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

(11) Numéro de publication: **0 018 869**
A1

(12) DEMANDE DE BREVET EUROPEEN

(21) Numero de dépôt: 80400476.0

(51) Int. Cl.³: H 04 K 1/06

(22) Date de dépôt: 09.04.80

(30) Priorité: 20.04.79 FR 7910092

(43) Date de publication de la demande:
12.11.80 Bulletin 80/23

(84) Etats Contractants Désignés:
BE CH DE GB IT LI NL SE

(71) Demandeur: **Etablissement Public Telediffusion de France**
10, rue d'Oradour-sur-Glane
F-75732 Paris Cedex 15(FR)

(72) Inventeur: **Maillard, Michel**
27, rue Maurice Coutant
F-94200 Ivry(FR)

(72) Inventeur: **Lemaire, Jean**
10, rue Adolphe Petrement
F-93600 Aulnay-sous-Bois(FR)

(72) Inventeur: **Ruiz, Michel**
13, boulevard des Frères Voisin
F-75015 Paris(FR)

(72) Inventeur: **Akrich, Charles**
34, rue de la République
F-92190 Meudon(FR)

(74) Mandataire: **Martinet, René et al,**
Cabinet Martinet 62, rue des Mathurins
F-75008 Paris(FR)

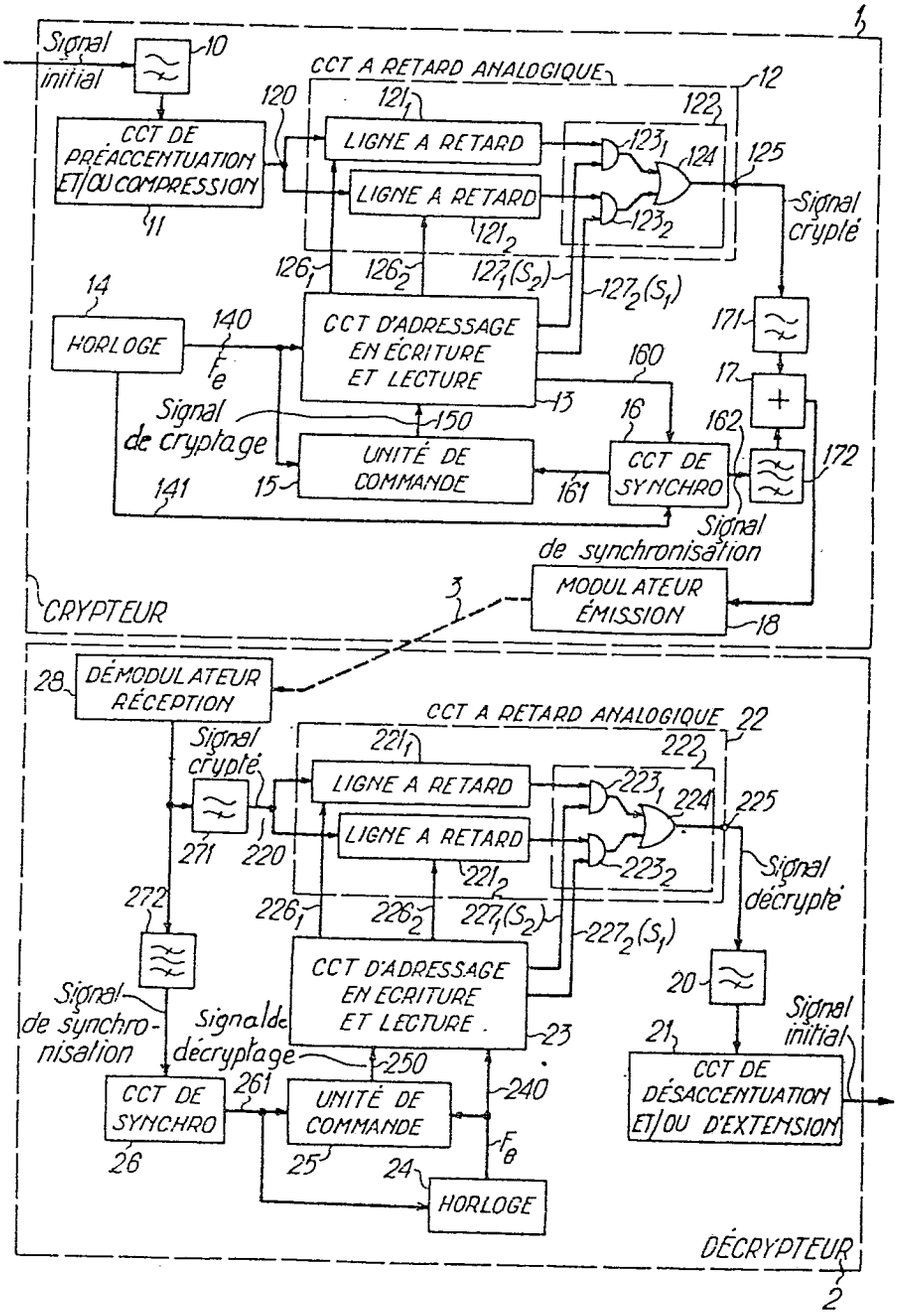
(54) Installation de cryptage et de décryptage d'un signal analogique par compressions et expansions temporelles.

(57) Dans l'installation, le crypteur (1) échantillonne le signal initial à période constante et produit un signal crypté par lecture des échantillons sous la commande d'un signal de cryptage ayant une période prédéterminée multiple de la période d'échantillonnage. Le décrypteur (2) effectue les opérations inverses des précédentes afin de restituer le signal décrypté analogue au signal initial. Le crypteur et le décrypteur comprennent des circuits à retard analogiques (11, 22). Dans le crypteur (1), le signal analogique initial est échantillonné et écrit à la cadence de la période d'échantillonnage pendant ladite période prédéterminée afin de remplir la totalité d'une ligne à retard analogique, puis les échantillons sont lus selon leur ordre initial à des instants ayant une répartition temporelle prédéterminée par le signal de cryptage et différente de celle répartie des instants d'ecriture précédents dans ladite période prédéterminée. Le signal crypté est ainsi obtenu par compressions et expansions temporelles des échantillons du signal initial. Des signaux de cryptage commandant ces compressions et expansions sont obtenus par modulation en impulsions de plusieurs signaux à ladite période prédéterminée, afin de permettre la sélection d'une pluralité de code de cryptage. L'installation peut être utilisée pour la réception sélective d'émissions spécialisées notamment radiophoniques.

./...

EP 0 018 869 A1

FIG.1


1
Signal initial
10
CCT A RETARD ANALOGIQUE
12
120
121_1
122_1
CCT DE PRÉACCENTUATION ET/OU COMPRESSION
11
LIGNE A RETARD
LIGNE A RETARD
123_1
124
125
123_2
121_2
Signal crypté
126_1
126_2
$127_1(S_2)$
$127_2(S_1)$
14
HORLOGE
140
f_e
CCT D'ADRESSAGE EN ÉCRITURE ET LECTURE
13
160
171
17
+
Signal de cryptage
150
16
162
172
141
15
UNITÉ DE COMMANDE
161
CCT DE SYNCHRO
Signal de synchronisation
CRYPTEUR
3
MODULATEUR ÉMISSION
18
28
DÉMODULATEUR RÉCEPTION
CCT A RETARD ANALOGIQUE
22
Signal crypté
221_1
222_1
LIGNE A RETARD
LIGNE A RETARD
223_1
224
225
223_2
221_2
271
220
Signal décrypté
272
226_1
226_2
$227_1(S_2)$
$227_2(S_1)$
CCT D'ADRESSAGE EN ECRITURE ET LECTURE .
23
20
Signal de synchro-nisation
Signal de décryptage
250
21
Signal initial
CCT DE DÉSACCENTUATION ET/OU D'EXTENSION
261
240
CCT DE SYNCHRO
UNITÉ DE COMMANDE
F_e
26
25
24
HORLOGE
DÉCRYPTEUR
2

INSTALLATION DE CRYPTAGE ET DE DECRYPTAGE D'UN SIGNAL ANALOGIQUE PAR COMPRESSIONS ET EXPANSIONS TEMPORELLES

La présente invention concerne une installation de cryptage et de décryptage d'un signal analogique dans lequel le crypteur, resp. le décrypteur, comprend des moyens du genre registres à décalage analogiques pour retarder 2N échantillons du signal entrant analogique initial, resp. crypté, des moyens pour produire des impulsions d'horloge à période T_e commandant l'écriture, resp. la lecture, de N échantillons successifs du signal entrant initial, resp. du signal sortant décrypté, et des moyens pour produire un signal de cryptage, resp. de décryptage, ayant N impulsions par période égale à NT_e, qui commandent la lecture, resp. l'écriture, de N échantillons du signal initial précédemment retardés et écrits dans le crypteur, resp. du signal entrant crypté avant d'être retardés et lus dans le décrypteur.

L'invention s'applique notamment au cryptage et au décryptage d'un signal à audiofréquence d'une émission radiophonique ou, plus généralement, au codage et décodage, chiffrement et déchiffrement, ou au brouillage et au débrouillage d'un signal analogique.

Actuellement, lorsqu'une chaîne de radiodiffusion ou de télévision désire transmettre une émission relative à un sujet bien spécifique adressée à une catégorie d'auditeurs particuliers, la transmission de cette émission doit être réalisée généralement la nuit, c'est-à-dire en dehors des heures à grande écoute du public. Comme peu d'auditeurs acceptent de rester à l'écoute la nuit, même si l'émission présente un intérêt certain, il est nécessaire de prévoir des récepteurs à enregistrement automatique des émissions, au moyen d'un magnétophone ou d'un magnétoscope, qui rendent les heures de réception des émissions pratiquement indépendantes des heures d'écoute des émissions par les auditeurs.

Cependant lorsqu'une émission spécialisée ne peut être écoutée que par des auditeurs spécialisés, tels que des médecins pour une émission médicale, il s'avère dangereux que d'autres auditeurs puissent

l'écouter. Pour ce faire, il est nécessaire de sélectionner les auditeurs en cryptant le signal à audiofréquence émis par l'émetteur de radiodiffusion ou de télévision selon une "clé" ou code de cryptage et en décryptant le signal à audiofréquence reçu par le récepteur de l'auditeur selon la "clé" ou code de décryptage correspondant à l'opération inverse du code de cryptage. Ces cryptage et décryptage doivent pouvoir être appliqués à des signaux analogiques tels que des signaux de parole et des signaux musicaux.

