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

(11) Numéro de publication: **0 156 428**
A1

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt: **85200353.2**

(51) Int. Cl.⁴: **H 04 K 1/00**

(22) Date de dépôt: **11.03.85**

(30) Priorité: **13.03.84 FR 8403812**

(43) Date de publication de la demande:
02.10.85 Bulletin 85/40

(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)

(84) Etats contractants désignés:
FR

(71) Demandeur: **N.V. Philips' Gloeilampenfabrieken**
Groenewoudseweg 1
NL-5621 BA Eindhoven(NL)

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

(72) Inventeur: **Hillion, Hervé**
SOCIETE CIVILLE 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) Système de cryptophonie pour des liaisons à largeur de bande étroite.

(57) Système de cryptage et de décryptage de signaux analogiques à bande étroite comprenant, dans des stations d'émission et de réception, des moyens (2, 32) de numériser un signal analogique entrant, respectivement clair et crypté, et de diviser les données résultantes en trames d'un nombre prédéterminé de bits, chaque trame étant divisée en un certain nombre de paquets d'un nombre prédéterminé de bits, lesdites stations d'émission et de réception comprenant en outre un générateur de code pseudo-aléatoire (7, 37), des moyens (13, 43) de synchroniser les deux générateurs de code pseudo-aléatoire l'un avec l'autre, et des moyens de permutation des paquets d'une trame, caractérisé en ce que ledit système comprend en outre des moyens (15, 45) d'inverser en synchronisme le spectre des signaux émis et reçus, et que les générateurs de code pseudo-aléatoire (7, 37) ont un cycle de (N+1) bits aléatoires dont N bits servent à commander la permutation des paquets et un bit commande l'inversion de spectre.

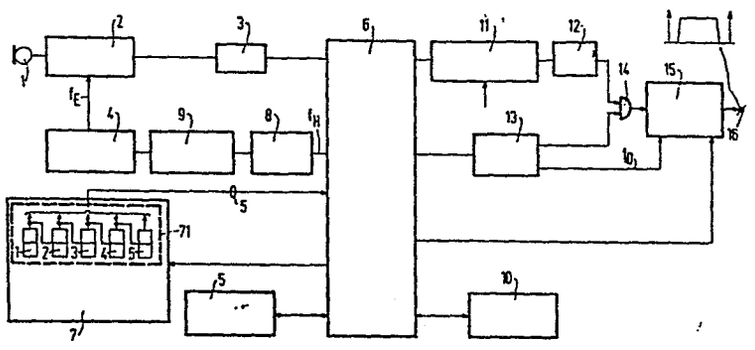

FIG.1

EP 0 156 428 A1

SYSTEME DE CRYPTOPHONIE POUR DES LIAISONS A LARGEUR DE BANDE ETROITE

La présente invention concerne un système cryptographique pour signaux de parole à bande étroite et, plus particulièrement un système cryptophonique pseudo-aléatoire s'appliquant à des signaux de parole analogiques ayant une bande passante de 0,3 à 3,3kHz approximativement.

Des systèmes cryptographiques numériques pseudo-aléatoires ont déjà été proposés. Dans de tels systèmes, des données numériques non cryptées ou "claires" sont appliquées à une unité de cryptage. Un flux de bits pseudos-aléatoires appelé "mot de clé" est produit par un premier générateur de code pseudo-aléatoire et il est également appliqué à l'unité de cryptage. L'unité de cryptage crypte les données du texte clair en réponse au mot clé, par exemple en additionnant modulo 2 les bits de même rang de la séquence claire et du mot de clé pour générer un flux numérique crypté et inintelligible. Ce flux numérique crypté est transmis par un câble ou une liaison radio à une unité de décryptage. Dans cette unité de décryptage, un second générateur de code pseudo-aléatoire produit un mot de clé de réception identique au mot de clé d'émission. Ce mot de clé de réception est utilisé pour le décryptage des données cryptées transmises. Les données décryptées sont alors disponibles pour un usage normal.

Pour que les unités de cryptage et de décryptage fonctionnent convenablement, les premier et second générateurs de code pseudo-aléatoire à chaque extrémité de la liaison doivent être identiques et synchrones, c'est-à-dire démarrer au même point de fonctionnement de leur cycle pour que des mots de clé identiques soient produits à chaque station et à chaque instant.

