(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication: **0 270 147**
**A1**

(12) # DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt: **87202057.3**

(51) Int. Cl.4: **H04K 1/00**

(22) Date de dépôt: **27.10.87**

(30) Priorité: **31.10.86 FR 8615209**

(43) Date de publication de la demande:
**08.06.88 Bulletin 88/23**

(84) Etats contractants désignés:
**BE CH DE FR GB IT LI NL SE**

(71) Demandeur: **TELECOMMUNICATIONS RADIOELECTRIQUES ET TELEPHONIQUES T.R.T.**
**88, rue Brillat Savarin**
**F-75013 Paris(FR)**

(72) Inventeur: **Masson, Jaques Société Civile S.P.I.D.**
**209, rue de l'Université**
**F-75007 Paris(FR)**

(74) Mandataire: **Chaffraix, Jean et al**
**Société Civile S.P.I.D. 209, rue de l'Université**
**F-75007 Paris(FR)**

(54) **Dispositif de cryptophonie analogique à permutations dynamiques de bande.**

(57) Dispositif de cryptophonie analogique à permutations dynamiques de bandes dans lequel le signal de parole est filtré (1), échantillonné (2) à la fréquence $f_e$, numérisé (3), transformé au moyen d'un banc de filtres d'analyse (4) en N signaux de sous-bandes échantillonnés à $f_e/N$ et transférés dans un ordre permuté vers un banc de filtres de synthèse (13) qui effectue les calculs du signal brouillé échantillonné à la fréquence $f_e$. Un ensemble de permutations est sauvegardé dans une mémoire (8) et un brouillage à permutations dynamiques dans le temps est obtenu par changement des adresses de lecture de la mémoire. Le signal brouillé reconverti en analogique (14,15) est transmis par l'intermédiaire d'un canal analogique à un débrouilleur où un prétraitement effectue les fonctions de synchronisation et d'égalisation et où les traitements effectués sont identiques à ceux effectués au brouilleur si ce n'est que l'ordre permuté des N signaux de sous-bande est inversé.

Application : télécommunications radio.

EP 0 270 147 A1

87202057.3

D



DESCRIPTION

# DISPOSITIF DE CRYPTOPHONIE ANALOGIQUE A PERMUTATIONS DYNAMIQUES DE BANDE

L'invention concerne un dispositif de cryptophonie analogique dans lequel le traitement du signal de parole effectué dans des processeurs numériques de signal comporte les opérations suivantes : filtrage, échantillonnage et numérisation par un convertisseur analogique-numérique, traitement par le banc de filtres d'analyse transformant le signal échantillonné à la fréquence $f_e$ en N signaux de sous-bande échantillonnés à $f_e/N$ et transférés dans un ordre permuté vers le banc de filtres de synthèse qui effectue les calculs du signal brouillé échantillonné à la fréquence $f_e$ auquel est ajouté en numérique l'onde de synchronisation $\sin(2\pi nTf_e/4)$, T étant la durée du cycle d'échantillonnage, le signal numérique brouillé ainsi obtenu étant converti en analogique, filtré et transmis par l'intermédiaire d'un canal analogique au débrouilleur où un prétraitement effectue les fonctions de synchronisation d'échantillonnage, de compensation de ladite onde de synchronisation et d'égalisation du signal brouillé et où les traitements effectués sont identiques à ceux effectués au brouilleur si ce n'est que ledit ordre permuté des N signaux de sous-bande est inversé.

Un tel dispositif est utilisé pour assurer la discrétion des communications sur voie radio. De façon générale, les systèmes de cryptophonie peuvent être classés en deux grandes familles : ce sont les systèmes à cryptophonie numérique et à cryptophonie analogique.

Les premiers systèmes nécessitent une numérisation et un codage du signal de parole, le débit binaire en résultant étant crypté à l'aide d'une séquence pseudo-aléatoire. Le degré de sécurité obtenu est potentiellement le plus élevé possible, c'est-à-dire que le message est indéchiffrable sans

la connaissance de la clé. Le problème qui se pose est la transmission du signal sur un canal radio standard de 3 kHz de bande passante. En effet, une telle transmission ne peut se faire qu'avec l'aide de modems travaillant à 2400 ou 4800 bits/s obligeant le codage de la parole à fonctionner à ces débits pour lesquels on ne peut assurer au mieux que l'intelligibilité du message. De tels systèmes qui, de plus, sont de mise en oeuvre relativement complexe, ne peuvent ainsi convenir qu'à des réseaux ou des liaisons où les abonnés sont des opérateurs spécialisés (armée, police, ...) pouvant accepter de converser avec une qualité de signal très fortement dégradée.

Les systèmes à cryptophonie analogique se distinguent des précédents en ce que la forme d'onde du signal transmis provient directement de transformations effectuées sur la forme d'onde du signal de parole original. Les transformations peuvent se faire dans le domaine du temps, de la fréquence ou des deux simultanément selon le degré de discrétion voulu. Il faut cependant remarquer qu'une sécurité absolue ne peut être atteinte avec ce genre de systèmes. Par contre, ils possèdent l'avantage d'une réalisation plus simple et offrent une qualité de signal restitué bien meilleure que dans les systèmes numériques.

Historiquement, les premiers brouilleurs analogiques étaient basés sur des transformations spectrales du type inversion, décalages ou permutation de bandes. Du fait de l'utilisation de techniques analogiques, le brouillage réalisé présentait des faiblesses dont les plus grandes étaient une intelligibilité résiduelle relativement importante ainsi qu'une robustesse à l'attaque très moyenne. Par exemple, la technique de permutations de bandes se limitait à 5 sous-bandes ce qui ne permettait pas de brouiller efficacement le signal. Avec l'apparition des mémoires et des microprocesseurs, les techniques utilisant des transformations temporelles ont vu le jour. Elles sont basées sur le principe de permutations

de blocs de 10 à 20 ms de signal. Ainsi la répartition de la puissance du signal en fonction du temps est différente de celle de la parole originale, alors que dans les brouilleurs spectraux, cette répartition est la même. Par contre, la forme d'onde des phonèmes permutés dans le temps reste inchangée. Cela constitue une faiblesse à l'attaque directe du signal brouillé visant à reconstituer l'ordre des segments de parole permutés. De plus, pour assurer une intelligibilité résiduelle la plus faible possible, les retards mis en jeu peuvent devenir assez importants (plusieurs centaines de ms) pouvant occasionner une gêne dans la communication.

On peut, à partir des deux techniques décrites précédemment, concevoir des brouilleurs relativement efficaces en mettant en cascade les transformations temporelles et spectrales. Néanmoins, avec l'apparition des processeurs numériques de signal, on peut envisager des techniques de brouillage très efficaces s'appuyant en fait sur les concepts des premiers brouilleurs et, notamment, les permutations de bandes de fréquence. L'emploi de techniques numériques permet de s'affranchir des problèmes de dérives qui affectent les modulateurs, démodulateurs et filtres utilisés dans un système analogique. Ainsi peut-on envisager de séparer un signal en un grand nombre de bandes de fréquence améliorant par là-même la qualité du brouillage. De plus, le fait de disposer de bancs de filtres miroir en quadrature pouvant reconstituer le signal original de façon presque parfaite, permet d'envisager un système à brouillage spectral très efficace.

On présente maintenant l'état de l'art en ce qui concerne les systèmes de brouillage analogique à traitement numérique utilisant des permutations spectrales et dont le traitement est fait en numérique. Ils peuvent être classés selon trois types :

- systèmes à permutations de coefficients de Transformée de Fourier Discrète,

- systèmes à permutations de bandes obtenues par bancs de filtres n'assurant pas une reconstitution parfaite de la bande,
- systèmes à permutations de bandes obtenues par bancs de filtres dits "QMF" ou "pseudo-QMF".