Les installations de cryptage et de décryptage faisant appel à un échantillonnage du signal analogique à des instants prédéterminés périodiques puis à un arrangement ou à un brouillage de ces échantillons sont déjà connues dans l'art antérieur. Tous les procédés de codages arithmétiques peuvent s'appliquer, les plus simples consistant en un codage selon une séquence pseudo-aléatoire ou selon des séquences de permutation d'un ou plusieurs échantillons.

Une installation de cryptage et de décryptage du genre défini dans l'entrée en matière est décrite dans le brevet américain 4.100.37(Les moyens de retard du crypteur, resp. du décrypteur, sont constitué: par deux registres à décalage analogiques à N étages dont les entrées des premiers étages reçoivent alternativement, pendant une période sur deux du signal de cryptage, resp. de décryptage, N échantillons du signal entrant initial, resp. crypté. Les 2N sorties d'étages des registres à décalage sont reliées à la sortie du crypteur, resp. du décrypteur, à travers un circuit de commutation analogique. Le circuit de commutation analogique joue le rôle d'un convertisseur parallèl(série et est commandé par le signal de code de cryptage, resp. de décryptage, afin de sélectionner alternativement, pour deux périodes consécutives NT_e, les N sorties de l'un des registres puis les N sortie: de l'autre registre. Pendant chaque période NT_e, les N sorties d'un registre à décalage sont sélectionnées selon un ordre prédéterminé, de manière à lire selon un ordre différent les échantillons précédemment écrits. Ceci revient à effectuer une permutation, à une même fréquenc de lecture que celle d'écriture $1/T_e$. Le signal de cryptage adresse ainsi les N sorties d'un registre selon une permutation prédéterminée

et à une fréquence constante de lecture.

Dans le décrypteur, pour reconstituer le signal analogique initial, le signal de décryptage doit être constitué d'une suite de mots d'adresse selon la permutation complémentaire à celle de cryptage. Il en résulte que, dans une telle installation, les moyens pour produire le signal de cryptage dans le crypteur et les moyens pour produire le signal de décryptage sont nécessairement différents. En outre, le fait qu'il est nécessaire d'adresser les sorties des registres selon un ordre prédéterminé différent de l'ordre initial d'écriture et d'échantillonnage du signal initial, complique singulièrement la logique de l'installation. De telles dispositions confèrent un prix de revient de l'installation relativement élevé, ce qui restreint le nombre d'auditeurs susceptibles d'acquérir un décrypteur pour des émissions spécialisées, ces auditeurs n'étant pas, à priori, des professionnels avertis.

La présente invention a pour but de fournir une installation de cryptage et de décryptage du genre défini dans l'entrée en matière qui est affranchie des inconvénients ci-dessus par le fait que les échantillons analogiques du signal initial ont leur ordre conservé dans le signal analogique crypté et subissent au moins une compression temporelle pour chaque période du signal de code, lequel est utilisé aussi bien pour le cryptage que pour le décryptage. La répartition des échantillons analogiques dans le signal crypté fluctue d'une manière analogue à un effet de pleurage sans pour cela que l'ordre initial des échantillons soit modifié.

A cette fin, une installation de cryptage et de décryptage telle que définie dans l'entrée en matière est caractérisée en ce que les N impulsions des périodes NT_e des signaux de cryptage et de décryptage ne sont pas équirépartis temporellement, et en ce que, pendant une période NT_e tous les échantillons écrits régulièrement dans le crypteur sont lus en série selon leur ordre initial en subissant au moins une compression temporelle et éventuellement une expansion temporelle partielle de leur répartition sous la commande des N impulsions d'une période du signal de cryptage, et tous les N échantillons du signal crypté entrant dans le décrypteur sont écrits en série d'une manière identique

à la lecture dans le crypteur.

La fonction de retard ou de compression et expansion temporelles du signal initial ou crypté est réalisée au moyen de deux lignes à retard comportant des registres à décalages analogiques tels que des circuits à transfert de charge, connus sous le sigle américain C.T.D. (" charge tranfer device").

Selon une première réalisation, les entrées des premiers étages des deux lignes à retard du crypteur, resp. du décrypteur sont reliées pour recevoir le signal analogique initial, resp. crypté. Les sorties des derniers étages des deux lignes à retard sont connectées à la sortie du crypteur, resp. du décrypteur, alternativement pendant une période sur deux du signal de cryptage, resp. de décryptage à travers des moyens de commutation analogiques. Chaque période du signal de code pour le cryptage et le décryptage correspond à la durée de remplissage de tous les étages d'une ligne à retard pendant laquelle sont écrits dans le crypteur, resp. sont lus dans le décrypteur les échantillons du signal initial, resp. décrypté. Pendant une période du signal de code, l'une des deux lignes à retard est commandée en écriture dans le crypteur au rythme de la période des impulsions d'horloge d'écriture, resp. dans le décrypteur au rythme des N instants d'écriture du signal de code selon ladite répartition prédéterminée, tandis que l'autre ligne à retard est commandée en lecture dans le crypteur au rythme des N instants de lecture du signal de code selon ladite répartition prédéterminée, resp. dans le décrypteur au rythme de la période des impulsions d'horloge de lecture. Les commandes en lecture et écriture précédentes sont inversées relativement aux deux lignes à retard pendant la période suivante du signal de code relatif au cryptage, resp. au décryptage.

Selon une seconde réalisation, dans le crypteur, resp. le décrypteur, une première ligne à retard à l'entrée de son premier étage recevant continûment le signal analogique initial, resp. crypté et a ses N sorties d'étages respectivement reliées en parallèle aux N entrées d'étages de la seconde ligne à retard dont la sortie du dernier étage est reliée à la sortie du crypteur, resp. du décrypteur. Pendant chaque période du signal de code, la première ligne à retard est commandée en

écriture dans le crypteur au rythme de la période des impulsions d'horloge d'écriture, resp. dans le décrypteur au rythme des N instants d'écriture du signal de code selon ladite répartition prédéterminée, tandis que la seconde ligne à retard est commandée en lecture dans le crypteur au rythme des N instants de lecture du signal de code selon ladite répartition prédéterminée, resp. dans le décrypteur au rythme de la période des impulsions d'horloge de lecture. Les première et seconde lignes à retard sont commandées simultanément en lecture et en écriture à la fin de chaque période du signal de cryptage, resp. de décryptage pour transférer en parallèle les N échantillons analogiques de la première dans la seconde ligne à retard.

Les moyens pour produire en synchronisme les signaux de cryptage et de décryptage qui sont identiques, sont fondés de manière générale sur la modulation en impulsions d'un signal prédéterminé. Cette modulation peut être du type en position ou en fréquence et la fréquence du signal de modulation peut être également programmable. Selon une autre variante moins complexe, les moyens de production du signal de cryptage ou de décryptage sont des multiplicateurs ou diviseurs de fréquence programmable. La sélection de ces différents moyens et de la fréquence programmable permet d'engendrer une pluralité de codes, chacun desquels étant attribué à une émission spécialisée. Comme en général la modulation en impulsions produit un nombre d'impulsions supérieur au nombre d'échantillons analogiques pendant une période du signal de cryptage et de décryptage, un compteur compte les N premières impulsions du signal de code au début de chaque période et bloque la transmission des impulsions suivantes jusqu'au début de la période suivante. Par suite, N échantillons du signal crypté sont toujours compressés temporellement pour une période NT_e du signal de code. Cependant l'intervalle temporel entre deux échantillons successifs d'une même période peut être plus petit que T_e. En fonction de la modulation sélectionnée, les échantillons du signal crypté dans une période NT_e peuvent être suivis d'un intervalle de silence plus ou moins long. Par ailleurs, on notera que le signal crypté est propre à être convoyé par une voie de transmission entre le crypteur et le décrypteur qui peut être du type par

câbles, par voie hertzienne, par fibres optiques, par diffusion directe, telle que par l'intermédiaire d'un satellite, ou par tout autre type de diffusion, et le signal décrypté présente toujours des caractéristiques de qualité d'écoute correctes.

D'autres avantages de la présente 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 d'une installation de cryptage et de décryptage conforme à l'invention incluant une organisation de lignes à retard analogiques selon la première réalisation ;
- la Fig. 2 est un diagramme temporel montrant l'élaboration des différents signaux d'adressage en lecture et en écriture des lignes à retard ;
- la Fig. 3 est un bloc-diagramme du circuit d'adressage en écriture et en lecture des lignes à retard du crypteur ou du décrypteur selon la première réalisation ;
- la Fig. 4 est un bloc-diagramme de l'unité de commande du crypteur ou du décrypteur ;
- la Fig. 5 est un bloc-diagramme du circuit de synchronisation du crypteur ; et
- la Fig. 6 est un bloc-diagramme du circuit à retard et du circuit d'adressage en écriture et en lecture du crypteur ou du décrypteur selon la seconde réalisation.

Telle que représentée à la Fig. 1, l'installation de cryptage et de décryptage conforme à l'invention comprend à l'émission un crypteur 1 et à la réception un décrypteur 2. La sortie du crypteur 1 est reliée à l'entrée du décrypteur 2 à travers une voie de transmission 3.

L'entrée du crypteur 1 reçoit le signal analogique initial à crypter. Ce signal est un signal de parole et/ou un signal musical, et est transmis par un magnétophone ou la bande audio d'un magnétoscope de la chaîne d'enregistrement d'un studio d'une station radiophonique ou de télévision par exemple. Un filtre passe-bas 10 filtre le signal analogique initial dans une bande de fréquence basse qui s'étend jusqu'à 8 kHz, par exemple. Le signal filtré est transmis éventuellement à un circuit de préaccentuation et/ou de compression 11 dont la sortie est reliée à

l'entrée 120 d'un circuit à retard analogique 12. Le circuit 11 contribue à améliorer les performances du crypteur en masquant les défauts éventuels dus aux échantillonnages et aux commutations inhérentes au cryptage. Le rapport signal/bruit est également augmenté grâce au circuit 11.