Un tel système cryptographique est par exemple décrit dans le brevet des Etats-Unis d'Amérique US-A-4133974.

Dans les systèmes cryptographiques qui viennent d'être rappelés, c'est un signal de parole numérisé qui est émis sur la

voie de transmission et cette dernière doit avoir une largeur de bande d'au moins le double de la bande passante du signal de parole.

Dans la présente invention, le signal de parole est traité numériquement dans les stations d'émission et de réception, mais il est transmis analogiquement sur la voie de transmission. Les dispositifs de cryptage et de décryptage peuvent donc être insérés en ligne sur des liaisons préexistantes non cryptées sans modification de ces dernières. Les liaisons de radiotéléphone par exemple peuvent être rendues secrètes sans modification autre que l'insertion en ligne des dispositifs de l'invention.

Conformément à l'invention, les stations d'émission et de réception comprennent chacune un générateur de code pseudo-aléatoire et un signal de synchronisation à fréquence audio est transmis de la station d'émission à la station de réception pour synchroniser les deux générateurs de code pseudo-aléatoire.

Dans la station d'émission, le signal de parole est numérisé par un convertisseur analogique numérique et le signal numérique obtenu est divisé en trames comprenant chacune un certain nombre de paquets de bits. Ces paquets sont mis en mémoire, puis sous la commande du générateur de code pseudo-aléatoire d'émission, les rangs des paquets dans la trame sont permutés. Toujours sous la commande du générateur de code pseudo-aléatoire, les paquets permutés sont lus dans un sens ou dans le sens opposé, puis, après être rendus analogiques par un convertisseur numérique analogique, ils sont soumis ou non soumis à une inversion de spectre.

La fréquence du signal porteur par rapport auquel est effectuée l'inversion de spectre est la même que celle du signal servant à la synchronisation des générateurs de code pseudo-aléatoire.

A la réception, les signaux analogiques sont numérisés par un convertisseur analogique numérique, puis les données obtenues sont mises en mémoire par paquets. Sous la commande du générateur de code pseudo-aléatoire, on effectue la permutation inverse de celle ayant servi à l'émission, puis les bits des paquets sont écrits en mémoire, soit dans l'ordre normal de la numérisation, soit dans

l'ordre inverse, selon qu'à l'émission, la lecture a été faite dans le sens direct ou dans le sens inverse. Enfin, une inversion de spectre est faite ou non sur les données redevenues analogiques selon qu'une inversion de spectre avait eu lieu ou non à l'émission.

Si l'on suppose qu'il y a N = 8 paquets par trame, et que les trames ont une durée T de 53,33 ms, le nombre de permutations de paquets est N ! = 8 ! = 40320 et comme chaque paquet peut être lu directement ou inversement et subir ou non une inversion de spectre, le nombre de combinaisons est :

$$2 \times 2 \times 8 ! = 161\ 280$$

Au cours d'une conversation par radiotéléphone d'une durée de 20 s, le nombre de combinaisons de cryptage est :

$$161\ 280 \quad \frac{20}{53{,}33 \times 10^{-3}} \approx 60 \times 10^{6}$$

L'invention va être maintenant décrite en détail, en relation avec les dessins annexés dans lesquels :

- la Fig. 1 représente le dispositif de cryptage à l'émission ;
- la Fig. 2 représente le dispositif de décryptage à la réception ; et
- la Fig. 3 représente un inverseur de spectre analogique.

En se référant à la Fig. 1, le signal de parole ayant une largeur de bande d'environ 300 - 3 300 Hz est capté par un microphone 1 et numérisé dans un convertisseur analogique numérique tel que, par exemple, un modulateur Δ, 2, suivi d'un filtre adapté 3. Le modulateur 2 est piloté par une horloge principale 4 à la fréquence de f_E = 32 kbits/s.

Le flux numérique de parole est découpé en trames de 53,3 ms composées de huit paquets de 213 bits d'une durée de 6,66 ms, et les paquets sont mémorisés dans la mémoire primaire 5 par l'intermédiaire d'un microprocesseur 6.