Les systèmes du premier type ont la propriété remarquable que le signal n'est absolument pas modifié quand, sans effectuer de permutations, on met bout à bout transformée et transformée inverse. En effet, on sait que $TFD^{-1}(TFD)$ = Identité. Néanmoins, le banc de filtres ainsi réalisé est de très mauvaise qualité en ce sens où, d'une part, la fonction de filtrage est du type $\frac{\sin x}{x}$ et, d'autre part, les recouvrements entre filtres sont très importants. Ainsi, le contrôle de la bande du signal crypté est mal aisé et, de plus, l'intelligibilité résiduelle du message crypté souffre de la "mollesse" des filtres.

Ces problèmes ont été résolus à l'aide de bancs de filtres très sélectifs qui permettent de plus de se passer de synchronisation. Cette propriété peut sembler attrayante mais est en fait une faiblesse en ce sens que la totalité du message transmis est permutée de la même façon. De plus, les filtres utilisés n'ont pas la propriété d'avoir la réponse composite analyse-synthèse unitaire et ainsi la qualité du signal restitué est médiocre.

Le dernier type de systèmes cumule les avantages des deux premiers dans la mesure où ils emploient des bancs de filtres "QMF" ou "pseudo-QMF" permettant un partage en bandes de fréquence relativement sélectives et ce, de façon quasi parfaite. Le brevet US 4 551 580 concerne un système de cryptophonie de ce type et du même genre que celui décrit dans le préambule.

Dans ce système les bancs de filtres "QMF" sont utilisés pour partager le signal en 5 sous-bandes, 25 échantillons consécutifs de chaque sous-bande constituant un bloc. La permutation joue alors sur l'ensemble des 125 échantillons des 5 blocs. Cette permutation est figée par le choix de la

clé. Bien que le système soit complexe, cette fixité est une faiblesse.

Une autre caractéristique de ce système est l'emploi d'un égaliseur qui compense uniquement la phase du canal en supposant que le module est unitaire. Cela implique que le système n'est exploitable que sur ligne téléphonique et non sur une liaison radiomobile. De plus, le principe de la mesure de la réponse impulsionnelle par envoi d'une impulsion de Dirac serait tout à fait inexploitable sur une liaison radio.

Des systèmes de cryptophonie basés sur des permutations dynamiques de bandes ont déjà été obtenus par traitements analogiques. Le but de l'invention est de proposer un système faisant toujours intervenir des permutations dynamiques, mais obtenu à partir de traitements numériques que permettent de réaliser aisément des bancs de filtres d'analyse et de synthèse quasi parfaits à l'aide de filtres "pseudo-QMF" et un partage du signal en un grand nombre de sous-bandes pouvant être permutées à un rythme très élevé.

Le système de cryptophonie analogique conforme à l'invention est remarquable en ce qu'un brouillage à permutations dynamiques dans le temps est obtenu par changement des adresses de lecture d'une mémoire contenant un ensemble de permutations, ces dites adresses provenant d'un générateur de séquence dont le rythme d'horloge donnant la fréquence de changement des permutations peut varier de 0 (permutation fixe) à $f_e/N$ (fréquence maximale), la clé du système étant un mot chargé dans le générateur, lors de la séquence d'initialisation.

La description suivante en regard des dessins annexés, le tout donné à titre d'exemple, fera bien comprendre comment l'invention peut être réalisée.

La figure 1 donne le schéma de principe du système de brouillage-débrouillage.

La figure 2 représente le schéma synoptique du brouilleur conforme à l'invention.

La figure 3 représente le schéma synoptique du débrouilleur conforme à l'invention.

La figure 4 donne le schéma de principe d'une boucle à verrouillage de phase entièrement numérique.

La figure 5 illustre l'auto-synchronisation d'une séquence PN.

Les figures 6 et 7 montrent le principe de la synchronisation lente avec l'égalisation travaillant respectivement en aveugle et avec référence locale.

Les tableaux des figures 8 et 9 explicitent respectivement les opérations de filtrage à réaliser dans les programmes d'analyse et de synthèse.

Disposant de filtres réalisant un découpage en sous-bandes et une reconstitution quasi parfaite, on peut réaliser un système brouilleur-débrouilleur selon le principe suivant (figure 1) :

- analyse du signal
- permutation P des signaux de sous-bandes
- obtention du signal brouillé par synthèse
- analyse du signal brouillé
- permutation inverse $P^{-1}$ des signaux de sous-bandes
- obtention du signal débrouillé par synthèse.

La sécurité du brouillage obtenu par un tel système repose sur la stratégie adoptée pour effectuer les permutations. Dans les systèmes à permutation fixe, le choix s'effectue de telle façon que l'intelligibilité résiduelle soit la plus faible possible. Malheureusement ce paramètre dépend fortement du locuteur et, de plus, l'attaque du système est relativement aisée si on suppose que l'on peut comparer un message de son choix et le cryptogramme associé.

Ces inconvénients peuvent être partiellement éliminés si les permutations, au lieu d'être fixes, varient dans le temps. L'attaque de la clé générant les permutations devient alors fastidieuse pour peu que le rythme de changement devienne élevé. De même, l'intelligibilité résiduelle peut devenir

très faible et devient complètement indépendante du locuteur. La contrepartie est le besoin de synchronisation au débrouilleur.

Le schéma synoptique d'un dispositif brouilleur-débrouilleur à permutations dynamiques de bandes conforme à l'invention est représenté sur les figures 2 et 3. Dans ce dispositif les calculs nécessaires aux différents traitements sont effectués par des processeurs numériques de signal tels que le TMS 32010 de Texas Instruments.

Pour les organes de conversion analogique-numérique et numérique-analogique ainsi que les filtrages, on a utilisé les circuits COFIDEC TP3057 de National Semi-conductor (conversion sur 8 bits -loi A). Ils présentent l'avantage de contenir toutes ces fonctions dans un seul boîtier de 16 broches.

Dans le brouilleur (figure 2), les différentes étapes du traitement sont les suivantes :

- Filtrage anti-repliements en 1 du signal original
- Echantillonnage en 2 et numérisation par un convertisseur analogique-numérique 3
- Analyse en 4 à l'aide d'un banc de filtres pseudo-QMF à 16 sous-bandes du signal échantillonné à la fréquence $f_e$ fournie par l'oscillateur 5 suivi du diviseur de fréquence 6. Le filtre prototype à 80 coefficients et les signaux de sous-bandes sont échantillonnés à $f_e/16$.
- Permutation en 7 à 12 des signaux de sous-bande au rythme de $f_e/16$ (seulement 12 signaux sont permutés, les 4 autres n'étant pas transmis).
- Synthèse en 13 des signaux de sous-bande permutés
- Restitution du signal analogique brouillé à l'aide d'un convertisseur numérique-analogique 14 et d'un filtre de lissage 15.
- Ajout en numérique d'une onde de synchronisation de fréquence $f_e/4$.

Le signal de parole provenant d'un microphone est appliqué à l'entrée du codeur analogique-numérique (circuit

COFIDEC) après adaptation de niveau. Le signal est filtré avant échantillonnage à la fréquence $f_e$ = 7 kHz puis est converti sur 8 bits MIC selon la loi A. L'échantillon est ensuite transféré dans le processeur réalisant, après linéarisation, le traitement par le banc de filtres d'analyse. Celui-ci transforme le signal original échantillonné à la fréquence $f_e$ en N signaux de sous-bande échantillonnés à $f_e/N$ (ici N = 16). Le séquencement des opérations se fait de la manière suivante :

- lecture par le processeur d'un échantillon ;
- calcul de la contribution de cet échantillon aux 16 signaux de sous-bande ;
- sortie d'un échantillon pour chacun des 16 signaux de sous-bande tous les 16 cycles d'échantillonnage (de durée T).