Selon une première réalisation, le circuit à retard 12 est constitué par deux lignes à retard analogiques 121_1, 121_2 qui sont connectées en parallèle, et par un circuit de commutation analogique 122. Les entrées communes 120 des lignes à retard 121_1, 121_2 sont reliées à la sortie du circuit de préaccentuation et/ou de compression 11. Les sorties des derniers étages des lignes à retard 121_1, 121_2 sont reliées respectivement aux deux entrées analogiques de deux portes ET analogiques 123_1 et 123_2 qui sont incluses dans le circuit 122. Les autres entrées des portes ET 123_1 et 123_2 reçoivent respectivement deux signaux complémentaires de lecture S_2 et $S_1 = \overline{S}_2$ qui sont transmis sur les fils 127_1 et 127_2 par un circuit d'adressage en écriture et lecture 13 afin d'ouvrir consécutivement ces portes pendant une durée NT_e. Cette durée NT_e est égale à la période des signaux de code de cryptage et de décryptage. Les sorties des portes ET analogiques 123_1 et 123_2 sont reliées aux entrées d'une porte OU analogique 124 dont la sortie 125 transmet le signal crypté.

Les deux lignes à retard 121_1 et 121_2 sont identiques et retardent chacune le signal analogique initial d'une durée NT_e. Conformément à l'invention, chaque ligne à retard analogique est un circuit intégré à transfert de charges ou est composée de plusieurs circuits intégrés à transfert de charges connectés en série. Bien qu'on se réfère dans la suite à une telle connexion en série, les circuits à transfert de charge d'une ligne à retard peuvent être connectés en parallèle ou en série-parallèle. Ces circuits intégrés sont connus sous le sigle C.T.D. ("charge tranfer device") et sont du type à éléments à chapelet ou à chaînes à saut, connus sous le sigle B.B.D. ("bucket brigade device" selon la dénomination américaine). Par exemple chaque ligne à retard analogique 121_1, 121_2 comprend P registres à décalage analogiques. Chaque registre est constitué de 512 étages série du type B.B.D. Le fonctionnement d'un registre analogique est tel que, à chaque période T_e

commandant l'écriture d'un échantillon dans le crypteur, qui est égale par exemple à 0,05 ms et qui est transmise sous la forme d'un signal d'horloge à fréquence constante $F_e = 1/T_e$ sur le fil respectif 126_1, 126_2 par une horloge 14 à travers le circuit d'adressage 13, un échantillon du signal analogique initial prélevé à l'entrée 120 soit décalé de deux étages vers la sortie de la ligne à retard 121_1, 121_2. Ainsi, le retard apporté par un registre à 512 étages est égal à 512 x 0,05 / 2 ms. Chaque ligne à retard retarde le signal analogique d'une durée qui est inférieure à deux fois la durée dite d'écriture $NT_e = (P \times 512 / 2) \times 0,05ms$ de N échantillons, et qui dépend de la fréquence de lecture, c'est-à-dire du code de cryptage sélectionné, comme on le verra dans la suite.

Comme montré à la Fig. 2, les signaux complémentaires de commande de lecture (ou d'écriture) S_1 et S_2 transmis par le circuit d'adressage 13 aux portes 123_2 et 123_1 ont une période égale à 2 NT_e. Les signaux impulsionnels transmis sur les fils de sortie 126_1 et 126_2 par le circuit d'adressage commandent l'avance pas-à-pas d'un échantillon dans les lignes à retard en phase de lecture et ont également une période égale à 2 NT_e. L'un d'eux, tel que celui sur le fil 126_1, est composé pendant une première demi-période NT_e par N impulsions à la période constante T_e qui commandent l'échantillonnage et l'écriture dans la ligne à retard 121_1. Pendant la seconde demi-période suivante NT_e, il est composé par N impulsions qui commandent la lecture des N échantillons écrits dans la ligne à retard 121_1 et qui ne sont pas équiréparties temporellement. En d'autres termes, les impulsions de lecture ont une répartition temporelle déterminée par le code de cryptage et différente de celle régulière des impulsions d'écriture précédentes. L'autre signal impulsionnel sur le fil 126_2 est composé pendant la première demi-période précédente NT_e par N impulsions qui ont ladite répartition temporelle déterminée et qui commandent la lecture de N échantillons dans la ligne à retard 121_2, et est composé pendant la seconde demi-période précédente NT_e par N impulsions qui sont équiréparties à la période constante T_e et qui commandent l'écriture de N échantillons dans la ligne à retard 121_2.

Il apparaît que sous la commande du circuit d'adressage 13,

lorsque la première ligne à retard 121_1 est en phase d'écriture pendant une demi-période de lecture NT_e pour laquelle les échantillons du signal initial entrant avancent à la période dite d'écriture T_e, la seconde ligne à retard 121_2 est en phase de lecture pour laquelle les échantillons du signal initial entrant, précédemment retardés, avancent à des instants successifs t_1 à t_N distribués selon le code de cryptage pendant la même demi-période NT_e. Pendant la demi-période NT_e suivante, les phases de lecture et d'écriture précédentes sont inversées : la première ligne à retard 121_1 est en phase de lecture et la seconde ligne à retard 122_2 est en phase d'écriture.

Les instants de lecture successifs t_1 à t_N sont élaborés selon un code de cryptage sélectionné par une unité de commande 15 éventuellement en dépendance du signal d'horloge à la fréquence F_e sur le fil 140. L'unité 15 transmet via le bus 150 les impulsions aux instants t_1 à t_N pendant chaque durée NT_e au circuit d'adressage 13. Une unité de synchronisation 16 reçoit sur deux fils de sortie 160 du circuit d'adressage 13 les signaux complémentaires de commande de lecture et d'écriture S_1 et S_2 pour produire des impulsions de synchronisation à la fréquence NT_e qui permettent de reconstituer convenablement le signal initial à partir du signal crypté dans le décrypteur 2. Les impulsions de synchronisation sont transmises sur le fil 161 vers l'unité de commande 15 et sont modulées convenablement, par un signal à une fréquence élevée transmis à travers le fil de sortie 141 par l'horloge 14, en un signal de synchronisation sur la sortie 162 du circuit 16.

Le signal crypté et le signal de synchronisation sont mélangés dans un mélangeur 17 après passage respectif à travers un filtre passe-bas 171 qui est analogue au filtre 10, et un filtre passe-bande 172 dont la bande passante est centrée sur la fréquence de modulation de synchronisation. Le signal composite issu de la sortie du mélangeur 17 est éventuellement transmis et mis en forme convenablement dans un modulateur d'émission 18 dépendant du mode de transmission de la voie 3 entre le crypteur 1 et le décrypteur 2.

A la réception dans le décrypteur 2, le signal composite traverse éventuellement un démodulateur de réception convenable 28, puis est

filtré. Un filtre passe-bas 271 qui est analogue au filtre 10, et un filtre passe-bande 272 qui est analogue au filtre 172, restituent le signal crypté et le signal de synchronisation, respectivement.

Le décrypteur 2 effectue la fonction inverse de celle du crypteur et comporte, d'une manière semblable aux circuits 12 à 16 du crypteur, des circuits 22 à 26. Un circuit à retard analogique 22 reçoit par son entrée 220 le signal crypté transmis par le filtre passe-bas 271, et restitue par sa sortie 225 le signal décrypté qui est analogue à celui reçu à l'entrée 120 du circuit à retard analogique 12 du crypteur 1. Un circuit d'adressage en écriture et lecture 23 commande alternativement en écriture et lecture les deux lignes à retard analogiques 221_1 et 221_2 du circuit 22, via les fils 226_1 et 226_2. Le circuit d'adressage 23 commande également, à travers les fils 227_1 et 227_2, alternativement au cours des lectures, les ouvertures de portes ET analogiques 223_1 et 223_2 du circuit de commutation analogique 222 qui est inclus dans le circuit 22. Le circuit 222 est identique au circuit 122 et comporte également une porte OU analogique 224 dont la sortie 225 transmet le signal décrypté. Une horloge 24 transmet un signal d'horloge à la fréquence constante F_e sur le fil 240 vers le circuit d'adressage 23 et une unité de commande 25. Cette unité 25 a enregistré préalablement le cod de décryptage qui est, conformément à l'invention, identique au code de cryptage sélectionné et transmet sur le fil 250 les impulsions d'écriture aux instants variables t_1 à t_N vers le circuit d'adressage 23. Les impulsions de synchronisation sont détectées dans un circuit de synchronisation 26 à partir du signal de synchronisation transmis par le filtre 272 et sont transmises sur le fil 261 vers l'unité de commande 25 et l'horlo 24. Le signal de synchronisation permet également de commander l'avance du support d'enregistrement chez l'auditeur, tel que la bande d'enregistrement d'un magnétophone par exemple (non représenté).

Le signal décrypté analogique analogue au signal analogique initial qui est reçu par l'entrée 120 du circuit à retard 12 dans le crypteur est transmis par la sortie 225 du circuit de commutation analogique 22 vers un filtre passe-bas 20 qui est analogue au filtre 10, puis éventuellement vers un circuit de désaccentuation et/ou d'extension 21 qui est

complémentaire du circuit 11. La sortie du circuit 21 commune à celle du décrypteur 2 restitue un signal analogique décrypté qui est analogue au signal analogique initial reçu à l'entrée du crypteur.

En se référant maintenant aux Figs. 3 et 4, on décrit en détail l'élaboration du cryptage du signal initial au moyen du circuit d'adressage 13 et de l'unité de commande 15.

Comme déjà dit, l'unité de commande 15 produit les N impulsions de lecture aux instants t_1 à t_N tels que, en général, $t_{i+1} - t_i \neq T_e$ avec $1 \leq i < N$. La répartition des N impulsions de lecture dans un intervalle de lecture NT_e est obtenue au moyen d'un circuit dit de modulation d'impulsions 151. Ce circuit 151 peut comprendre un ou plusieurs "modulateurs d'impulsions" ou "horloges de lecture à pas variable" 1510 qui sont programmables ou non et qui engendrent chacun une séquence d'impulsions de lecture ayant une durée NT_e.

