temps 1 aux entrées d'horloge du compteur 82 et du compteur-décompteur 80. Les mémoires 3 et 6 sont mises respectivement en phase d'écriture et de lecture.

En réponse à chaque $n^{ième}$ impulsion d'horloge H_m, le compteur 82 est incrémenté d'une unité et fournit par son bus de sortie 82S l'entier n-1 au bus d'adressage 6a de la mémoire 6 en phase de lecture. Les cellules de la mémoire 6 sont donc lues selon leur ordre naturel d'adresse et leurs contenus correspondant aux adresses de lecture de la mémoire 6 selon le plan de permutation élaboré et mémorisé, sont transférés successivement vers l'entrée d'adressage 3a. Les mots sortant de la sortie 6S de la mémoire 6 sont ainsi les mots initiaux écrits mais lus selon l'ordre d'adressage du plan de permutation.

La fin de la phase P_3 est signalée à la base de temps par le détecteur 81 qui détecte zéro sur le bus de sortie 80S du compteur-décompteur 80 et qui commande la remise à zéro (RZ) du compteur 82.

Le dispositif dit de reconstitution, effectuant l'opération inverse de celle décrite précédemment, à savoir l'obtention du message initial à partir du message résultant de la permutation, n'a pas été représenté, car il contient pratiquement des éléments analogues à celui du dispositif prédécrit et illustré, selon la même organisation, à l'exception que les adressages de la mémoire de message sont inversés.

Dans ce dispositif de reconstitution, les mots du message résultant sont écrits et rangés dans la mémoire de message aux adresses indiquées par la mémoire de plan de permutation tandis qu'ils sont lus selon l'ordre naturel des adresses 0 à N-1 sous la commande d'un compteur, tel que 82.

En effet, le plan de permutation obtenu dans la mémoire 6 est commodément utilisable à la réception qu'aussi bien à l'émission. Le dispositif de reconstitution est synchronisé avec le dispositif de permutation, comme déjà dit par des moyens connus, et les plans de permutation initiaux mémorisés dans les mémoires, telles que 6, des deux dispositifs par des moyens, tels que le compteur 70 ou une mémoire morte, sont identiques. Dans le dispositif de permutation, le message ayant été préalablement mémorisé selon l'ordre naturel des mots, le mot m_n figurant à la cellule d'adresse n de la mémoire 3, il suffit de lire la mémoire du plan de permutation 6 dans l'ordre naturel des adresses des cellules de cette dernière mémoire. Le contenu de la cellule d'adresse n de la mémoire 6 donne l'adresse A_n du mot à émettre dans la mémoire de message 3. Corrélativement, dans le dispositif de reconstitution, au fur et à mesure de la réception des mots du message résultant, le $n+1^{ième}$ mot reçu peut être écrit dans la cellule d'adresse A_n de la mémoire de message, adresse qui sera lue à l'adresse n de la mémoire du plan de permutation.

Selon une autre réalisation, la permutation est effectuée directement sur les mots du message reçu initial (ou résultant). Cette réalisation est avantageuse dans le cas où le message est relativement long, c'est-à-dire comporte un nombre élevé de mots. Dans ce cas, le nombre de digits binaires des numéros d'ordre ou adresse des mots est notablement plus élevé que celui des mots eux-mêmes qui peuvent se réduire à un seul bit. La mémoire de plan de permutation selon la réalisation précédente aurait alors une capacité très importante.

Selon cette seconde réalisation, la mémoire 6 est donc supprimée. Le dispositif de chargement 7 (Fig. 3) opère directement sur la mémoire de message 3 pendant la phase P_2 et le compteur 82 lit

la mémoire de message 3, selon l'ordre naturel des adresses pendant la phase P_3. Dans la Fig. 3, il suffit de substituer à la mémoire 6, supprimée, la mémoire de message 3. La mémoire auxiliaire 77 sert alors à la permutation de chaque paire de mots du message qui sont rangés initialement aux adresses indiquées en sortie des circuits de complémentation et d'addition 74, 75. Le processus de permutation de mots du message se déroule de sorte que, après mise en mémoire des mots du message initial selon l'ordre naturel des adresses de la mémoire 3, le contenu de la cellule d'adresse $r_n + n-1$ est échangé avec le contenu de la cellule d'adresse n-1 à la $n^{ième}$ opération de la phase P_2. Puis les cellules de la mémoire 3 sont adressées, selon leur ordre initial, en lecture par le compteur 82 au cours de la dernière phase P_3.