Un générateur de code pseudo-aléatoire 7 est également relié au microprocesseur 6. Ce dernier est piloté par une horloge de microprocesseur 8 à la fréquence de f_H = 3,2 Mhz. La fréquence

f_E est déduite de la fréquence f_H par le diviseur de fréquence 9 ayant un facteur de division de 100.

Les paquets mis en mémoire dans la mémoire 5 sont permutés sous la commande du générateur de code pseudo-aléatoire 7 via le microprocesseur 6. Les paquets permutés sont mémorisés dans la mémoire secondaire 10, puis ils sont convertis en signaux analogiques par un convertisseur numérique analogique 11, par exemple un démodulateur Δ^{-1}, suivi d'un filtre passe-bas 12.

Un modem à cadence basse (150 bits par seconde) 13 utilisant une porteuse modulée APSK (Amplitude Controlled Phase Shift Keying) à bande étroite réalise les fonctions suivantes :

- synchronisation entre émetteur et récepteur avec maintien de cette synchronisation pendant les périodes de fading des voies à radio-fréquence ;
- transmission de données à cadence basse (cette fonction n'est pas directement utilisée dans la présente invention).

La fréquence f_0 du modem est la fréquence par rapport à laquelle se fait l'inversion de spectre. Pour une bande passante 300 - 3 300 Hz, f_0 = 3 600 Hz.

Le générateur de code pseudo-aléatoire 7 est un registre à décalage 71 à cinq bits convenablement bouclé. Les générateurs de code pseudo-aléatoire sont bien connus dans la technique et sont par exemple décrits dans l'ouvrage "Theory and Application of Digital Signal Processing" par Lawrence R. RABINER et Bernard GOLD, pages 565-567.

Les bits 1, 2 et 3 sont utilisés pour la permutation des paquets dans la trame. Le bit 4 est utilisé pour commander l'inversion de spectre et le bit 5 est utilisé pour commander l'inversion de lecture des paquets dans la mémoire 10. Le registre 71 avance à la fréquence de trame de 18,75 Hz.

Les signaux analogiques de parole cryptés et la porteuse f_0 sont additionnés dans la porte analogique ET, 14. Le signal résultant est appliqué à l'inverseur de spectre 15. Ce dernier inverse donc le spectre 300 - 3 300 Hz par rapport à la fréquence 3 600 Hz, c'est-à-dire que les composantes aux fréquences 300 Hz et

3 300 Hz deviennent respectivement les composantes aux fréquences 3 300 Hz et 300 Hz.

L'inverseur de spectre 15 est relié à la borne de sortie du dispositif de cryptage d'émission. Cette borne 16 est reliée soit à une ligne d'abonné, soit à une voie à radio-fréquence.

En se référant maintenant à la Fig. 2, le signal analogique émis par le dispositif de cryptage de la Fig. 1 est appliqué à la borne d'entrée 46 du dispositif de décryptage et de là, par l'intermédiaire d'un inverseur de spectre 45, à un convertisseur analogique numérique 32 suivi d'un filtre passe-bas 33 et à un modem 43. Le convertisseur analogique numérique 32 peut être un modulateur Δ.

Le signal de sortie du modem à la fréquence f_0 est appliqué à un oscillateur commandé par tension, VCO 47 réglé sur f_H et à l'inverseur de spectre 45. La sortie du VCO 47 pilote à la fréquence f_E le convertisseur analogique numérique 32 par l'intermédiaire d'un diviseur de fréquence 39.

Le filtre 33, l'oscillateur commandé par tension 47, le générateur de code pseudo-aléatoire 37 et la mémoire primaire 35 sont reliés à un microprocesseur 36. Celui-ci est relié à une mémoire secondaire 40, à un convertisseur numérique analogique 41, par exemple, au démodulateur Δ^{-1} et à l'inverseur de spectre 45. Ce dernier reçoit du microprocesseur 36 les commandes d'inversion ou de non-inversion et du modem 43 la porteuse à la fréquence f_0.

On aperçoit qu'il existe un grand parallélisme entre dispositif de cryptage et dispositif de décryptage. Sous la commande des cinq bascules du registre à décalage 371 monté en générateur de code pseudo-aléatoire, le dispositif de décryptage effectue une permutation des paquets, inverse de la permutation ayant eu lieu à l'émission, met en mémoire les bits des paquets dans le sens direct ou dans le sens inverse et contrôle l'inversion de spectre.