Lors de ce cycle particulier où le calcul final des échantillons de sous-bande est effectué, les 16 résultats sont écrits dans une RAM externe 10. Ces échantillons vont être ensuite immédiatement transférés dans le processeur effectuant le banc de synthèse mais dans un ordre permuté. La permutation joue sur les adresses de lecture de la RAM. Un ensemble de 256 permutations est sauvegardé dans une PROM 8. Le choix de la permutation à effectuer est donc représenté par un mot de 8 bits. Un brouillage à permutations dynamiques dans le temps est obtenu par changements des adresses de lecture de la PROM. Ces 8 bits d'adresse proviennent d'un générateur 7 d'une séquence PN à longueur maximale $2^n$-1 constitué de 16 bascules. La RAM externe 10 est adressée en écriture (E) ou en lecture (L) à travers le multiplexeur 9 par la permutation issue de la PROM. Le multiplexeur 9 et la PROM 8 reçoivent respectivement de 11 et 12 les adresses d'écriture et de lecture.

Le rythme de l'horloge réalisant les décalages de la séquence est la fréquence des permutations. Celle-ci peut varier de 0 (permutation fixe) à $f_e/N$ qui est la fréquence maximale ; en effet, $f_e/N$ est la fréquence d'échantillonnage

des signaux de sous-bande et donc, deux échantillons consécutifs d'un signal de sous-bande seront permutés de façon différente.

Les échantillons des signaux de sous-bande permutés sont ensuite lus par le processeur de synthèse. Celui-ci, de façon duale aux traitements effectués dans l'analyse, forme 16 échantillons du signal brouillé échantillonné à la fréquence $f_e$ à partir de 16 échantillons de sous-bande permutés qui sont échantillonnés à la fréquence $f_e/N$. A ce signal brouillé est ajouté en numérique l'onde de synchronisation $\sin(2\pi nTf_e/4)$. Pour éviter que ce signal, dont le niveau maximal est situé à -18 dB du niveau de saturation du décodeur, ne soit trop perturbé par la parole, les sous-bandes 13 et 14 sont mises autour de $f_e/4$, ces sous-bandes ayant été préalablement mises à zéro. De même, les sous-bandes 15 et 16 du signal original ne sont pas transmises.

Le signal numérique ainsi obtenu est, après compression MIC, transféré dans le COFIDEC où il est converti en signal analogique puis filtré. Le signal analogique est ensuite transmis puis traité par le débrouilleur.

Les traitements effectués au débrouilleur (figure 4) sont les suivants :

- Filtrage anti-repliements en 1' du signal brouillé.
- Synchronisation d'échantillonnage 2' effectuée par une boucle à verrouillage de phase entièrement numérique et compensation de l'onde de synchronisation.
- Numérisation par un convertisseur analogique-numérique 3'.
- Synchronisations des blocs et des permutations, et calcul des coefficients de l'égaliseur, lors de la séquence d'initialisation.
- Egalisation du signal brouillé à l'aide d'un filtre transverse.

  L'ensemble des traitements de synchronisations et d'égalisation est réalisé sur le processeur de signal 17.
- Analyse en 4' du signal brouillé.

- Permutation inverse en 7' à 12' des signaux de sous-bande.
- Synthèse en 13' des signaux de sous-bande remis à leur place.
- Restitution du signal analogique débrouillé à l'aide d'un convertisseur numérique-analogique 14' et d'un filtre de lissage 15'.

Les traitements énumérés ci-dessus sont, pour le coeur du système, identiques à ceux effectués au brouilleur si ce n'est que les permutations à faire subir aux signaux de sous-bande sont inverses à celles faites au brouilleur.

Le signal de parole brouillé est appliqué à l'entrée analogique du COFIDEC du débrouilleur et est filtré avant échantillonnage. La commande d'échantillonnage est élaborée par le processeur 17. La boucle s'accroche sur l'onde de synchronisation à $f_e/4$ où $f_e$ est la fréquence d'échantillonnage au brouilleur. On effectue ensuite successivement une compensation de cette onde de synchronisation (neutrodynage), un filtrage du signal par l'égaliseur dont les coefficients ont été obtenus lors de la séquence d'initialisation à l'aide d'un programme d'égalisation adaptative. Le signal, une fois égalisé, est transféré au processeur réalisant l'analyse, et le traitement qui suit est équivalent à celui expliqué dans le fonctionnement du brouilleur. La PROM 8' des permutations contient les permutations inverses de celles effectuées au brouilleur. Ses adresses de lecture proviennent d'un générateur 7' d'une séquence PN à 16 bascules. La RAM externe 10' disposée entre les processeurs d'analyse et de synthèse est adressée en écriture E ou en lecture L à travers le multiplexeur 9' par la permutation inverse issue de la PROM. Le multiplexeur 9' et la PROM 8' reçoivent respectivement de 11' et 12' les adresses d'écriture et de lecture.

Pour débrouiller parfaitement le signal, il faut que les signaux de sous-bande, après analyse du signal brouillé, soient identiques aux signaux appliqués au banc de synthèse du brouilleur. Pour ce faire, on doit réaliser :

- une synchronisation de l'échantillonnage à la fréquence $f_e$ du signal brouillé.
- une égalisation du canal tant en amplitude qu'en temps de propagation de groupe.
- une synchronisation des blocs permettant de transmettre l'information de la phase de sous-échantillonnage effectuée dans le banc de filtres d'analyse.
- une synchronisation des permutations.

On analyse maintenant en détail ces différents points.

En ce qui concerne la synchronisation d'échantillonnage, des essais subjectifs sur la qualité de la parole restituée ont montré que l'on peut tolérer des écarts de phase d'échantillonnage de ± 5 % de la période T.

Pour atteindre cet objectif, une boucle à verrouillage de phase entièrement numérique réalisée à l'aide d'un processeur de signal a été étudiée. Cette boucle dont le schéma de principe est représenté sur la figure 4, comporte les éléments constitutifs suivants :

- un échantillonneur-bloqueur 18 et un convertisseur analogique-numérique 19,
- deux démodulateurs en quadrature (cosinus et sinus) 20 et 21 et leurs filtres associés 22 et 23,
- une logique de décision permettant de faire la correction de phase d'échantillonnage 24. Dans le contexte d'un processeur de signal 8, cette correction s'effectue autour de la valeur de fréquence libre ($f_e$) par l'ajout ou le retrait d'un
- certain nombre de cycles "machine", ce qui permet d'obtenir un verrouillage à double vitesse de la boucle.

La boucle entièrement numérique ainsi réalisée présente les caractéristiques principales suivantes :

- une acquisition rapide (≈ une centaine de périodes d'échantillonnage)
- un suivi correct en présence de perturbations (bruit-dérive)
- une réalisation simple sur processeur de signal.

On dispose donc du moyen permettant de retrouver la phase d'échantillonnage du signal brouillé quand, avant transmission, et en numérique, on lui ajoute la séquence.

Pour compenser les distorsions d'amplitude et de temps de propagation de groupe apportées par le canal, un filtrage par un égaliseur du signal brouillé est nécessaire.

La fonction d'un égaliseur est de réaliser le filtre inverse du canal ; si on appelle h et g les réponses impulsionnelles du canal et de l'égaliseur, on doit avoir dans le cas idéal :

$$(h \otimes g)(n) = \delta(n-n_0)$$

où $n_0$ représente le retard que subit le signal lors de la transmission dans le canal puis l'égaliseur. L'égaliseur a été réalisé à l'aide d'un filtre transverse à 48 coefficients.

Lors de la séquence d'initialisation, un programme d'égalisation adaptative sur processeur de signal permet de trouver les coefficients du filtre égaliseur à l'aide de l'algorithme du gradient. L'égaliseur adaptatif travaille d'abord en aveugle (figure 6) puis en référence local (figure 7). Pour travailler dans ce deuxième mode, on se sert de la propriété d'auto-synchronisation (figure 5) des séquences PN. Cette propriété sert également pour transmettre les synchronisations de blocs et des permutations.