Selon une première variante, un modulateur 1510 est un multiplicateur de fréquence programmable qui multiplie par un entier prédéterminé Q une fréquence de référence, par exemple la fréquence F_e transmise par l'horloge 14 sur le fil 140. Dans ce cas, les N impulsions de lecture sont à la fréquence $Q \times F_e$, comme montré à la ligne a de la Fig. 2 pour $Q = 3$. Selon une seconde variante, un modulateur 1510 est un "modulateur en impulsions" d'un signal périodique ou non, de préférence à enveloppe simple. Ce signal peut être un signal en dents de scie périodique comme montré à la ligne b de la Fig. 2 ou un signal périodique à plusieurs niveaux comme montré à la ligne c de la Fig. 2. Un tel signal est produit par un générateur de signal inclus dans le modulateur 1510. Le circuit de modulation inclus dans le modulateur 1510 fonctionne selon l'une des modulations en impulsions connues. Si la modulation est une modulation de position, c'est-à-dire si les positions temporelles des impulsions sont proportionnelles à l'amplitude du signal modulant, les impulsions de lecture sont réparties comme montré aux lignes b_1 et c_1 de la Fig.2. Lorsque la modulation est une modulation de fréquence, des suites d'impulsions à fréquences prédéterminées correspondent aux niveaux prédéterminés du signal modulant, comme montré aux lignes b_2 et c_2 de la Fig. 2. On notera que d'autres "modulations en impulsions"

1510 peuvent être facilement imaginables pour l'homme de l'art et peuvent résulter de la combinaison des variantes précédentes. En particulier, les modulateurs du type à dents de scie ou à multiniveau peuvent avoir la fréquence du signal de modulation programmable. En général, le crypteur et surtout le décrypteur comporteront un ou plusieurs "modulateurs d'impulsions" qui permettent d'engendrer chacun un signal crypté qui est, dans une large mesure, pratiquement incompréhensible.

Il apparaît que, conformément à l'invention, et quel que soit le type de modulation sélectionné, il y a toujours une compression temporelle des échantillons lus dans le crypteur 1, puisque tous les échantillons écrits dans les lignes à retard 121_1 , 121_2 sont lus et transmis. En d'autres termes, l'intervalle temporel $(t_N - t_1)$ est toujours inférieur à la période NT_e du signal de cryptage. Cependant, il peut exister une expansion temporelle entre au moins deux échantillons i, j d'une période NT_e, ce qui se traduit par $t_j - t_i > (j-i)\, T_e$.

Une telle expansion temporelle apparaît par exemple sur la Fig.2 à la ligne c_1, entre t_2 et t_1 ou entre t_4 et t_3 et à la ligne c_2, entre t_2 et t_1, bien que l'ont toujours $(t_N - t_1) < NT_e$.

Les modulateurs d'impulsions et/ou les fréquences du signal modulant de ceux-ci sont adressées par une mémoire morte de codes de cryptage 152 de l'unité de commande 15 montrée à la Fig. 4. Chaque cellule 1520 de la mémoire 152 contient l'adresse d'un modulateur 1510 et, si nécessaire, de l'une des fréquences de modulation. Cette mémoire de codes 152 est adressée, d'une manière connue, en lecture par un clavier alphanumérique 153 à travers un registre d'adresses de code 154 qui fait correspondre à chaque nombre identifiant un code de cryptage et transmis par le clavier 153, l'adresse d'une cellule 1520 de la mémoire 152. Lorsqu'un code de cryptage est sélectionné, le modulateur en impulsions 1510 adressé est mis sous tension et produit sur la sortie 1511 du circuit 151 à travers une porte OU 1512 les impulsions de lecture à des instants prédéterminés t_1 à t_N.

Cependant, afin que les N échantillons écrits précédemment dans une ligne à retard 121_1, 121_2 soient uniquement lus pendant la durée suivante NT_e, il est nécessaire d'inhiber les autres impulsions de rang

supérieur à N pendant cette durée. Par ailleurs, on notera que la fréquence de modulation et le procédé de modulation de chaque modulateur 1510 sont choisis de telle qorte qu'au moins N impulsions de lecture soient transmises à la sortie 1511 pendant NT_e afin de transmettre le signal initial échantillonné sans pertes d'information. Pour ce faire, l'unité de commande 15 comprend un compteur 155 de compte maximal N dont l'entrée de comptage est reliée à la sortie 1511 du circuit de modulation 151, et une porte ET 156 ayant ses entrées reliées à la sortie 1550 du compteur 155 et à la borne 1511. Le compteur 155 est remis à zéro (RAZ) chaque fois qu'il reçoit une impulsion de synchronisation qui est transmise sur le fil 161 par le circuit de synchronisation 16 et qui définit une transition entre les phases de lecture et d'écriture de durée NT_e relativement à chaque ligne à retard. Dès que le compte du compteur 155 est égal à N, le compteur 155 délivre sur sa sortie 1550 un signal qui ferme la porte ET 156 jusqu'à la prochaine remise à zéro, de sorte que N impulsions de lecture seulement traversent la porte ET 156 pendant une durée NT_e. Les N impulsions de lecture transmises sont représentées en traits pleins sur les lignes b_1, b_2, c_1 et c_2 de la Fig. 2, tandis que les impulsions suivantes, qui sont inhibées, sont représentées en traits pointillés. Si le modulateur sélectionné 1510 a un signal de modulation dont la fréquence n'est pas un multiple entier de la fréquence $1/NT_e$, l'impulsion de synchronisation sur le fil 161 est également transmise au modulateur sélectionné 1510 afin qu'il soit réinitialisé au début de chaque phase de lecture et d'écriture de durée NT_e pour produire un signal de modulation de période NT_e, comme montré aux lignes b et c de la Fig. 2.

Le circuit d'adressage 13 montré à la Fig. 3 produit le signal S_1 qui commande simultanément la mise en phase d'écriture de la ligne à retard 121_1 et la mise en phase de lecture de la ligne à retard 121_2. Le circuit d'adressage 13 produit également le signal S_2 qui commande la mise en phase de lecture de la ligne à retard 121_1 et la mise en phase d'écriture de la ligne à retard 121_2. Le signal S_1 est produit à la sortie d'un diviseur de fréquence par N 130, dont l'entrée reçoit les impulsions d'écriture à la fréquence constante F_e qui sont transmises par l'horloge

14 sur le fil 140. Le signal complémentaire $S_2 = \overline{S}_1$ est produit par la sortie d'un inverseur 131 reliée à la sortie du diviseur de fréquence 130.

Le circuit d'adressage 13 comporte également deux circuits logiques identiques permettant la transmission alternative des impulsions d'écriture et des impulsions de lecture vers les lignes à retard 121_1, 121_2. Chaque circuit logique est constitué par une première porte ET 132_1, 132_2 qui commande l'écriture dans la ligne à retard 121_1, 121_2, par une seconde porte ET 133_1, 133_2 qui commande la lecture dans la ligne à retard 121_1, 121_2 et par une porte OU 134_1, 134_2 dont les entrées sont reliées aux sorties des première et seconde portes ET 132_1, 133_1, resp. 132_2, 133_2 et dont la sortie commande à travers le fil 126_1, 126_2, l'avance des échantillons du signal initial dans la ligne à retard 121_1, 121_2. Deux entrées communes des portes ET 132_1 et 133_2 reçoivent le signal S_1 qui commande également l'ouverture de la porte ET analogique 123_2 du circuit de commande 122 via le fil 127_2. Deux entrées communes des portes ET 133_1 et 132_2 reçoivent le signal S_2 qui commande également l'ouverture de la porte ET analogique 123_1 du circuit de commutation 122 via le fil 127_1. Les autres entrées des portes dites d'écriture 132_1 et 132_2 reçoivent, à travers le fil de sortie d'horloge 140, les impulsions d'écriture à la fréquence constante F_e et commandent alternativement pendant les durées successives NT_e l'échantillonnage et l'écriture du signal initial dans les lignes à retard 121_1 et 121_2. Les autres entrées des portes dites de lecture 133_1 et 133_2 reçoivent, à travers le fil de sortie 150 de l'unité de commande 15, les impulsions de lecture et commandent, alternativement, pendant les durées successives NT_e la lecture et la transmission du signal crypté à partir des lignes à retard 121_1 et 121_2, à travers les portes ET analogiques 123_1 et 123_2 qui sont ouvertes alternativement et en correspondance avec les ouvertures des portes ET 132_1 et 133_2.

Le circuit de synchronisation 16 est montré schématiquement sur la Fig. 3. Il comprend une double bascule monostable 160 qui transmet sur le fil 161 une impulsion de synchronisation à chaque front montant des signaux complémentaires S_1 et S_2, c'est-à-dire au début de chaque durée

NT_e. A cet égard, les entrées de la bascule 163 sont reliées aux sorties du diviseur 130 et de l'inverseur 131, via le bus à deux fils 160. Le circuit de synchronisation 16 comporte également un modulateur en fréquence 164 dont l'entrée est reliée à la sortie de la bascule 163 et dont la sortie transmet le signal de synchronisation sur le fil 162 vers l'entrée du filtre passe-bande 172. Le modulateur 164 module par exemple en phase l'impulsion de synchronisation à une fréquence sous-porteuse de 15 kHz transmise par le fil de sortie 141 de l'horloge 14. Comme déjà dit, cette impulsion de synchronisation modulée est mélangée au signal crypté dans le mélangeur 17 du crypteur 1 et est détectée par le circuit de synchronisation 26 du décrypteur 2.

Sur les Figs. 3 et 4, on voit que les circuits d'adressage 13, 23 et les unités de commande 15, 25 respectivement dans le crypteur 1 et le décrypteur 2 ont des blocs-diagrammes respectivement identiques. Les numéros de référence indiqués entre parenthèses correspondent aux blocs et fils du décrypteur 2 montré à la Fig. 1. Le circuit de synchronisation 26 du décrypteur 2 est constitué essentiellement par un démodulateur en fréquence dont la sortie 261 transmet les impulsions de synchronisation à l'entrée de remise à zéro (RAZ) du compteur 155 et éventuellement à l'entrée de réinitialisation de certains "modulateurs d'impulsions" 1510 de l'unité de commande 25. Les impulsions de synchronisation sont également reçues dans l'horloge 24 en vue de caller la boucle d'asservissement en phase qu'elle contient à la fréquence F_e.