La sortie du dispositif de décryptage est reliée à un écouteur 31.

La Fig. 3 représente un circuit qui peut être utilisé comme inverseur de spectre. Il comprend un amplificateur différentiel

constitué des transistors 151 et 152 dont les émetteurs sont interconnectés aux bornes d'une source à courant constant 153. Un tel circuit est connu dans la technique et est par exemple décrit dans l'ouvrage "Differential Amplifiers" par L.J. GIACOLETTO, Ed. WILEY-INTERSCIENCE, page 71, Fig. 5.2.

L'émetteur du transistor 151 est relié à la sortie de la porte ET 14 et l'émetteur du transistor 153 est relié au modem 13. La commande d'inversion ou de non inversion de spectre s'effectue grâce au transistor 154 qui courcircuite ou non le transistor 153. L'inverseur de spectre est relié à un filtre passe-bas 155 dont la sortie 16 est la sortie du dispositif de cryptage.

Bien que le système de cryptage et de décryptage de l'invention ait été décrit d'après un exemple de réalisation, il reste entendu que des variantes sont possibles sans sortir du domaine de l'invention tel que défini par les revendications. Notamment, le générateur de code pseudo-aléatoire comprend trois bits pour la permutation des paquets dans la trame. On pourrait bien entendu consacrer 4 ou plus de 4 bits à la permutation de paquets, ce qui augmenterait le nombre de combinaisons possibles.

REVENDICATIONS

1 - Système de cryptage et de décryptage de signaux clairs analogiques à bande étroite comprenant, dans des stations d'émission et de réception, des moyens (2, 32) de numériser un signal analogique entrant, respectivement clair et crypté, et de diviser les données résultantes en trames d'un nombre prédéterminé de bits, chaque trame étant divisée en un certain nombre de paquets d'un nombre déterminé de bits, lesdites stations d'émission et de réception comprenant en outre

un générateur de code pseudo-aléatoire (7, 37) dans chaque station,

des moyens (13, 43) de synchroniser les deux générateurs de code pseudo-aléatoire l'un avec l'autre, et

des moyens de permutation des paquets d'une trame,

caractérisé en ce que

ledit système comprend en outre des moyens (15, 45) d'inverser en synchronisme le spectre des signaux émis et reçus, et que les générateurs de code pseudo-aléatoire (7, 37) ont un cycle de (N+1) bits aléatoires dont N bits servent à commander la permutation des paquets et un bit commande l'inversion de spectre.

2 - Système de cryptage et de décrytage conforme à la revendication 1, caractérisé en ce qu'il comprend en outre des moyens de lire les paquets dans le sens allant du début de chaque paquet à sa fin ou en sens inverse, et que les générateurs de code pseudo-aléatoire ont un cycle de (N+2) bits aléatoires dont N bits commandent la permutation des paquets, un bit commande l'inversion de spectre et un bit commande l'inversion du sens de lecture.

3 - Système de cryptage et de décryptage conforme à la revendication 1, dans lequel les moyens de synchronisation des générateurs de code pseudo-aléatoire comprennent des moyens d'envoyer un signal à fréquence audio de la station d'émission à la station de réception et une boucle de verrouillage de phase dans la station de réception, caractérisé en ce que cette fréquence audio (f_0) est la même que celle servant à l'inversion de spectre.