Dans le dispositif de reconstitution selon cette réalisation, il est nécéssaire d'introduire une mémoire d'adresses auxiliaire qui permette de retrouver le plan de permutation inverse. Les adresses $r_n + n-1$ calculées sont rangées dans les cellules d'adresse n-1 de cette mémoire d'adresses. Le message résultant est alors mis en mémoire dans la mémoire de message selon l'ordre de réception des mots, par adresses décroissantes à partir de 0.

Puis les informations contenues dans la mémoire d'adresses sont lues une par une selon l'ordre décroissant des adresses de la mémoire d'adresses. Après lecture du contenu $r_n + n-1$ de la cellule ayant l'adresse n-1 de la mémoire d'adresses, le contenu de la cellule ayant l'adresse $r_n + n-1$ de la mémoire de message est échangé avec celui de la cellule ayant l'adresse n-1, au moyen d'une mémoire auxiliaire telle que 77. Puis les mots ainsi échangés sont lus dans la mémoire de message par adressage de 0 à N-1 afin de reconstituer le message initial.

On notera que l'organisation du dispositif de permutation (ou de reconstitution) est réalisée autour de circuits logiques dont de nombreuses variantes sont concevables par l'homme de métier pour obtenir le même résultat. Ainsi, par exemple, les compteurs 52 et 53 du circuit d'élaboration de nombres aléatoires (ou pseudo-aléatoires) peuvent être des compteurs ayant des modules fixes 52' et 53' qui sont respectivement supérieurs ou égaux à K et N+1.

Cette variante est montrée à la Fig. 5 dans laquelle, comparativement à la Fig. 2, les compteurs 52 et 53 sont remplacés par un compteur 52' et un comparateur 520 et par un compteur 53' et un comparateur 530. Comme pour la Fig. 2, les compteurs 52' et 53' reçoivent les impulsions d'horloge rapides H_r provenant de la sortie de la porte ET 54. Cependant, le bus de sortie 52'S du compteur est relié à l'un des bus d'entrée du comparateur 520 qui compare le compte du compteur 53' à l'entier k_n reçu sur son autre bus d'entrée. Ce comparateur 520 joue le rôle du détecteur de zéro 55 de la Fig. 2. Dès que le compteur du compteur 52' a atteint k_n, la sortie du comparateur 520 bloque la porte ET 54, ouvre la porte ET 56 et remet à zéro les compteurs 52' et 53' (ou 53).

Le bus de sortie 53'S du compteur 53 est relié au jeu de portes ET 56 ainsi qu'à l'un des bus d'entrée du comparateur 530 dont l'autre bus d'entrée reçoit l'entier N+1-n provenant du décompteur 51. Chaque fois que le compte du compteur 53 atteint l'entier N+1-n, il est remis à zéro par le comparateur 50.

Ainsi, le circuit 5 peut comporter deux compteurs à module fixe 52, 53 ou à module variable 52', 53' ou bien un compteur à module fixe 52' ou 53' et un compteur à module variable 53 ou 52.

Par ailleurs, la présente invention se rapporte également à la permutation de sous-messages dits segments consécutifs qui sont d'une durée égale et qui composent un message traité en continu. Dans ce cas, chacun des dispositifs de permutation et de reconstitution comporte deux mémoires de segment en parallèle. L'une de ces mémoires est en phase de lecture pendant que l'autre est en phase d'écriture. Chaque mémoire de segment est alors composée de deux sous-mémoires identiques dont les contenus sont transférés rapidement en parallèle après la phase P_1 ou P_2, la permutation des adresses ou des mots s'effectuant relativement à l'une de ces sous-mémoires. Chaque segment est assigné à un plan de permutation à priori différent de celui des autres segments.