Lorsque l'auditeur désire enregistrer l'émission correspondant au code de cryptage sélectionné, il frappe le même numéro d'identification sur le clavier 153 du décrypteur 2, ce qui provoque, à travers le registre 154 et la mémoire de codes 152 du décrypteur, l'adressage et la mise sous tension du modulateur correspondant 1510 et, si celui-ci est programmable en fréquence, la sélection d'une fréquence du signal de modulation. Le modulateur sélectionné 1510 dans le décrypteur est identique à celui sélectionné dans le crypteur. En effet, le décrypteur doit reconnaître après chaque début d'un intervalle d'écriture NT_e les échantillons transmis par le crypteur aux instants de lecture successifs t_1 à t_N. Par conséquent, dans le décrypteur, les écritures du signal

crypté dans les deux lignes à retard analogiques 221_1 et 221_2 pendant des intervalles successifs de durée NT_e doivent être identiques à la lecture des échantillons dans les lignes à retard 121_1 et 121_2 du crypteur. La lecture dans le décrypteur est identique à l'écriture dans le crypteur et est rythmée à la fréquence constante F_e. Comme on le voit sur la Fig.3, pour ce qui concerne le circuit d'adressage 23 du décrypteur 2, les portes ET dites d'écriture, 132_1 et 132_2, reçoivent les impulsions d'écriture à répartition variable selon le code de cryptage qui sont transmises par la sortie 250 de l'unité de commande 25, tandis que les portes ET dites de lecture, 133_1 et 133_2, reçoivent les impulsions de lecture à fréquence constante F_e qui sont transmises par la sortie 240 de l'horloge 24.

D'autre part, du fait que le circuit de synchronisation 26 synchronise à travers le fil 261 les émissions des impulsions d'écriture transmises par le modulateur 1510 sélectionné et des impulsions de lecture transmises par l'horloge 24, le découpage du signal crypté et la reconstitution du signal initial dans le décrypteur sont commandés en synchronisme avec l'échantillonnage et la lecture du signal initial dans le crypteur.

Selon une seconde réalisation montrée à la Fig. 6, les deux lignes à retard analogiques $121'_1$, $121'_2$, resp. $222'_1$, $221'_2$ du circuit à retard 12', resp. 22' dans le crypteur 1, resp. le décrypteur 2 sont destinées respectivement à l'écriture et à la lecture. Dans la Fig. 6, les numéros de référence entre parenthèses représentent les composants inclus dans le circuit à retard 22' et le circuit d'adressage en écriture et lecture 23' du décrypteur qui sont identiques à ceux 12' et 13' du crypteur. On se réfère dans la suite au crypteur, sauf indication contraire.

L'entrée 120' du premier étage de la première ligne à retard $121'_1$ reçoit continûment le signal analogique initial. Cette ligne à retard échantillonne pendant chaque période NT_e le signal initial en N échantillons analogiques série au rythme du signal périodique d'écriture à la fréquence constante F_e qui est transmis sur le fil $126'_1$ par le circuit d'adressage 13'. A la fin de chaque période NT_e détectée par la double bascule monostable 163, cette dernière ouvre N portes ET analogiques $122'_1$ à $122'_N$ (resp. $222'_1$ à $222'_N$ pour le décrypteur) lors de la transmis-

sion d'une impulsion de synchronisation sur le fil 161 (resp. 261 pour le décrypteur). Les autres entrées des portes $122'_1$ à $122'_N$ sont reliées aux sorties des N paires d'étages de la première ligne à retard $121'_1$ et transmettent simultanément en parallèle les N échantillons mémorisés précédemment vers les entrées des N paires d'étages de la seconde ligne à retard $121'_2$. Au début de chaque période NT_e, la ligne à retard $121'_2$ est commandée en lecture aux instants t_1 à t_N selon la répartition prédéterminée du code sélectionné par le circuit d'adressage 13', via le fil $126'_2$. La sortie 126' du dernier étage de la ligne à retard $121'_2$ délivre ainsi le signal crypté comme selon la première réalisation.

Comme on le voit sur la Fig. 6, le circuit d'adressage 13' du crypteur est nettement plus simple. Il ne comporte plus que le diviseur de fréquence 130 transmettant le signal S_1, l'inverseur 131 transmettant le signal S_2 et deux portes ET telles que 132_1 et 133_1. Tous ces composants sont interconnectés d'une manière analogue à celle montrée à la Fig. 3.

La porte d'écriture 132_1 du circuit 13', resp. 23' transmet les impulsions dites d'écriture sur le fil $126'_1$ à la fréquence constante F_e reçue à partir de l'horloge 14 via le fil 140, dans le crypteur, resp. sur le fil $226'_1$ aux instants t_1 à t_N déterminés par les impulsions d'écriture reçues à partir de l'unité de commande 25 via le fil 250, dans le décrypteur. La porte de lecture 133_1 du circuit 13', resp. 23' transmet les impulsions dites de lecture sur le fil $126'_2$ aux instants t_1 à t_N déterminés par les impulsions de lecture reçues à partir de l'unité de commande 15 via le fil 150, dans le crypteur, resp. sur le fil $226'_2$ à la fréquence constante F_e reçue à partir de l'horloge 24 via le fil 240, dans le décrypteur.

On notera que, en pratique, les séquences de code récurrentes de durée NT_e sont choisies d'une part, pour obtenir un signal crypté complètement indéchiffrable et, d'autre part, pour reconstituer le signal analogique initial à partir du signal crypté avec un rapport signal/bruit élevé afin que la qualité d'écoute du signal décrypté soit voisine de celle du signal initial. Par ailleurs, le choix entre les différentes organisations des deux lignes à retard et également entre les types de modulateurs

en impulsions dépend de contraintes d'exploitation telles que le coût de fabrication du décrypteur, qui contrairement au crypteur, est réalisé en un grand nombre d'exemplaires.

Bien que l'invention ait été décrite selon des exemples préférés de réalisation illustrés de manière générale à la Fig. 1, d'autres réalisations, notamment en ce qui concerne la structure des unités de commande et des circuits d'adressage des lignes à retard peuvent être facilement imaginables par l'homme de métier sans sortir du cadre de l'invention défini par les revendications annexées.

Au moins l'une des unités de commande, 15 et 25, de préférence celle 25 du décrypteur, ne peut comporter qu'un seul modulateur en un diviseur de impulsions ou plus simplement un multiplicateur ou/fréquence synchronisée sur une fréquence d'horloge. Ce dernier circuit engendre une unique répartition temporelle des instants t_1 à t_N pendant une durée NT_e et peut être fabriqué sous la forme d'un circuit intégré qui est enfichable dans le bâti du décrypteur. Sa mise sous tension est commandée par un simple bouton-poussoir d'initialisation remplaçant le clavier. Ceci permet avantageusement de contrôler efficacement les écoutes d'une émission prédéterminée, puisque l'auditeur désirant écouter ou enregistrer cette émission devra se procurer un tel circuit. Complémentairement, cette sélection des auditeurs peut être réalisée par des décrypteurs incluant des lignes à retard d'un nombre prédéterminé d'étages inférieur à celui des lignes à retard du crypteur ce qui permet pour une émission prédéterminée d'être reçue par des décrypteurs ayant des lignes à retard dont le nombre d'étages est égal à celui véritablement utilisé dans les lignes à retard du crypteur. En effet, il est facile de sélectionner dans le crypteur des premiers étages d'une ligne à retard.

La transmission du signal composite issu du mélange du signal crypté et du signal de synchronisation dans le crypteur peut être réalisé comme déjà dit, par câble, par voie hertzienne ou par fibre optique ou analogue. Le signal analogique initial peut appartenir au domaine de la radiodiffusion, de la télévision, du téléphone, etc ... Lorsque le signa crypté est véhiculé dans un canal de fréquence de la voie de transmissic 3, le signal de synchronisation peut être mélangé au signal crypté dans

canal, ou moduler une onde sous-porteuse à fréquence audible, qui est mélangée au signal crypté, la sous-porteuse étant modulée par exemple en phase par le signal de synchronisation. Dans le cas d'un signal analogique initial à crypter transmis par un système de transmission d'images de télévision, le signal composite peut être transmis dans un canal classique de télévision, ou être multiplexé temporellement avec le signal vidéo par exemple en l'insérant convenablement dans les signaux de synchronisation et de suppression de ligne et/ou dans les signaux de synchronisation et de suppression de trame.

Enfin on notera que toute combinaison de moyens de cryptage selon l'invention et de moyens de décryptage connus en vue d'obtenir un signal crypté par compression et expansion temporelle d'un signal analogique échantillonné à période constante ou d'un signal analogique échantillonné dont les échantillons ont été préalablement mélangés périodiquement par permutation ou selon une séquence quelconque convenable, rentre également dans le cadre de la présente invention. L'opération inverse effectuée par le décrypteur correspondant appartient également au domaine de la présente invention.

Revendications.

1 - Installation de cryptage et de décryptage d'un signal analogique dans lequel le crypteur (1), resp. le décrypteur (2), comprend des moyens (12 ; 22) du genre registres à décalage analogiques pour retarder 2N échantillons du signal entrant analogique initial, resp. crypté, des moyens (14 ; 24) pour produire des impulsions d'horloge à période T_e commandant l'écriture, resp. la lecture, de N échantillons successifs du signal entrant initial, resp. du signal sortant décrypté, et des moyens (15 , 25) pour produire un signal de cryptage, resp. de décryptage, ayant N impulsions par période égale à NT_e, qui commandent la lecture, resp. l'écriture, de N échantillons du signal initial précédemment retardés et écrits dans le crypteur (1), resp. du signal entrant crypté avant d'être retardés et lus dans le décrypteur (2), caractérisée en ce que les N impulsions des périodes NT_e des signaux de cryptage et de décryptage ne sont pas équiréparties temporellement, et en ce que, pendant une période NT_e tous les échantillons écrits régulièrement dans le crypteur (1) sont lus en série selon leur ordre initial en subissant au moins une compression temporelle et éventuellement une expansion temporelle partielle de leur répartition sou la commande des N impulsions d'une période du signal de cryptage, et tous les N échantillons du signal crypté entrant dans le décrypteur (2) sont écrits en série d'une manière identique à la lecture dans le décrypteur (1).