La figure 5 explique cette propriété d'auto-synchronisation pour la séquence PN 27 ou 27' générée par le polynôme P(x) = x16+x5+x3+x2+1. La sortie E du circuit d'émission est obtenue par addition modulo 2 de x, message à transmettre, et de F, signal de rebouclage. Si à l'entrée du circuit réception on applique E, après 16 coups d'horloge (ce qui correspond au degré maximal du polynôme générateur) la sortie S est égale à x. En effet, quel que soit l'état initial, il suffit de 16 temps d'horloge pour que les bascules de rang identique contiennent les mêmes informations. Comme E = x + F, on peut calculer :

$$S = E \oplus F = (x \oplus F) + F \ldots = x \oplus (F \oplus F) = x \oplus 0 = x.$$

La sortie E du circuit émission (figure 5) étant prise comme séquence pseudo-aléatoire pour l'égalisation adaptative, et si l'on fonctionne comme précédemment en "aveugle" (figure 6), on essaye de synchroniser le circuit réception sur le signal appelé E', résultat de la décision sur le signal égalisé. Le message imposé x est une suite de "1" ; si l'égaliseur 25 bouclé à travers l'adaptateur 28 a "suffisamment bien" convergé, c'est-à-dire que 32 bits successifs décidés ont la valeur juste, la sortie S va prendre 16 fois la valeur "1". On peut estimer alors que les deux séquences 27 et 27' sont synchronisées et l'égalisation peut ainsi travailler avec référence locale (figure 7). A ce moment là, le circuit au récepteur est basculé en émission locale permettant le calcul d'adaptation des coefficients de façon optimale. En effet, en présence de bruit, il peut se produire des erreurs de décision quand l'égaliseur travaille en aveugle.

Lorsque l'égaliseur 25 fonctionne avec référence locale, les synchronisations de bloc et de permutations se font par reconnaissance d'un état particulier des bascules des registres PN.

En résumé, les traitements effectués par le processeur (17) pendant la séquence d'initialisation au débrouilleur sont, de façon séquentielle, les suivants :

. détection de la tonalité de fréquence $f_e/4$ indiquant le début de communication et accrochage de la boucle à verrouillage permettant d'effectuer la synchronisation d'échantillonnage.
. égalisation adaptative aveugle.
. commutation en égalisation adaptative avec référence locale.
. gel de l'adaptation des coefficients et passage de la synchronisation des blocs et celle des permutations qui termine la séquence d'initialisation.

Les traitements qu'effectue le processeur (17) en fonctionnement "normal" (hors séquence d'initialisation) sont les suivants :

. boucle à verrouillage de phase.

. compensation de l'onde de synchronisation.

. égalisation du signal.

Voici maintenant quelques indications succinctes concernant les programmes de traitement implantés sur les processeurs.

Programme d'analyse

Le banc de filtres que l'on veut réaliser est composé de 16 filtres à 80 coefficients chacun. Si les filtres du banc sont obtenus par modulation d'un même filtre prototype, la réalisation peut se faire de façon très efficace. En effet, on montre que l'on peut dans ce cas séparer les opérations de filtrage et de modulation. Les traitements sont effectués de la façon suivante :

Soit $Xk(m)$ le $k^{ème}$ signal de sous-bande ($k = 0, \ldots, N-1$) échantillonné à la fréquence $f_e/N$. Il s'obtient à partir des signaux de sortie des cellules de filtrage notés $p(m)$ par :

$$Xk(m) = \sum_{\varrho=0}^{N-1} p_\varrho(m).c(k.\varrho)$$

où $c(k,\varrho) = 2\cos((2k+1)(2\varrho+1)(2\varrho+1)\pi/4N)$ est le noyau de la transformée en cosinus impaire.

Les tableaux de la figure 8 explicitent les opérations de filtrage à réaliser pour obtenir les signaux $p_\varrho(m)$. Formellement, $p_\varrho(m)$ s'écrit :

$$p_\varrho(m) = -\sum_{r=0}^{\lambda-1} \cos(r\pi/2).h_\varrho(r).x_\varrho(m-r)$$

$$-\sum_{r=0}^{\lambda-1} \sin(r\pi/2).h_\varrho(r).x_{N-1-\varrho}(m-\lambda+r+1)$$

où . $h_\varrho(r) = h(rN+\varrho)$, h étant la réponse impulsionnelle du filtre prototype,

. $x_\varrho(m) = x(mN-\varrho)$, x étant le signal d'entrée,

. $\lambda = Nc/N$, Nc étant le nombre de coefficients du filtre prototype. Dans le cas présent, $Nc = 80$ coefficients, $N = 16$ et donc $\lambda = 5$.

Le tableau supérieur de la figure 8 représente la mémoire des 80 échantillons les plus récents du signal, orga-

nisés en 5 lignes de 16 éléments. L'échantillon le plus récent est situé en haut à gauche, alors que l'échantillon le plus vieux se trouve en bas à droite. Le tableau inférieur représente la mémoire des 80 coefficients du filtre prototype rangés également en 5 lignes de 16 éléments et affectés des signes des nombres $\cos(r\pi/2)$ et $\sin(r\pi/2)$ apparaissant dans la formule ci-dessus.

L'obtention de $p_\varrho(m)$ se fait par le calcul de la somme des 5 produits dont les facteurs sont visualisés par le même signe dans chacun des tableaux. On voit que le calcul de $p_\varrho(m)$ ne nécessite pas la connaissance complète du tableau et qu'il peut s'effectuer en fait dès l'arrivée de $x_\varrho(m)$. Le calcul de $Xk(m)$ nécessite, quant à lui, la connaissance de tous les signaux $p_\varrho(m)$. Néanmoins on peut effectuer après chaque calcul de $p_\varrho(m)$ les produits partiels $p_\varrho(m)$, $C(k,\varrho)$ par $k=0, \ldots, N-1$, c'est-à-dire la contribution de $p_\varrho(m)$ au calcul de chacun des signaux de sous-bande.

Programme de synthèse

Les traitements effectués dans le banc de synthèse sont duaux de ceux effectués dans le banc d'analyse. Les signaux de sous-bandes permutés vont d'abord être modulés par la transformée de cosinus impaire selon la formule suivante :

$$y(m) = -N \sum_{k=0}^{N-1} c(k,\varrho).Xs(k)(m)$$

où s est la permutation.

Les signaux $y_\varrho(m)$ sont ensuite filtrés pour obtenir le signal brouillé de la façon indiquée sur les deux tableaux de la figure 9.

$$x_\varrho^{(b)}(m) = -\sum_{r=0}^{\lambda-1} \sin(r\pi/2).h_\varrho(r).y_\varrho(m-r)$$

$$+\sum_{r=0}^{\lambda-1} \cos(r\pi/2).h_\varrho(r).y_{N-1-\varrho}(m-r)$$

REVENDICATIONS :

1. Dispositif de cryptophonie analogique dans lequel le traitement du signal de parole effectué dans des processeurs numériques de signal comporte les opérations suivantes : filtrage (1), échantillonnage (2) et numérisation dans un convertisseur analogique-numérique (3), traitement par un banc de filtres d'analyse (4) transformant le signal échantillonné à la fréquence $f_e$ en N signaux de sous-bande échantillonnés à $f_e/N$ et transférés dans un ordre permuté vers le banc de filtres de synthèse (13) qui effectue les calculs du signal brouillé échantillonné à la fréquence $f_e$ auquel est ajouté en numérique une onde de synchronisation, le signal numérique brouillé ainsi obtenu étant converti en analogique (14), filtré (15) et transmis par l'intermédiaire d'un canal analogique au débrouilleur où un prétraitement effectue en (17) les fonctions de synchronisation d'échantillonnage, de compensation de ladite onde de synchronisation et d'égalisation du signal brouillé et où les traitements effectués sont identiques à ceux effectués au brouilleur si ce n'est que ledit ordre permuté des N signaux de sous-bande est inversé, caractérisé en ce que ladite onde de synchronisation étant dans un rapport simple avec la fréquence d'échantillonnage et lesdites fonctions de synchronisation d'échantillonnage et de compensation de ladite onde de synchronisation étant effectuées en numérique, un brouillage à permutations dynamiques dans le temps est obtenu par changement des adresses de lecture d'une mémoire (8) contenant un ensemble de permutations, ces dites adresses provenant d'un générateur pseudo-aléatoire (7) dont le rythme d'horloge donnant la fréquence de changement des permutations peut varier de 0 (permutation fixe) à $f_e/N$ (fréquence maximale), la clé du système étant un mot chargé, lors de la séquence d'initialisation, dans le générateur pseudo-aléatoire.