Cependant on notera que, selon la première réalisation, lorsque le message est traité d'un seul bloc, l'élaboration du plan de permutation peut

être préalable à la réception du message initial ou résultant, de sorte que l'écriture dans la mémoire de message succède immédiatement à la lecture.

Comme déjà dit, le procédé de l'invention s'applique directement à toute sorte d'ensembles d'éléments, tels qu'également des messages analogiques. Dans ce dernier cas, chacune des cellules de la mémoire de message mémorise une portion du signal analogique ou suite d'échantillons analogiques et est composé par un ou plusieurs registres à décalage analogiques en série du genre à circuits intégrés à transfert de charge. Les étages des registres analogiques peuvent être du type à éléments en chapelets ou à chaîne à sauts, connus sous les sigles américains CTD ("Charge Transfer Device") et BBD ("Bucket Brigade Device").

Enfin, le générateur de nombres aléatoires ou pseudo-aléatoires 50 n'a pas été décrit en détail, car il est d'un genre connu. Il peut être constitué simplement par un générateur de séquences maximales, dont diverses structures sont par exemple présentées dans l'ouvrage de W. W. Peterson, intitulé "Error Correcting Code", Wiley and Son, 1972, Chapitre 7. L'inconvénient de ce type de générateur, à savoir une reconstitution relativement aisé de ses séquences, est sans objet pour l'invention, car le processus de calcul des résidus aléatoires r_n est très fortement non linéaire.

On peut également utiliser, comme générateur 50, un générateur "non linéaire" composé de registres à décalage dont les étages sont bouclés par des portes OU Exclusif et des portes ET.

Revendications

1 - Procédé de permutation des N éléments ordonnés d'un ensemble selon lequel les éléments sont permutés selon un plan de permutation défini par un ordre prédéterminé de N éléments prédéterminés qui sont liés à la désignation des éléments de l'ensemble et qui sont préalablement mémorisés selon un ordre initial dans N cellules d'une mémoire (6 ; 3), caractérisé en ce que, pour chaque permutation de rang n parmi N-1 permutations consécutives, les éléments prédéterminés contenus dans les cellules ayant les adresses $r_n + n-1$ et n-1 sont échangés, r_n étant un entier aléatoire ou pseudo-aléatoire compris entre 0 et N-n.

2 - Procédé conforme à la revendication 1, caractérisé en ce que l'entier r_n résulte de l'opération k_n modulo N-n+1, où k_n est un entier aléatoire ou pseudo-aléatoire compris entre 0 et un entier K supérieur ou égal à N.

3 - Procédé conforme à la revendication 1 ou 2, caractérisé en ce que les éléments prédéterminés mémorisés sont des adresses d'une mémoire des éléments de l'ensemble (3) rangées initialement selon leur ordre naturel ou selon un plan de permutation donné.

4 - Procédé conforme à la revendication 1 ou 2, caractérisé en ce que les éléments prédéterminés mémorisés sont les éléments de l'ensemble rangés initialement selon leur ordre naturel d'arrivée dans ladite mémoire (3).

5 - Dispositif pour la mise en œuvre du procédé conforme à l'une des revendications 1 à 3 comprenant une mémoire d'ensemble à N éléments (3), des moyens (5, 6, 7) comprenant un générateur d'entiers aléatoires ou pseudo-aléatoires (50) pour produire les N adresses de la mémoire d'ensemble suivant l'ordre prédéterminé, des moyens (80) pour écrire (ou lire) les éléments de l'ensemble selon leur ordre naturel dans la mémoire d'ensemble (3) et des moyens (82) pour lire (ou écrire) les éléments de l'ensemble dans la mémoire d'ensemble (3) selon l'ordre prédéterminé des adresses, caractérisé en ce que les moyens de production d'adresses comprennent une mémoire des N adresses (6), des moyens (5) pour produire les entiers r_n, des moyens (74, 75) pour calculer les entiers $r_n + n-1$ et n-1 pour chaque per-

mutation de rang n, et des moyens (77, 78) pour adresser les cellules de la mémoire d'adresses (6) ayant les adresses $r_n + n-1$ et $n-1$ afin d'écrire le contenu de l'une de ces cellules dans l'autre cellule et inversement.