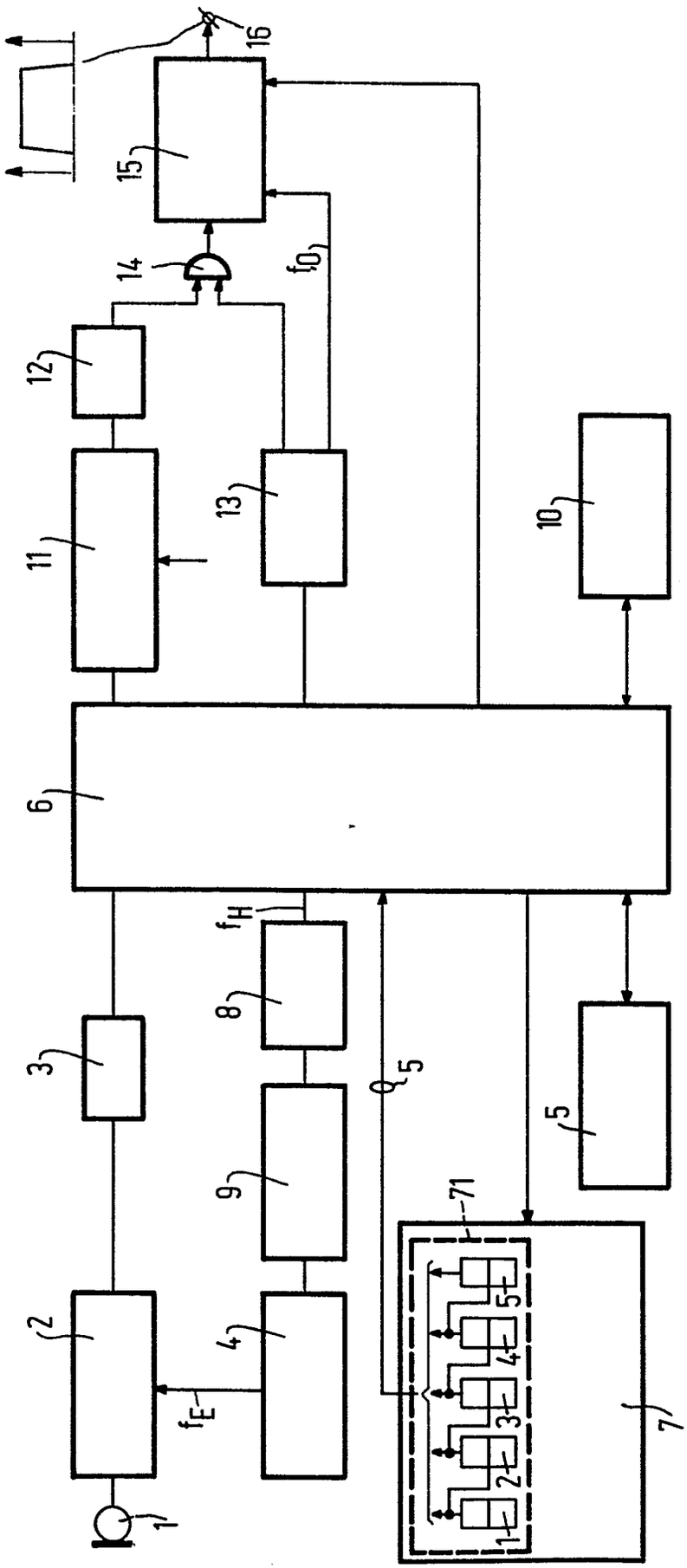

FIG.1

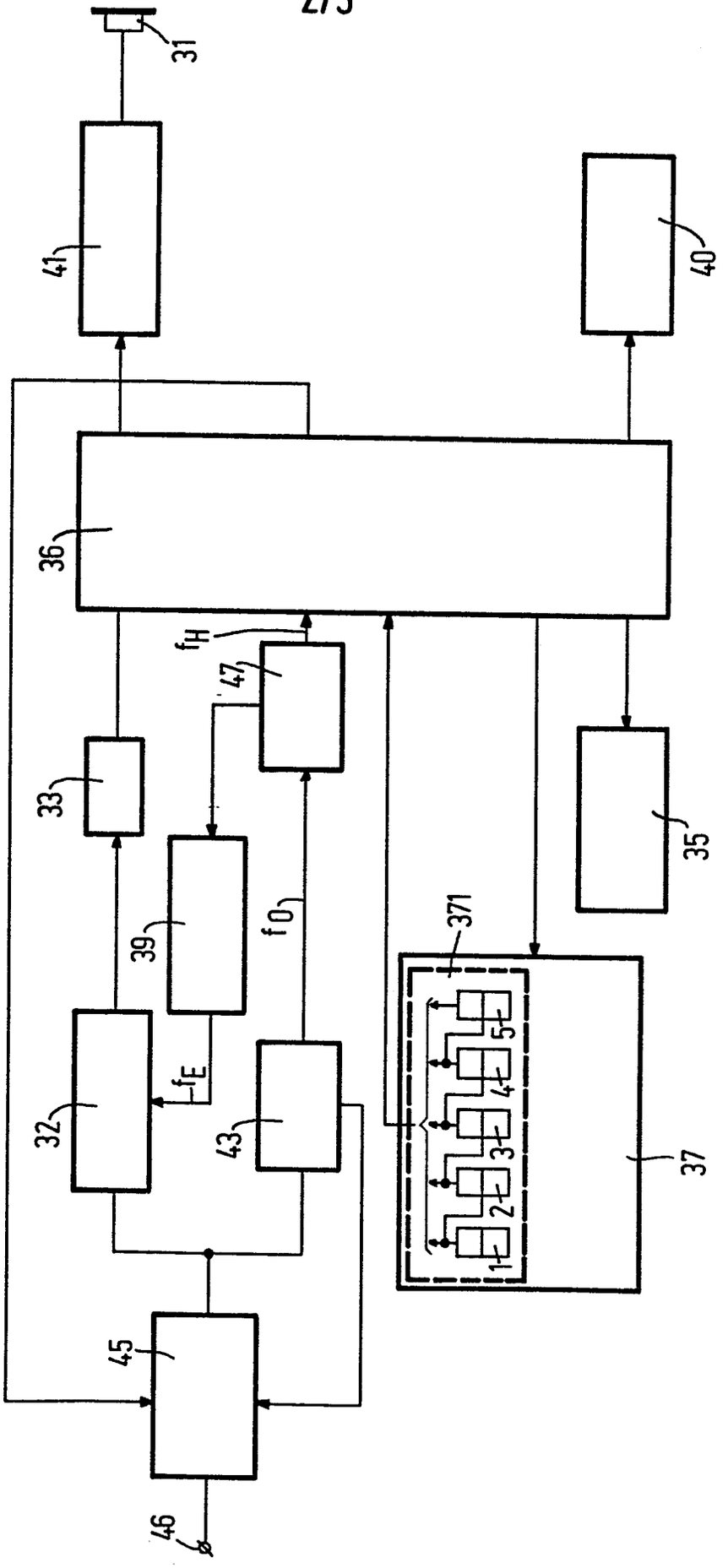

FIG.2

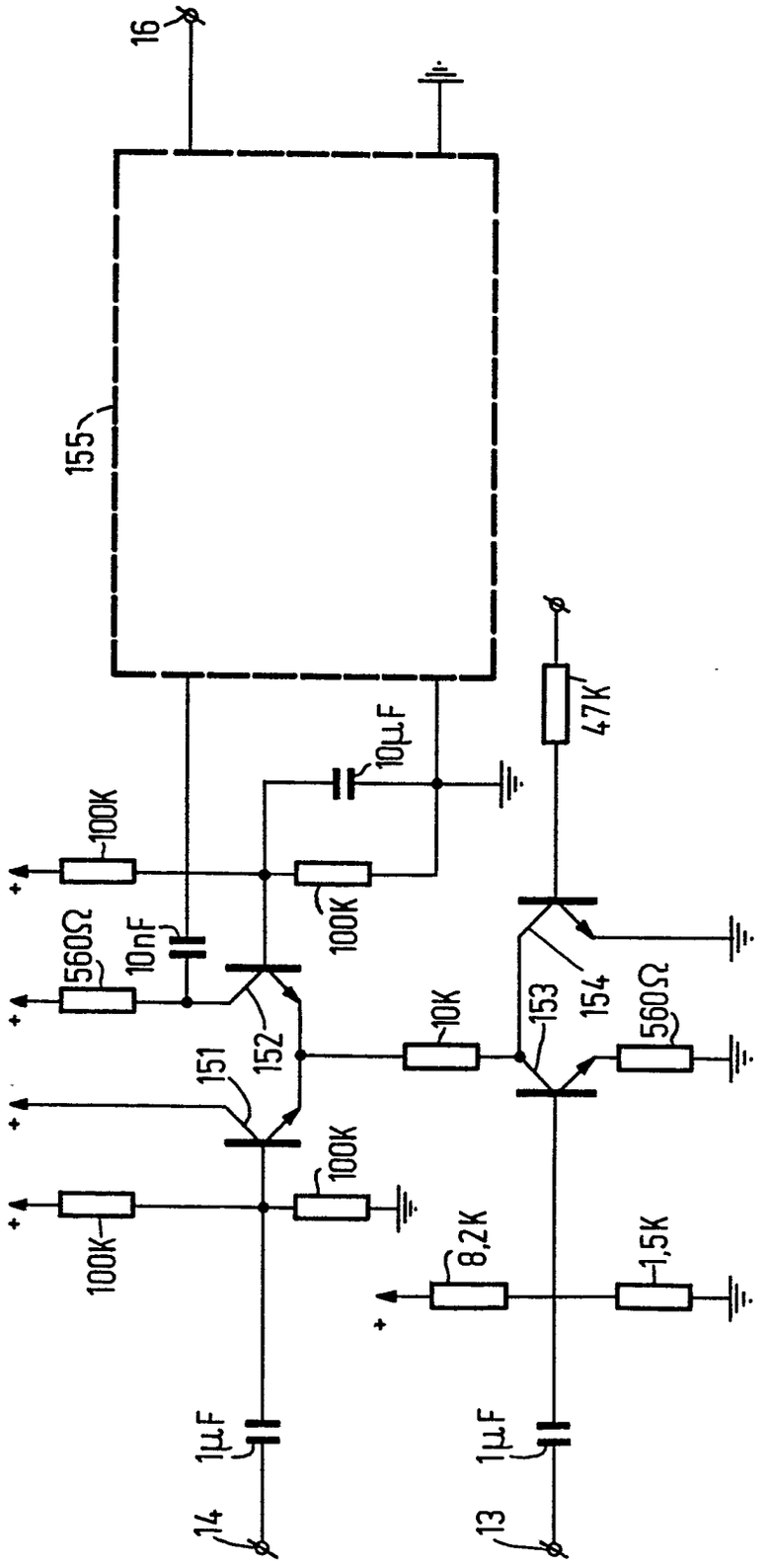
16
155
10µF
100K
100K
47K
560Ω
10nF
10K
153
154
560Ω
151
152
100K
100K
8,2K
1,5K
1µF
1µF
14
13

FIG.3

Office européen des brevets

0156428
Numéro de la demande

RAPPORT DE RECHERCHE EUROPEENNE

EP 85 20 0353

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)
X	PROCEEDINGS OF THE 1980 CARNAHAN CONFERENCE ON CRIME COUNTERMEASURES, 14-16 mai 1980, Lexington, Kentucky, pages 27-37; S. UDALOV: "Analog voice privacy with a microprocessor" * Page 31, colonne de droite, lignes 30-37; page 