2. Dispositif de cryptophonie selon la revendication 1, caractérisé en ce que la synchronisation d'échantillonnage de l'onde de synchronisation est effectuée au débrouilleur au

moyen d'une boucle à verrouillage de phase entièrement numérique et à double vitesse de verrouillage.

3. Dispositif de cryptophonie selon la revendication 1, caractérisé en ce que les distorsions d'amplitude et de phase apportées par le canal de transmission au signal brouillé sont corrigées au moyen d'un égaliseur.

4. Dispositif de cryptophonie selon la revendication 2, caractérisé en ce que ladite boucle à verrouillage de phase est utilisée pour effectuer une prise de synchronisation d'échantillonnage préalable au calcul des coefficients de l'égaliseur à l'aide d'un algorithme d'égalisation adaptative travaillant successivement en mode d'égalisation aveugle et en mode d'égalisation avec référence locale.

5. Dispositif de cryptophonie selon la revendication 4, caractérisé en ce que lesdits coefficients de l'égaliseur sont obtenus à l'aide d'un algorithme d'égalisation adaptative travaillant successivement en mode d'égalisation aveugle et en mode d'égalisation avec référence locale.

6. Dispositif de cryptophonie selon la revendication 5, caractérisé en ce que le fonctionnement de ladite égalisation adaptative avec référence locale permet la synchronisation des permutations par reconnaissance d'un état particulier du système générant ladite référence locale.