2 - Installation conforme à la revendication 1, dans laquelle les moyens de retard (12 , 22) du crypteur (1), resp. du décrypteur (2) comprennent deux lignes à retard (121_1 - 121_2 ; 221_1 - 221_2) ayant leurs entrées (120 ; 220) reliées pour recevoir alternativement pendant une période sur deux du signal de cryptage, resp. de décryptage, N échantillons du signal entrant initial, resp. crypté, l'une des deux lignes à retard étant commandée pendant une période sur deux du signal de cryptage, resp. de décryptage, au rythme des impulsions d'horloge (F_e), en écriture dans le crypteur (1), resp. en lecture dans le décrypteur (2), pendant que l'autre est commandée en lecture dans le crypteur (1),

resp. en écriture dans le décrypteur (2), caractérisée en ce que les sorties (123_1 - 123_2; 223_1 - 223_2) des derniers étages des deux lignes à retard (121_1 - 121_2 ; 221_1 - 221_2) sont commutées alternativement à la sortie (125 ; 225) du crypteur (1), resp. du décrypteur (2), à chaque période du signal de cryptage, resp. de décryptage, afin que chacune transmettent, resp. reçoivent, en série, N échantillons lus, resp. écrits, sous la commande des N impulsions non équiréparties temporellement pendant une période sur deux du signal de cryptage, resp. de décryptage.

3 - Installation conforme à la revendication 1, caractérisée en ce que, dans les moyens de retard (12 ; 22) du crypteur (1), resp. du décrypteur (2), une première ligne à retard (121_1 ; 221_1) a l'entrée (120' ; 220') de son premier étage recevant continûment le signal analogique initial, resp. crypté, et a ses N sorties (122' ; 222') d'étages respectivement reliées en parallèle aux N entrées d'étages d'une seconde ligne à retard (121' ; 221') dont la sortie (125' ; 225') du dernier étage est reliée à la sortie du crypteur (1), resp. du décrypteur (2) et en ce que pendant chaque période NT_e du signal de cryptage, resp. de décryptage, la première ligne à retard ($121'_1$; $221'_1$) est commandée en écriture dans le crypteur (1) au rythme des impulsions d'horloge, resp. dans le décrypteur (2) au rythme des impulsions du signal de décryptage, tandis que la seconde ligne à retard ($121'_2$; $221'_2$) est commandée en lecture dans le crypteur (1) au rythme des impulsions du signal de cryptage, resp. dans le décrypteur (2) au rythme des impulsions d'horloge, les première et seconde lignes à retard étant commandées simultanément en lecture et écriture à la fin de chaque période NT_e du signal de cryptage, resp. de décryptage, pour transférer en parallèle les N échantillons analogiques de la première ($121'_1$; $221'_1$) dans la seconde ($121'_2$; $221'_2$) ligne à retard.

4 -Installation conforme à l'une des revendications 1 à 3, caractérisée en ce que les moyens de production du signal de code de cryptage, resp. de décryptage (14, 24) comprennent chacun des moyens (151) pour produire périodiquement des impulsions dont les N premières pendant une période NT_e du signal de code sont propres à commander la lecture,

resp. l'écriture de N échantillons auxdits instants selon ladite répartition prédéterminée et en ce que le crypteur (1), resp. le décrypteur (2) comprend des moyens (155) pour compter N impulsions pendant chaque période NT_e du signal de code afin de bloquer la lecture, resp. l'écriture des échantillons après la Nième impulsion jusqu'au début de la période du signal de code suivante et des moyens de synchronisation (16 ; 26) pour détecter la fin d'une période du signal de code sous la commande, dans le crypteur (1), d'un signal d'horloge à période NT_e, resp. dans le décrypteur (2) d'une impulsion de synchronisation transmise par le crypteur (1) afin de remettre à zéro lesdits moyens de comptage (155) et de réinitialiser les moyens de production d'impulsions (151).

5 - Installation conforme à la revendication 4, caractérisée en ce que le crypteur (1), resp. le décrypteur (2) comprend une pluralité de moyens de production d'impulsions (1510) dont les répartitions prédéterminées des N premières impulsions pendant une période NT_e de signal de code sont différentes et des moyens (152, 153, 154) pour adresser lesdits moyens de production d'impulsions (1510) afin de sélectionner un code.

6 - Installation conforme à la revendication 4, caractérisée en ce que les moyens de production d'impulsions (151) du décrypteur (2) sont enfichables dans le bâti du décrypteur.

7 - Installation conforme à la revendication 5, caractérisée en ce qu'au moins l'un des moyens de production d'impulsions (1510) est un diviseur/ou multiplicateur de fréquence programmable (Fig. 2a) par lesdits moyens d'adressage (152, 153, 154).

8 - Installation conforme à la revendication 5, caractérisée en ce qu'au moins l'un des moyens de production d'impulsions (1510) est un modulateur en impulsions d'un signal selon une modulation en position (Figs. $2b_1$; $2c_1$) ou en fréquence (Figs. $2b_2$; $2c_2$) dont la fréquence peut être programmable sous la commande des moyens d'adressage (152, 153, 154).

9 - Installation conforme à l'une des revendications 4 à 8, caractérisée en ce que le crypteur (1) comprend des moyens (16) pour transmettre un signal de synchronisation modulé correspondant à la fin

de chaque période du signal de code, des moyens (171) pour filtrer le signal crypté, des moyens (172) pour filtrer le signal de synchronisation modulé, des moyens (17) pour mélanger les signaux analogiques crypté et de synchronisation filtrés en un signal composite transmis vers le décrypteur (2) et en ce que le décrypteur (2) comprend des moyens (271, 272) pour filtrer le signal composite afin de transmettre ledit signal analogique crypté à l'entrée (220) des moyens de retard analogiques (22) du décrypteur (2) et ledit signal de synchronisation modulé auxdits moyens de détection de synchronisation (26) du décrypteur (2).

10 - Installation conforme à l'une des revendications 1 à 9, caractérisée en ce que le crypteur (1), resp. le décrypteur (2) comprend à l'entrée de réception du signal analogique initial, resp. à la sortie de transmission du signal décrypté, un circuit de préaccentuation et/ou de compression (11), resp. un circuit de désaccentuation et/ou d'extension (21) qui sont complémentaires.