6 - Dispositif conforme à la revendication 5, caractérisé en ce que les moyens de production des entiers r_n (5) comprennent, outre le générateur d'entiers aléatoires ou pseudo-aléatoires k_n (50), des moyens (51, 53) pour effectuer l'opération $k_n = r_n$ modulo $(N+n-1)$.

7 - Dispositif conforme à la revendication 6, caractérisé en ce que les moyens pour effectuer l'opération modulo comprennent des moyens (51) de comptage d'impulsions à une fréquence prédéterminée (H_m) pour produire l'entier $N+1-n$ en synchronisme avec l'entier k_n produit par le générateur (50), des premiers moyens (52) pour compter k_n impulsions rapides (H_r) ayant une fréquence au moins égale à N fois la fréquence prédéterminée des permutations (H_m), des seconds moyens (53) pour compter les impulsions rapides (H_r) par tranches de $N-n+1$ et des moyens de détection (55 ; 520) reliés aux premiers moyens de comptage (52) pour bloquer le compte des seconds moyens de comptage (53) à r_n en réponse à un compte des seconds moyens de comptage égal à k_n.

8 - Dispositif conforme à la revendication 7, caractérisé en ce qu'au moins les premiers et/ou seconds moyens de comptage (52, 53) comprennent un compteur à module variable k_n, resp. $N-n+1$.

9 - Dispositif conforme à la revendication 7, caractérisé en ce qu'au moins les premiers et/ou seconds moyens de comptage (52', 53') comprennent un compteur à module fixe au moins supérieur à tous les entiers k_n, resp. à l'entier $N+1$, et des moyens de comparaison (520 ; 530) des comptes respectifs des compteurs à k_n et $N+1-n$ afin de bloquer et/ou de remettre à zéro ces compteurs lorsqu'ils ont atteint ces derniers entiers.

10- Dispositif conforme à l'une des revendications 6 à 9, caractérisé en ce que les moyens d'adressage comprennent une mémoire auxiliaire ayant au moins des première et seconde cellules (77), des

moyens (761, 760, 78) pour adresser, selon un ordre prédéterminé en lecture, les cellules d'adresses $r_n + n-1$ et $n-1$ de la mémoire d'adresses (6) et en écriture les première et seconde cellules de la mémoire auxiliaire (77) afin de transférer les contenus des cellules $r_n + n-1$ et $n-1$ dans les première et seconde cellules, des moyens (78) pour inverser l'ordre d'adressage des cellules $r_n + n-1$ et $n-1$ ou des première et seconde cellules par rapport au précédent et des moyens (78, 760, 761) pour adresser en écriture, selon l'ordre précédent ou inverse, les cellules d'adresses $r_n + n-1$ et $n-1$ de la mémoire d'adresses (6) en lecture et, selon l'ordre inverse ou précédent, les première et seconde cellules de la mémoire auxiliaire (77) afin d'obtenir l'échange des contenus des cellules d'adresses $r_n + n-1$ et $n-1$.

11 - Dispositif conforme à l'une des revendications 5 à 10, caractérisé en ce qu'il comprend des moyens (70) pour écrire, préalablement aux permutations de chaque ensemble, en tant qu'éléments prédéterminés, les N adresses dans la mémoire d'adresses (6) selon ledit ordre initial.

12 - Dispositif pour la mise en œuvre du procédé conforme à l'une des revendications 1, 2 et 4, caractérisé en ce qu'il est analogue à celui des revendications 5 à 10, à l'exception qu'il ne contient pas de mémoire d'adresses (6) et que les moyens d'adressage (77, 78) opèrent directement sur la mémoire d'ensemble (3) en vue d'échanger les éléments de l'ensemble contenus dans les cellules ayant les adresses $r_n + n-1$ et $n-1$.