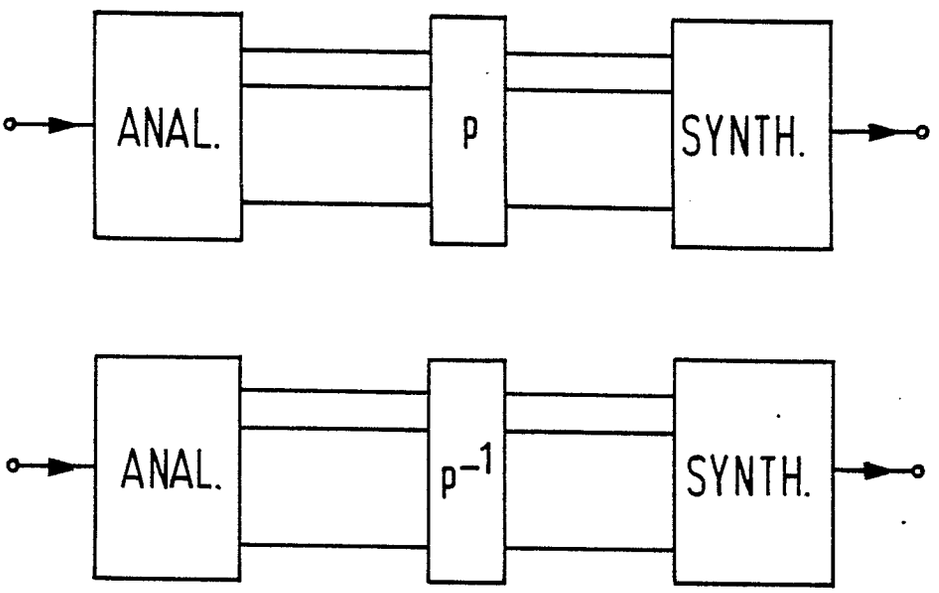


FIG.1

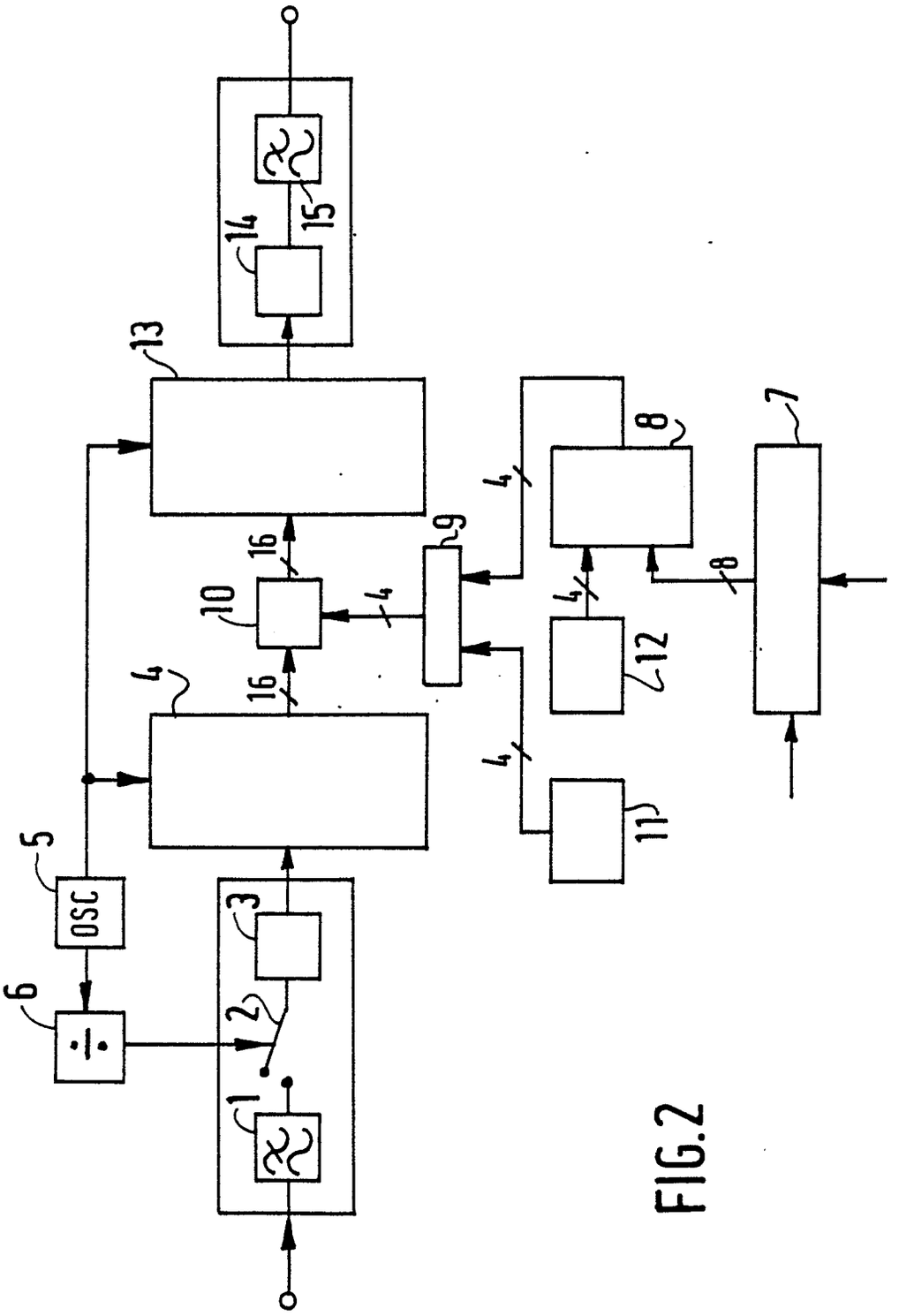


FIG.2

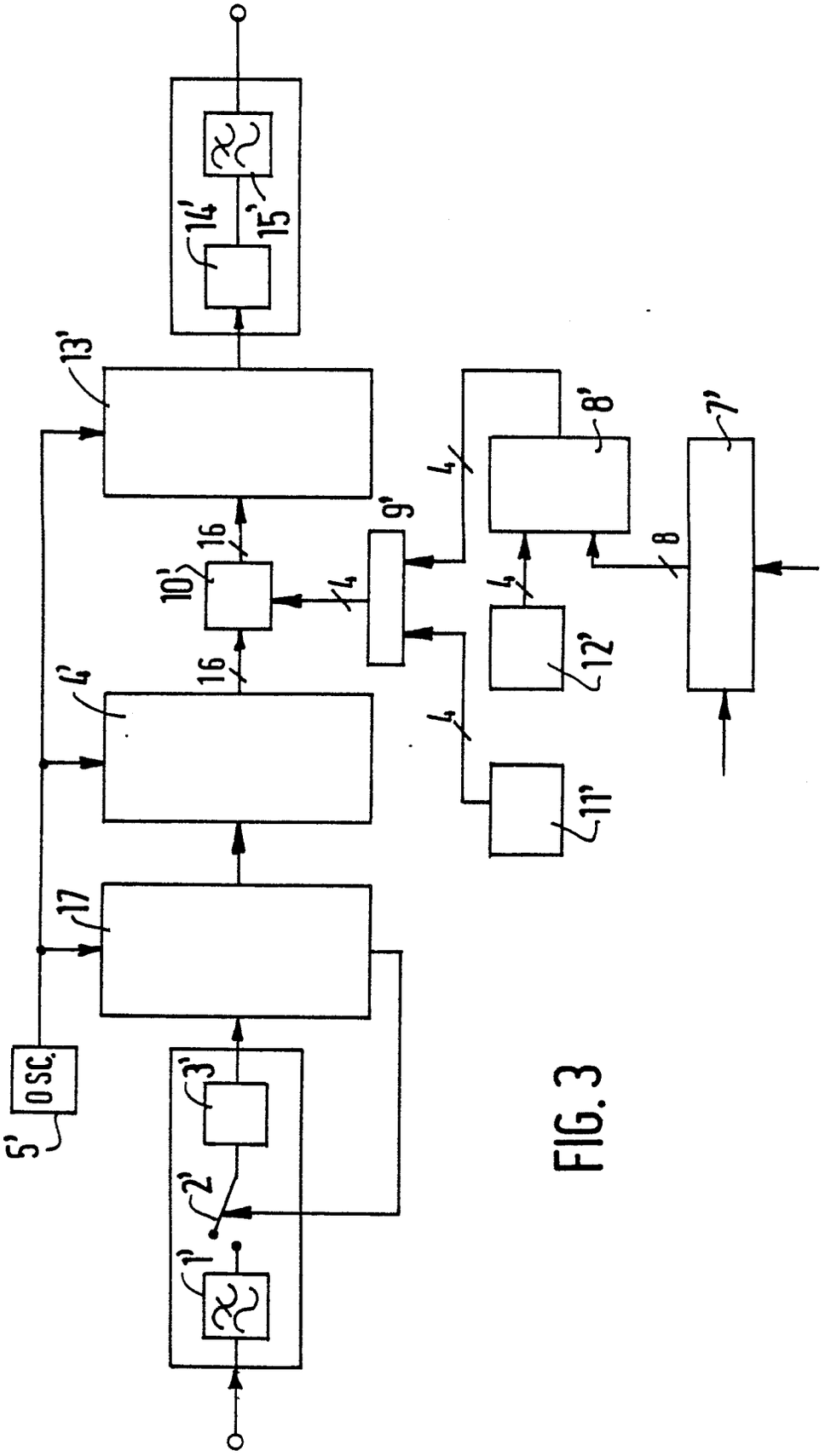


FIG. 3

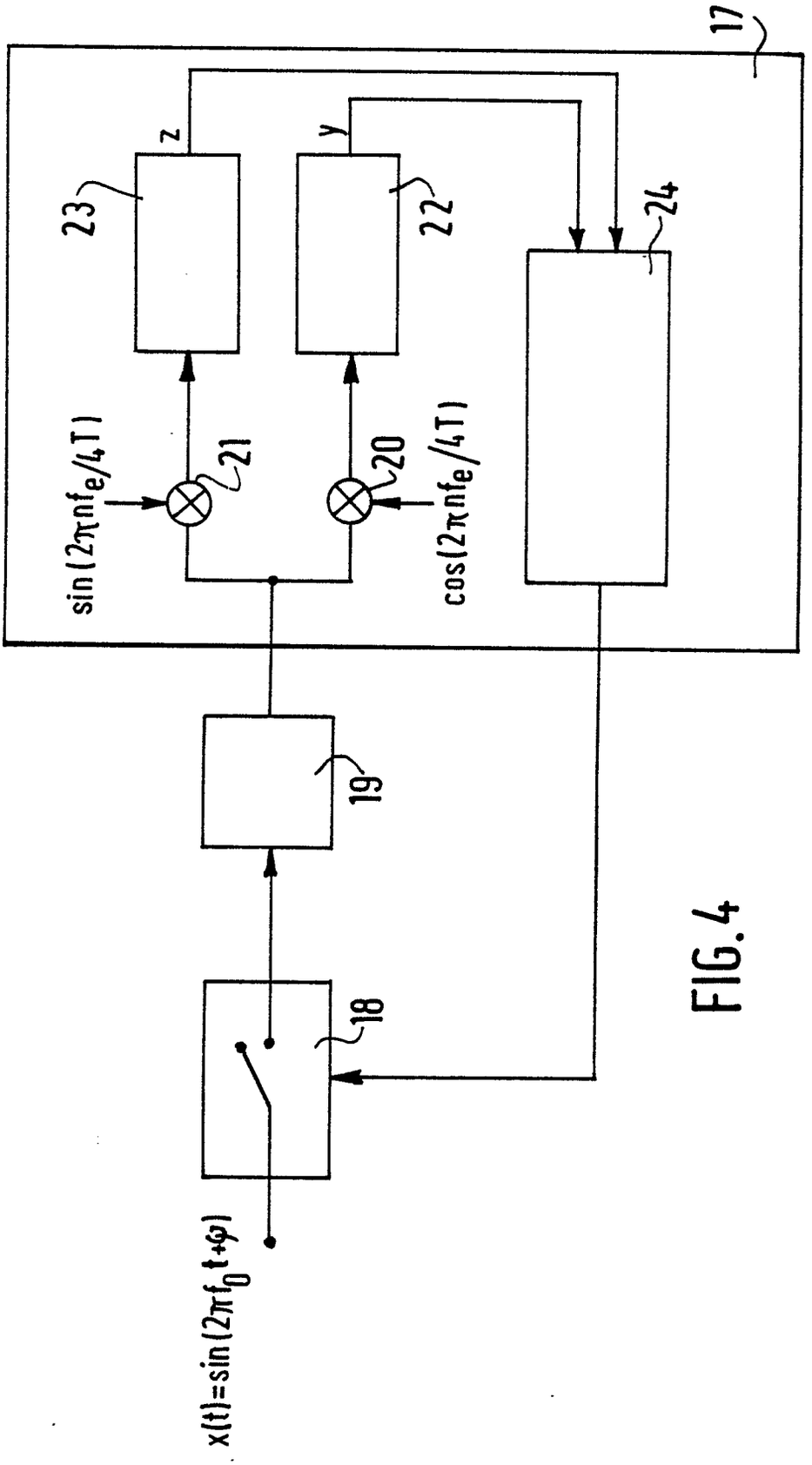


FIG.4

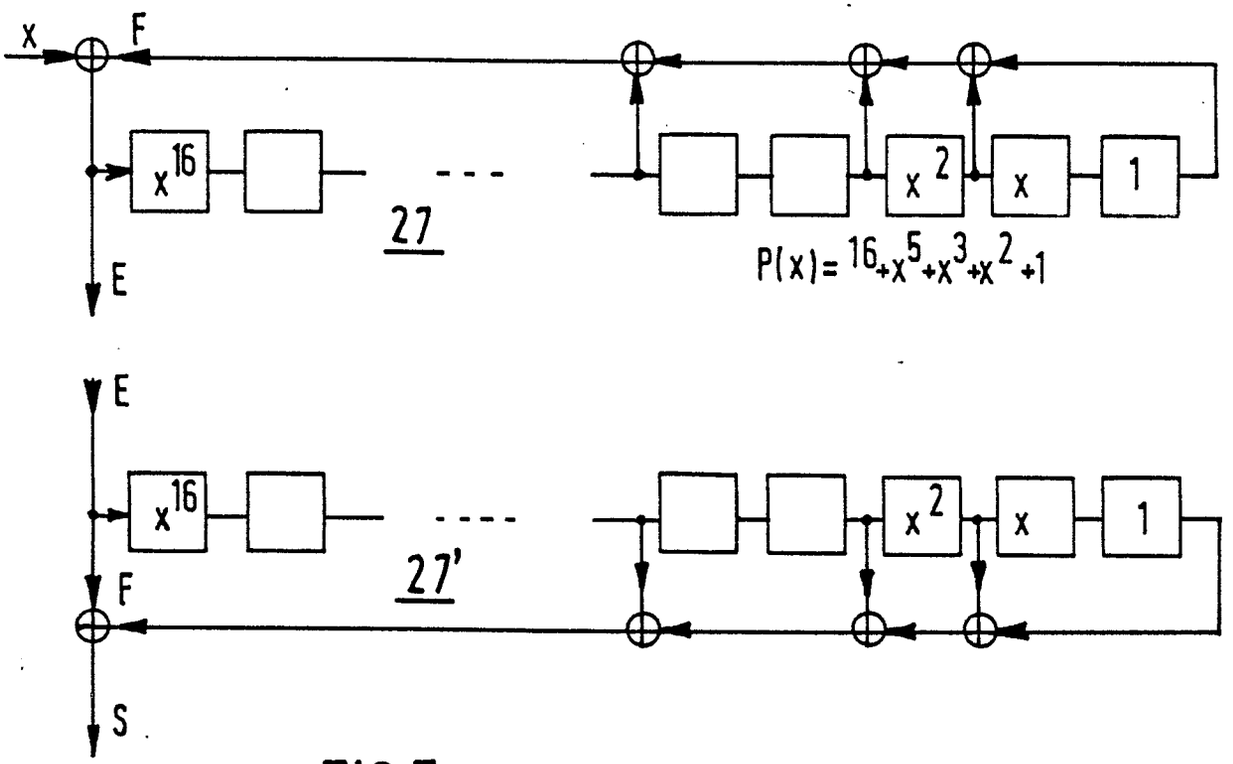


FIG.5

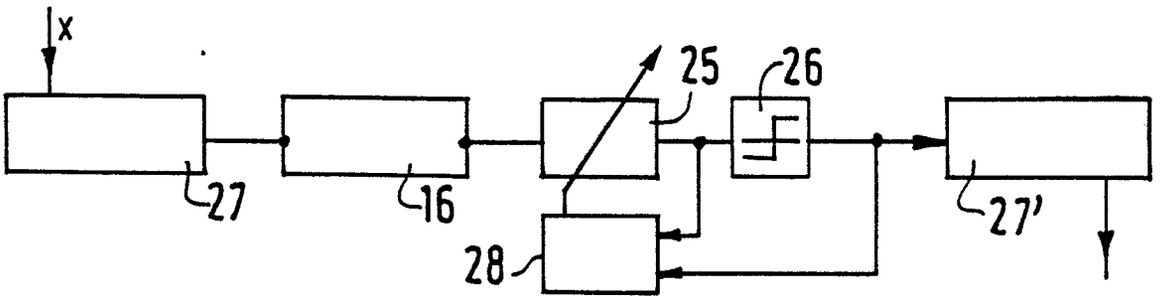


FIG.6

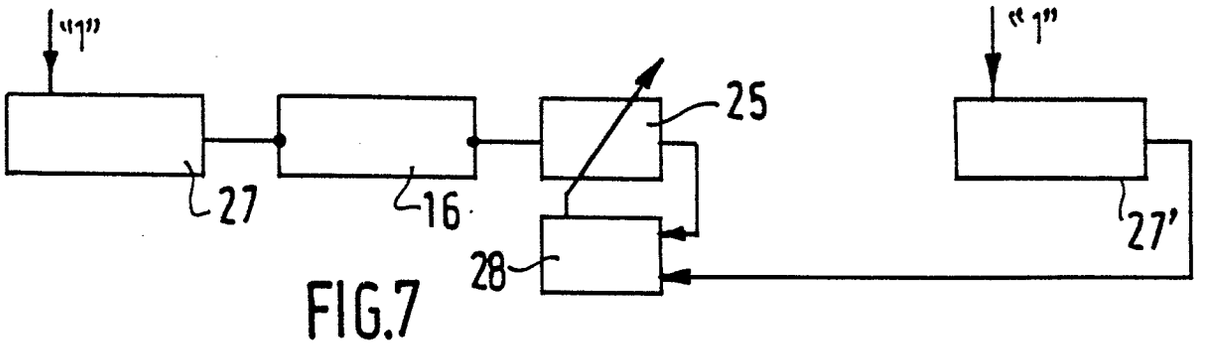