1/4 FIG.1

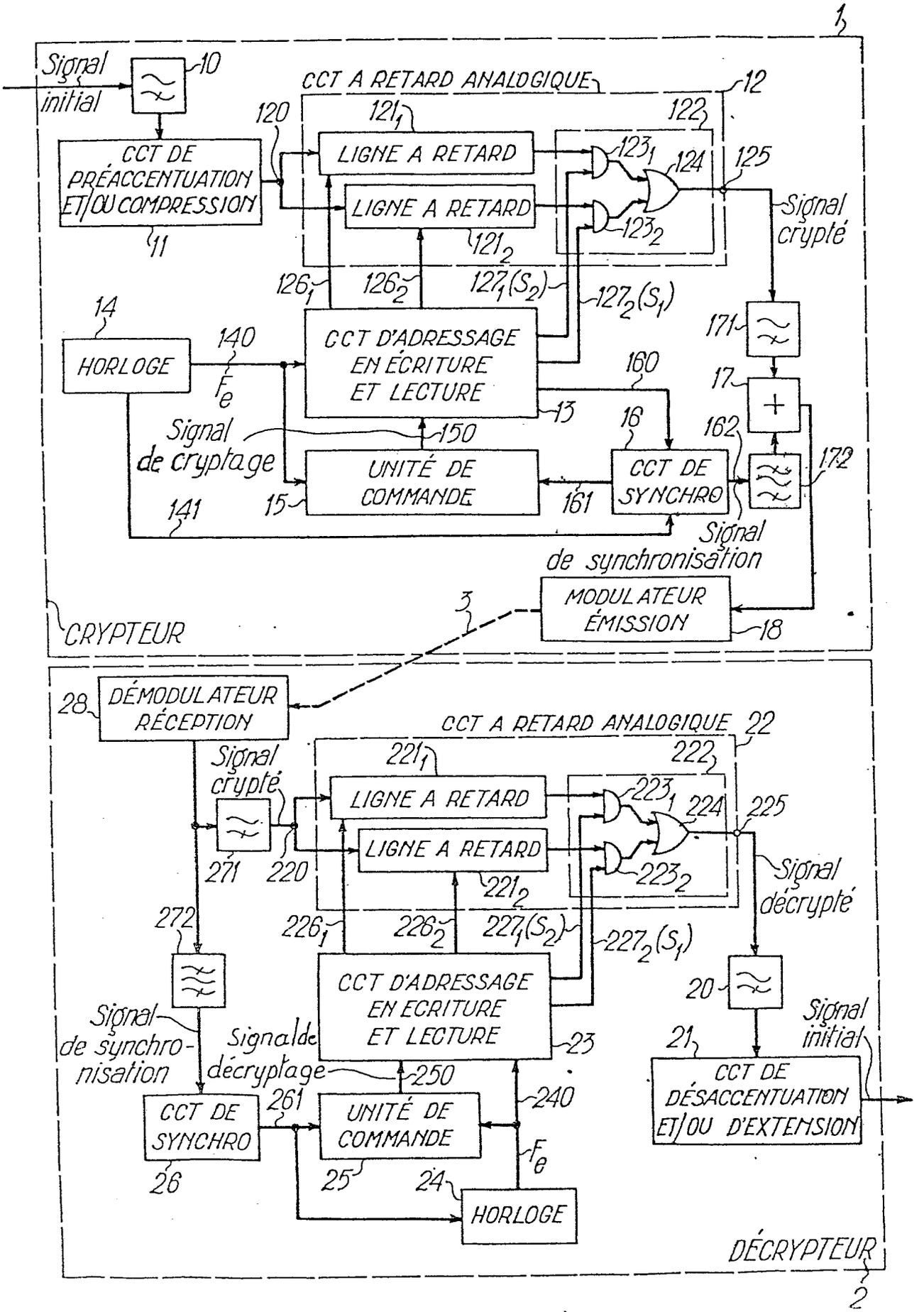

1
Signal initial
10
CCT A RETARD ANALOGIQUE
12
120
121₁
122
CCT DE PRÉACCENTUATION ET/OU COMPRESSION
11
LIGNE A RETARD
123₁
124
125
LIGNE A RETARD
121₂
123₂
Signal crypté
126₁
126₂
127₁(S₂)
127₂(S₁)
14
HORLOGE
140
Fe
CCT D'ADRESSAGE EN ÉCRITURE ET LECTURE
13
160
171
17
16
162
172
Signal de cryptage
150
UNITÉ DE COMMANDE
15
CCT DE SYNCHRO
161
141
Signal de synchronisation
MODULATEUR ÉMISSION
18
3
CRYPTEUR
28
DÉMODULATEUR RÉCEPTION
CCT A RETARD ANALOGIQUE
22
Signal crypté
221₁
222
LIGNE A RETARD
223₁
224
225
LIGNE A RETARD
221₂
223₂
271
220
Signal décrypté
272
226₁
226₂
227₁(S₂)
227₂(S₁)
CCT D'ADRESSAGE EN ECRITURE ET LECTURE
23
20
Signal de synchro-nisation
Signal de décryptage
250
240
21
Signal initial
CCT DE DÉSACCENTUATION ET/OU D'EXTENSION
CCT DE SYNCHRO
261
UNITÉ DE COMMANDE
26
25
24
Fe
HORLOGE
DÉCRYPTEUR
2

FIG.2

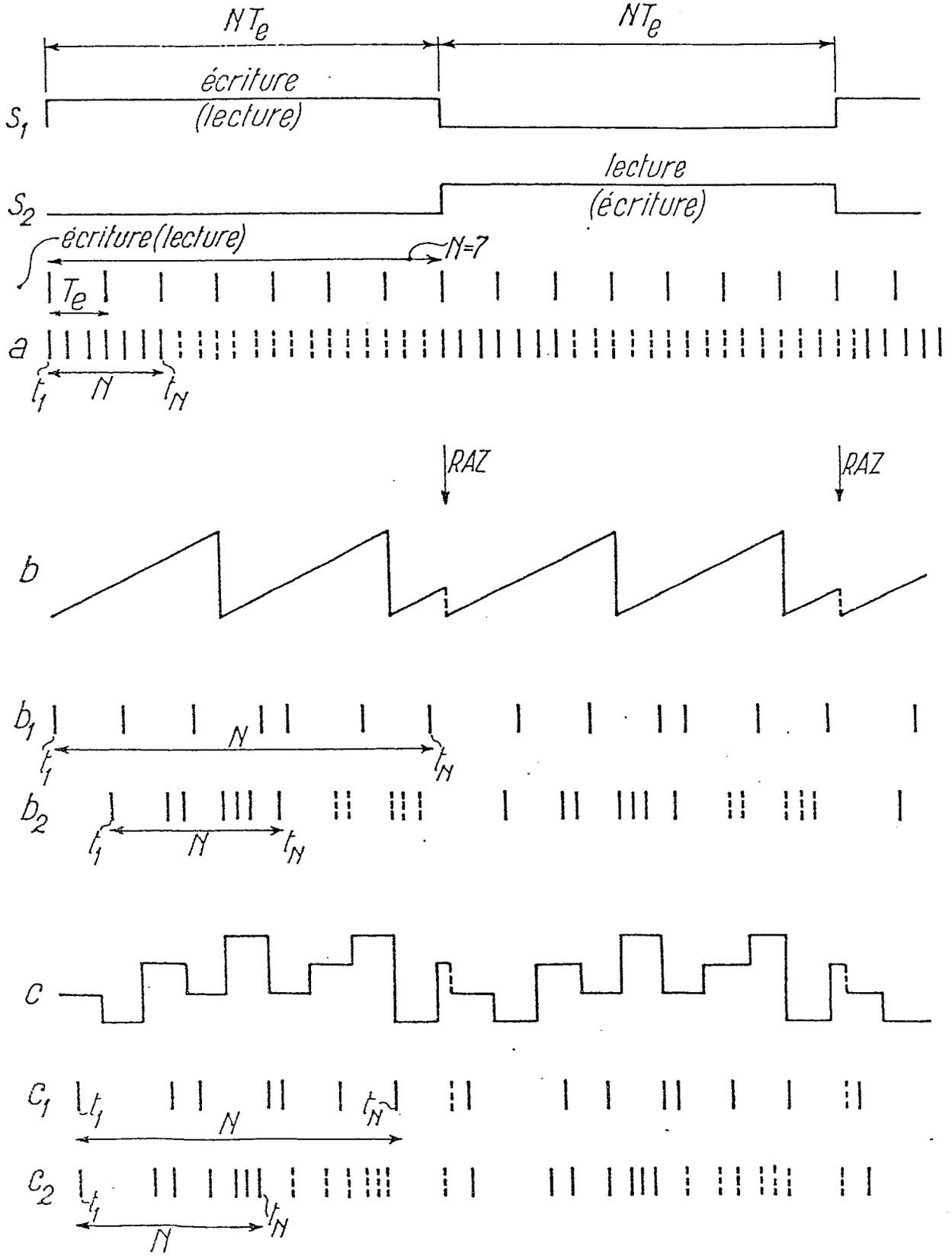

NTe
NTe
écriture
(lecture)
S1
lecture
(écriture)
S2
écriture (lecture)
N=7
Te
a
t1
N
tN
RAZ
RAZ
b
b1
N
t1
tN
b2
t1
N
tN
c
c1
t1
N
tN
c2
t1
tN
N

FIG.3

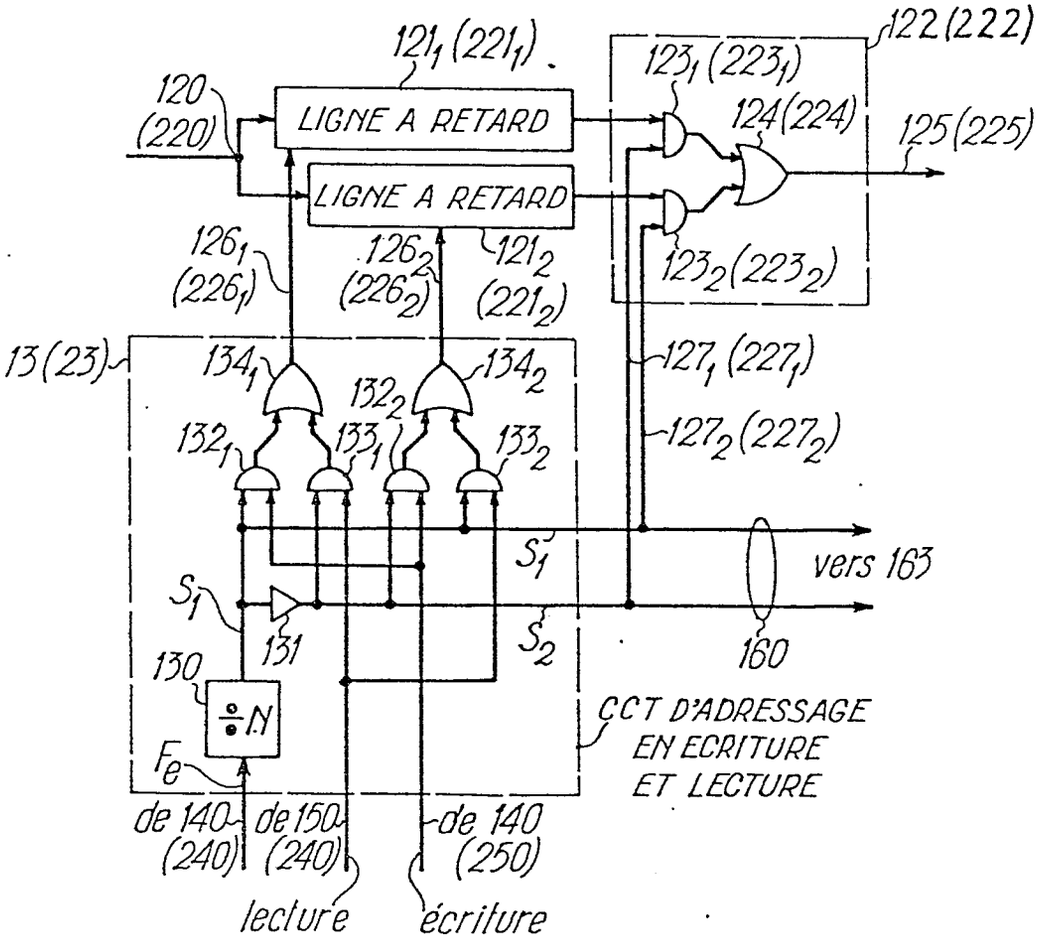

121₁ (221₁)
122 (222)
123₁ (223₁)
120 (220)
LIGNE A RETARD
124 (224)
125 (225)
LIGNE A RETARD
126₁ (226₁)
126₂ (226₂)
121₂ (221₂)
123₂ (223₂)
13 (23)
134₁
134₂
132₂
127₁ (227₁)
132₁
133₁
133₂
127₂ (227₂)
S₁
vers 163
S₁
131
S₂
160
130
÷N
CCT D'ADRESSAGE EN ECRITURE ET LECTURE
Fe
de 140 (240)
de 150 (240)
de 140 (250)
lecture
écriture