FIG.1

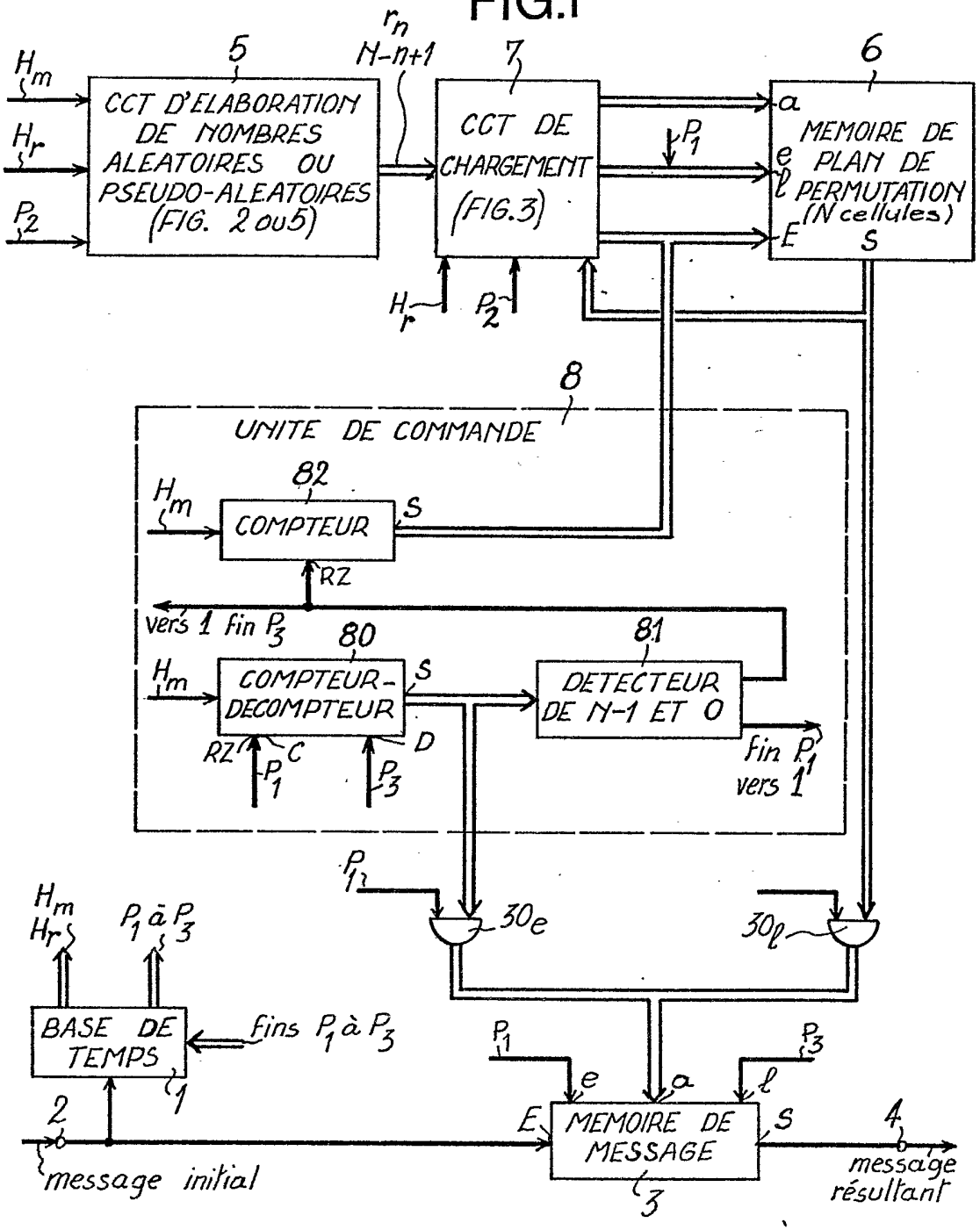

H_m
H_r
P_2
5
CCT D'ELABORATION DE NOMBRES ALEATOIRES OU PSEUDO-ALEATOIRES (FIG. 2 ou 5)
r_n
N-n+1
7
CCT DE CHARGEMENT (FIG.3)
P_1
6
a
e
l
MEMOIRE DE PLAN DE PERMUTATION (N cellules)
E
S
8
UNITE DE COMMANDE
82
COMPTEUR
RZ
vers 1 fin P_3
80
COMPTEUR-DECOMPTEUR
C
D
81
DETECTEUR DE N-1 ET 0
fin P_1 vers 1
30e
30l
H_m H_r
P_1 à P_3
BASE DE TEMPS
fins P_1 à P_3
1
2
message initial
E
MEMOIRE DE MESSAGE
3
S
4
message résultant