FIG.7

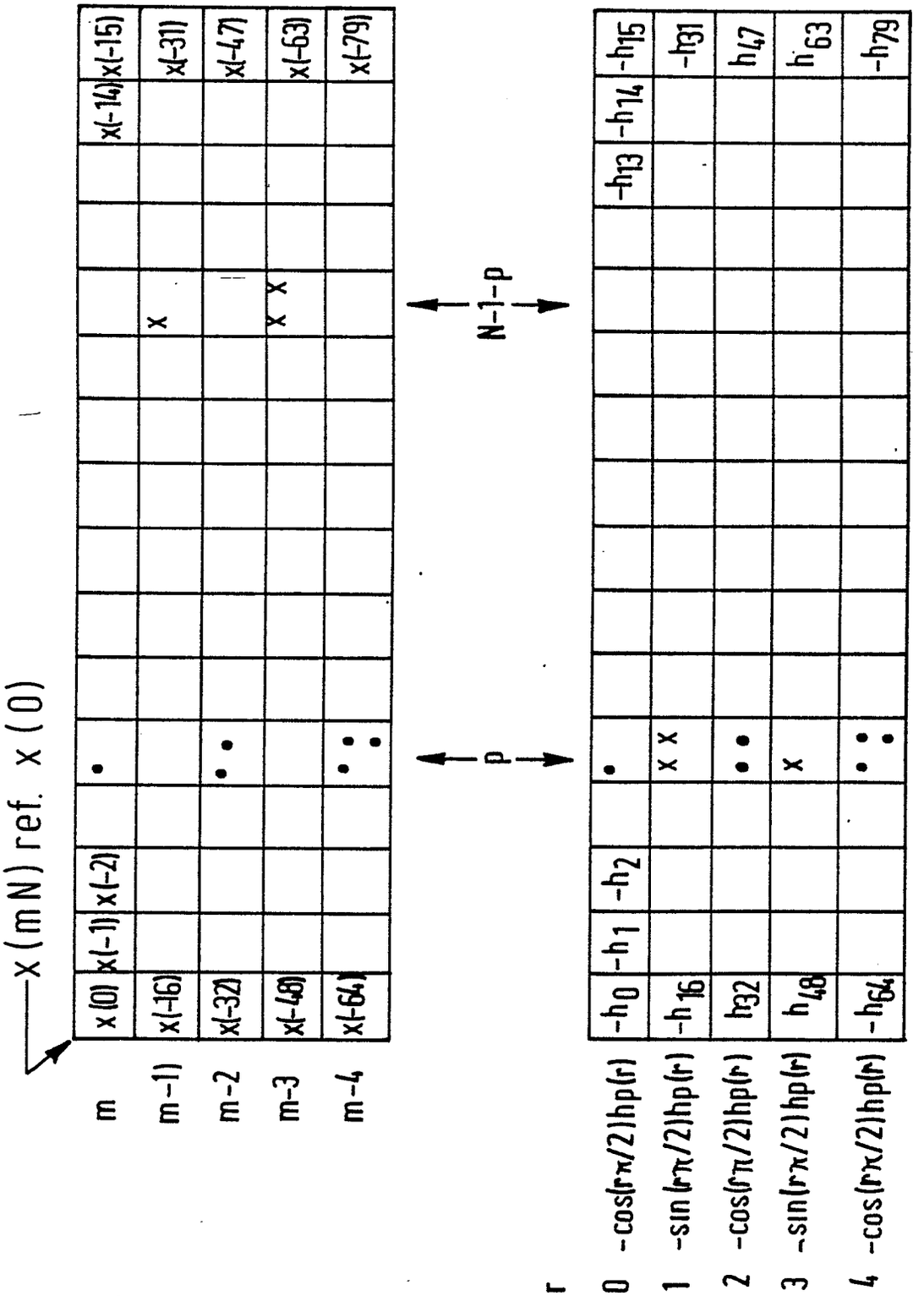
x (mN) ref. x (0)
m
m-1
m-2
m-3
m-4
x(0) x(-1) x(-2) x(-14) x(-15)
x(-16) x(-31)
x(-32) x(-47)
x(-48) x(-63)
x(-64) x(-79)
p
N-1-p
r
0 -cos(rπ/2)hp(r)
1 -sin(rπ/2)hp(r)
2 -cos(rπ/2)hp(r)
3 -sin(rπ/2)hp(r)
4 -cos(rπ/2)hp(r)
-h0 -h1 -h2 -h13 -h14 -h15
-h16 -h31
h32 h47
h48 h63
-h64 -h79