FIG.4

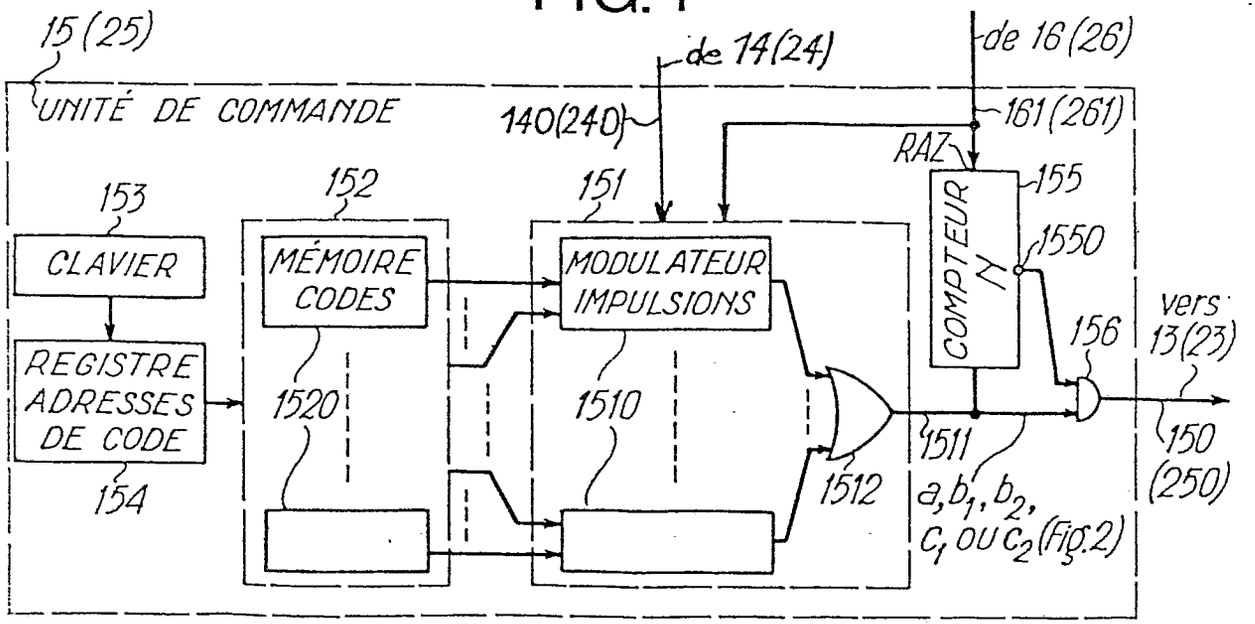

15 (25)
de 14 (24)
de 16 (26)
UNITÉ DE COMMANDE
140 (240)
161 (261)
RAZ
155
153
152
151
COMPTEUR N
1550
CLAVIER
MÉMOIRE CODES
MODULATEUR IMPULSIONS
156
vers 13 (23)
REGISTRE ADRESSES DE CODE
1520
1510
1511
1512
150 (250)
154
a, b₁, b₂, c₁ ou c₂ (Fig.2)

FIG.5

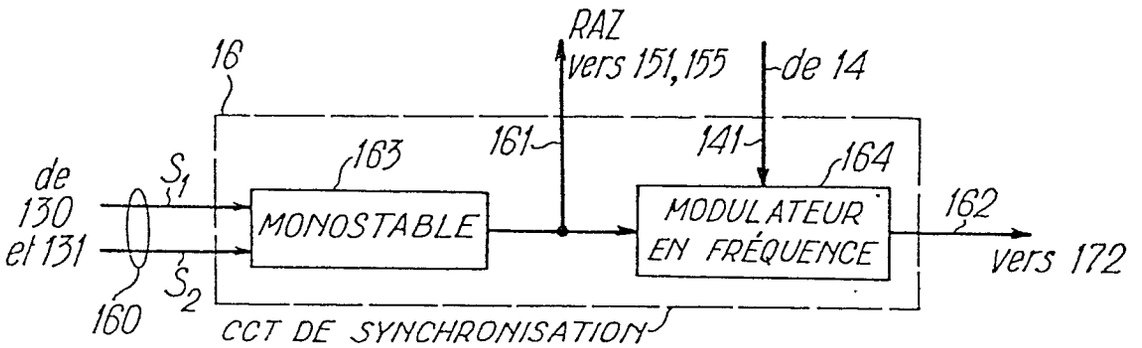
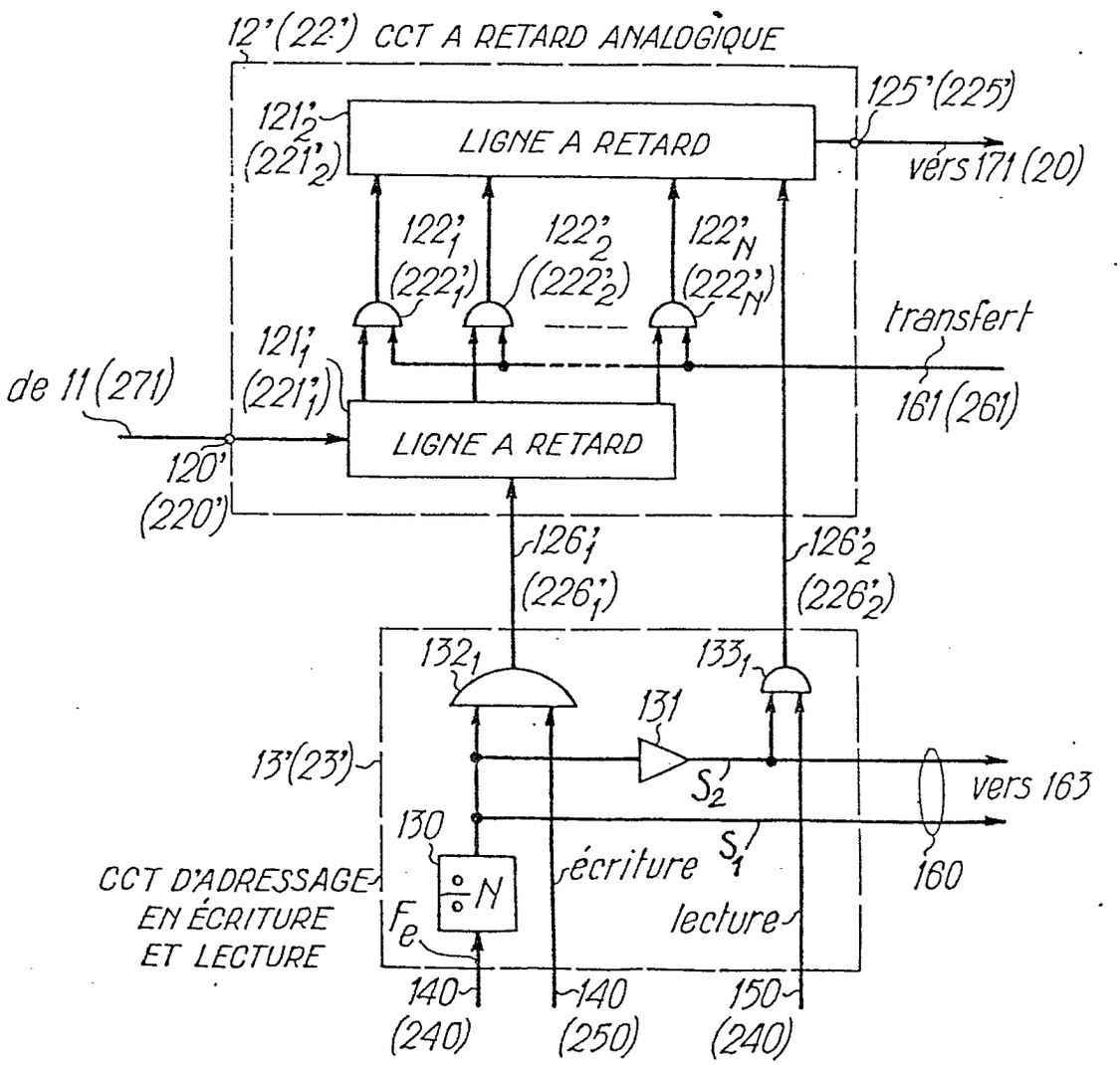

RAZ
vers 151, 155
de 14
16
161
141
163
164
de
130
et 131
S_1
MONOSTABLE
MODULATEUR
EN FRÉQUENCE
162
vers 172
S_2
160
CCT DE SYNCHRONISATION

FIG.6


12'(22') CCT A RETARD ANALOGIQUE
$121'_2$ ($221'_2$)
LIGNE A RETARD
125'(225')
vers 171 (20)
$122'_1$ ($222'_1$)
$122'_2$ ($222'_2$)
$122'_N$ ($222'_N$)
transfert
$121'_1$ ($221'_1$)
de 11 (271)
161 (261)
LIGNE A RETARD
120'
(220')
$126'_1$ ($226'_1$)
$126'_2$ ($226'_2$)
132_1
133_1
131
13'(23')
S_2
vers 163
130
S_1
écriture
160
CCT D'ADRESSAGE EN ÉCRITURE ET LECTURE
÷N
F_e
lecture
140 (240)
140 (250)
150 (240)

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande
EP 80 40 0476

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernee
	DE - A - 2 412 732 (LICENTIA) * Page 4, lignes 9-22; page 13, lignes 1-6; dernier alinéa; page 14, dernier alinéa *	1,2
	US - A - 4 099 027 (WHITTEN) * Colonne 2, ligne 67 à colonne 3, ligne 5; lignes 12-44; colonne 9, lignes 28-55; colonne 10, lignes 23-44 *	1
	DE - A - 2 648 674 (GRUBE) * Page 2, lignes 2-9; lignes 25-28 *	6
	GB - A - 1 340 327 (PLESSEY) * Page 1, lignes 9-12; page 2, lignes 2-7; lignes 58-65; page 3, lignes 30-36; lignes 73-85 *	9
EP	EP - A - 0 008 086 (SIEMENS) * Page 2, lignes 18-33; page 3, lignes 14-19; page 4, ligne 8 à page 5, ligne 2; ligne 26 à page 6, ligne 15 *	1,2,7

CLASSEMENT DE LA DEMANDE (Int. Cl.)
H 04 K 1/06

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.)
H 04 K 1/06
1/00
H 04 L 9/04

CATEGORIE DES DOCUMENTS CITES

- X. particulièrement pertinent
- A: arriere-plan technologique
- O: divulgation non-ecrite
- P: document intercalaire
- T: theorie ou principe à la base de l'invention
- E: demande faisant interference
- D: document cite dans la demande
- L: document cite pour d'autres raisons
- &: membre de la même famille, document correspondant

X Le present rapport de recherche a ete établi pour toutes les revendications

Lieu de la recherche	Date d'achevement de la recherche	Examinateur
La Haye	23-07-1980	HOLPER