FIG.2

CCT D'ELABORATION DE NOMBRES ALEATOIRES OU PSEUDO-ALEATOIRES

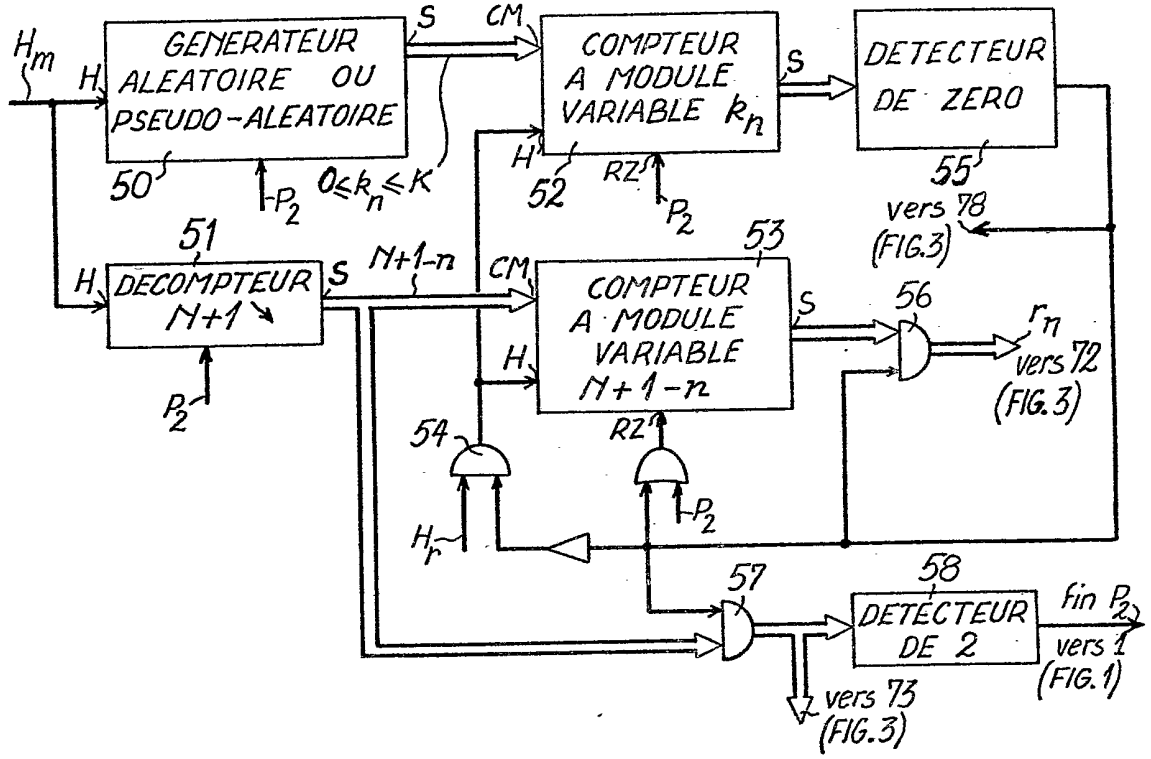


FIG.5

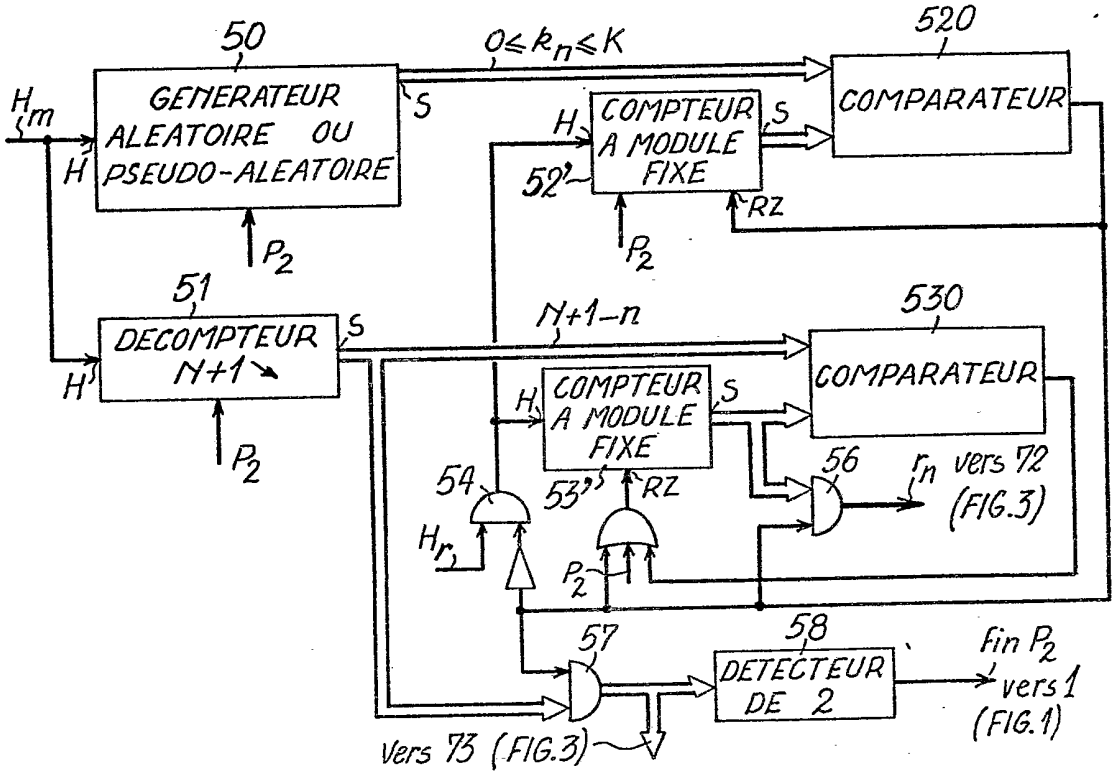


FIG.3

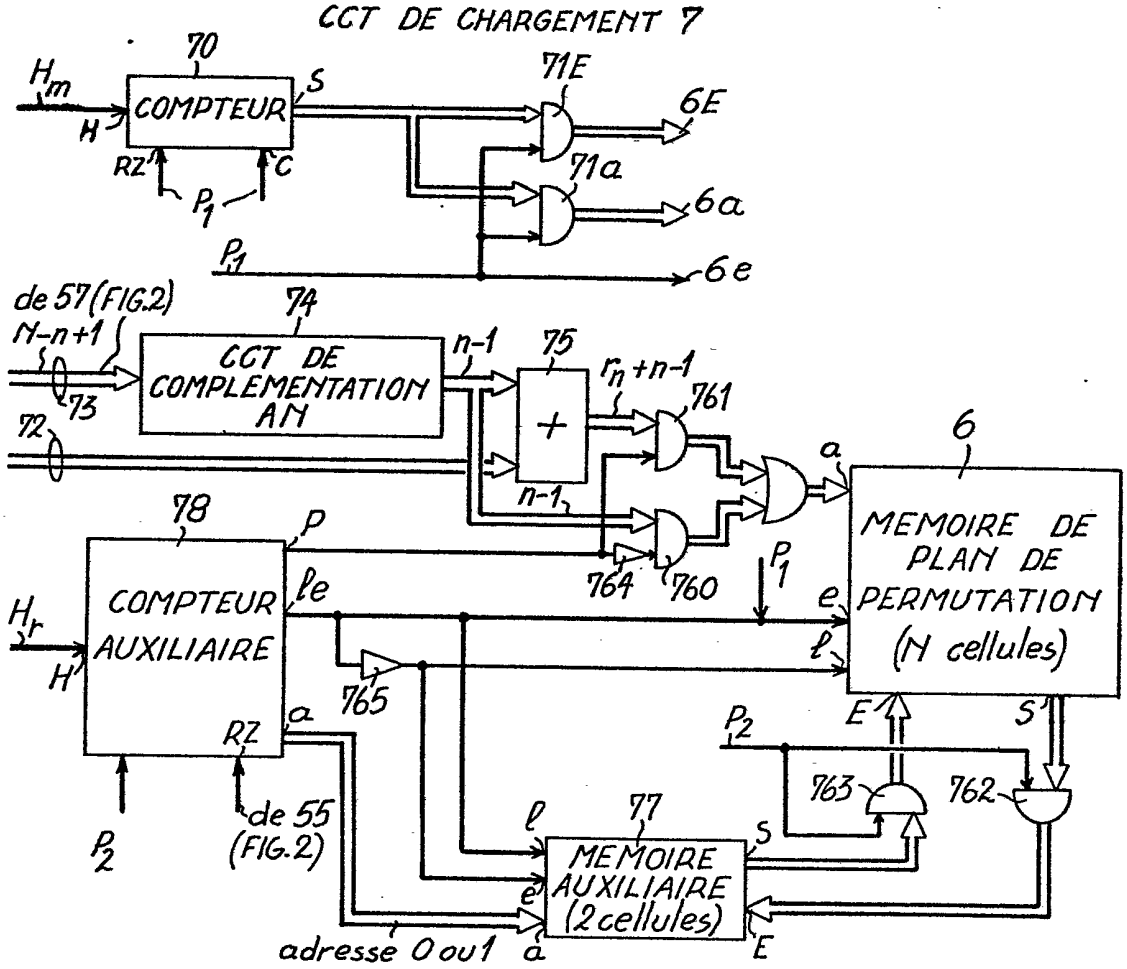
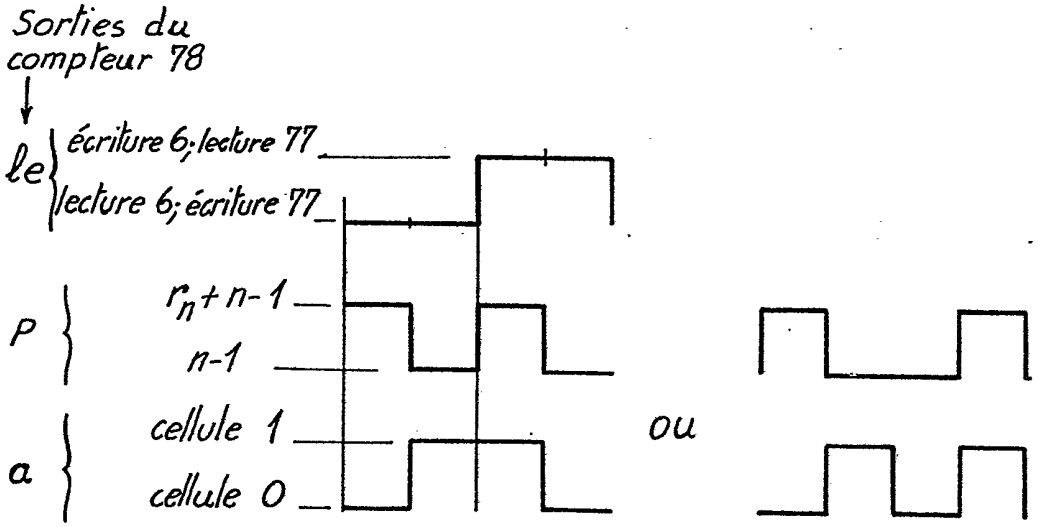

CCT DE CHARGEMENT 7
70
COMPTEUR
H_m
H
RZ
C
S
P_1
71E
6E
71a
6a
6e
de 57 (FIG.2)
N-n+1
73
72
74
CCT DE COMPLEMENTATION A N
n-1
75
+
r_n+n-1
761
n-1
764
760
6
MEMOIRE DE PLAN DE PERMUTATION (N cellules)
78
COMPTEUR AUXILIAIRE
H_r
H'
P
le
765
RZ
a
P_2
de 55 (FIG.2)
P_1
e
l
E
S
763
762
P_2
77
MEMOIRE AUXILIAIRE (2 cellules)
adresse 0 ou 1

FIG.4


Sorties du compteur 78
le
écriture 6; lecture 77
lecture 6; écriture 77
P
r_n+n-1
n-1
a
cellule 1
cellule 0
ou