FIG.8

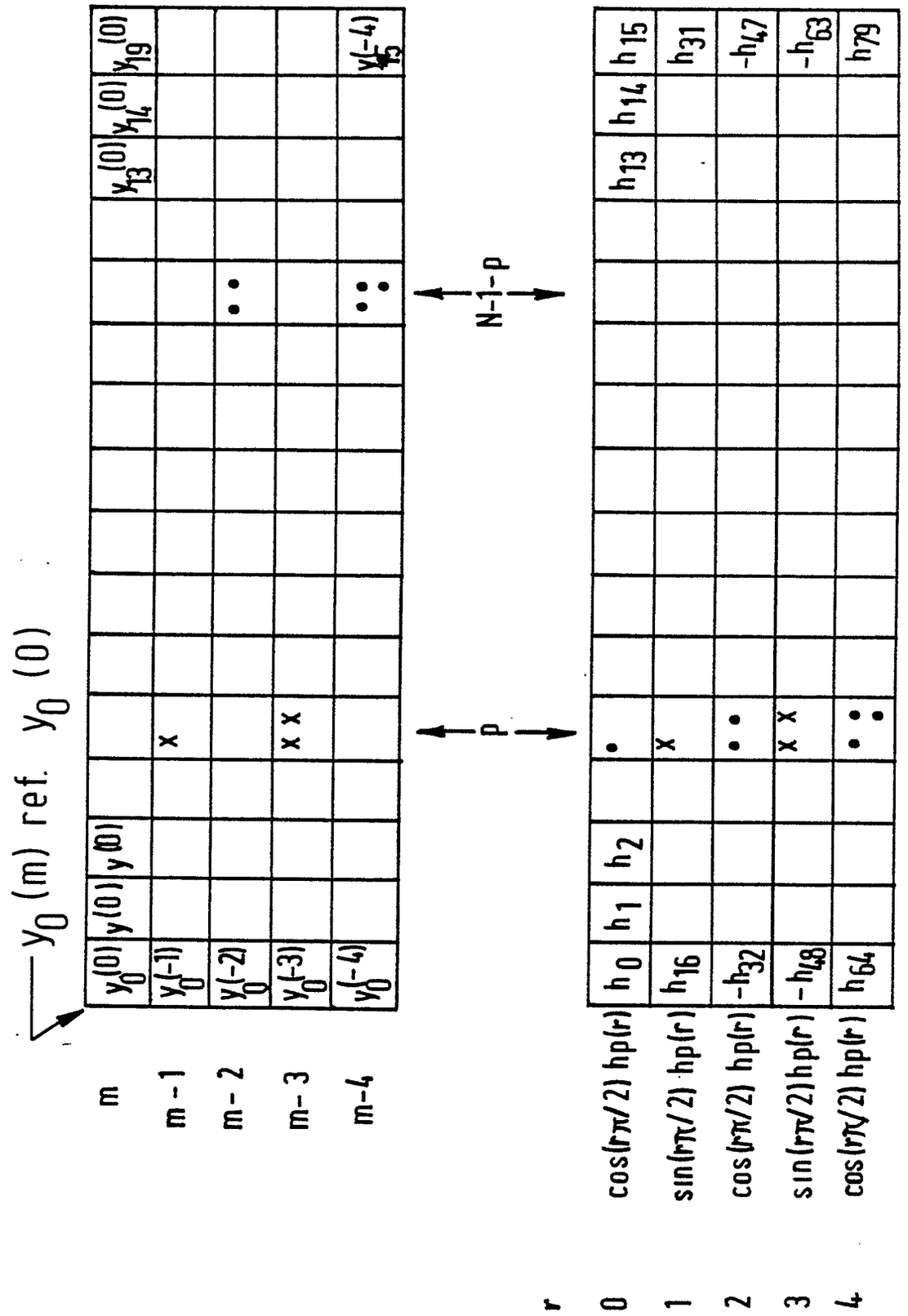
m
m-1
m-2
m-3
m-4
$y_0$ (m) ref. $y_0$ (0)
$y_0^{(0)}$ $y_0^{(-1)}$ $y_0^{(-2)}$ $y_0^{(-3)}$ $y_0^{(-4)}$
$y_{13}^{(0)}$ $y_{14}^{(0)}$ $y_{19}^{(0)}$ $y_{15}^{(-4)}$
P
N-1-p
r
0
1
2
3
4
$\cos(r\pi/2)\, hp(r)$
$\sin(r\pi/2)\, hp(r)$
$\cos(r\pi/2)\, hp(r)$
$\sin(r\pi/2)\, hp(r)$
$\cos(r\pi/2)\, hp(r)$
$h_0$ $h_1$ $h_2$ $h_{13}$ $h_{14}$ $h_{15}$
$h_{16}$ $h_{31}$
$-h_{32}$ $-h_{47}$
$-h_{48}$ $-h_{63}$
$h_{64}$ $h_{79}$

FIG.9

Office européen des brevets

# RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande

EP 87 20 2057

## DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie | Citation du document avec indication, en cas de besoin, des parties pertinentes | Revendication concernée | CLASSEMENT DE LA DEMANDE (Int. Cl.4) |
|---|---|---|---|
| A,D | US-A-4 551 580 (COX et al.)<br>* En entier *<br>--- | 1,3 | H 04 K 1/00 |
| A | US-A-3 504 286 (JACOBAEUS)<br>* Revendications 1,2,6,11 *<br>--- | 1,3 | |
| A | FR-A-2 379 947 (S.E.C.R.E.)<br>* Page 6, ligne 11 - page 7, ligne 1; figure 4 *<br>--- | 1 | |
| A | US-A-4 221 931 (SEILER)<br>* Résumé; revendications 1,2 *<br>--- | 1 | |
| A | EP-A-0 156 428 (T.R.T.)<br>* Revendications 1,3 *<br>--- | 1,2 | |
| A | GLOBECOM '82 - IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, Miami, 29 novembre - 2 décembre 1982, Conference Record, vol. 1/3, pages A6.2.1 - A6.2.5, IEEE, New York, US; R.V. COX et al.: "An analog scrambler for speech based on sequential permutations in time and frequency"<br>* En entier *<br>----- | 1,3 | |

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.4)

H 04 K
H 04 L

Le présent rapport a été établi pour toutes les revendications

| Lieu de la recherche | Date d'achèvement de la recherche | Examinateur |
|---|---|---|
| LA HAYE | 05-02-1988 | SNELL T. |

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0402)