34, colonne de gauche, premier alinéa; page 35, colonne de gauche, dernier alinéa - colonne de droite, ligne 14 *	1	H 04 K 1/00
A	IDEM	2	

A	WO-A-8 301 717 (TECHNICAL COMMUNICATIONS) * Page 6, ligne 24 - page 7, ligne 21; page 9, lignes 18-27; page 10, ligne 35 - page 11, ligne 23, lignes 29-33 *	1,2	DOMAINES TECHNIQUES RECHERCHES (Int. Cl.4)
	---		H 04 K
A	INTERNATIONAL CONFERENCE ON COMMUNICATIONS, ICC '80, CONFERENCE RECORD, 8-12 juin 1980, Seattle, WA., vol. 1, pages 16.6.1 - 16.6.5, IEEE, New York, US; N.S. JAYANT et al.: "A comparison of four methods for analog speech encryption" * Page 16.6.1, colonne de droite, lignes 1-26 *	1	
	--- -/-		

Le présent rapport de recherche a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	14-06-1985	HOLPER G.E.E.

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

OEB Form 1503 03.82

RAPPORT DE RECHERCHE EUROPEENNE

EP 85 20 0353

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	FR-A-2 530 101 (THOMSON-BRANDT) * Page 3, lignes 11-20; figures 12,13 *	1,3	

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.4)

Le présent rapport de recherche a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	14-06-1985	HOLPER G.E.E.

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

OEB Form 1503 03.82