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

(11) Numéro de publication: **0 018 869**
B1

(12) # FASCICULE DE BREVET EUROPEEN

(45) Date de publication du fascicule du brevet: **18.05.83**

(51) Int. Cl.³: **H 04 K 1/06**

(21) Numéro de dépôt: **80400476.0**

(22) Date de dépôt: **09.04.80**

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

(30) Priorité: **20.04.79 FR 7910092**

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

(45) Mention de la délivrance du brevet:
18.05.83 Bulletin 83/20

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

(56) Documents cités:
EP - A - 0 008 086
DE - A - 2 412 732
DE - A - 2 648 674
GB - A - 1 340 327
US - A - 4 099 027

(73) Titulaire: **Etablissement Public Télédiffusion de France**
10, rue d'Oradour-sur-Glane
F-75015 Paris (FR)

(72) Inventeur: **Maillard, Michel**
27, rue Maurice Coutant
F-94200 Ivry (FR)
Inventeur: **Lemaire, Jean**
10, rue Adolphe Petrement
F-93600 Aulnay-sous-Bois (FR)
Inventeur: **Ruiz, Michel**
13, boulevard des Frères Voisin
F-75015 Paris (FR)
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)

Courier Press, Leamington Spa, England.

EP 0 018 869 B1

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 comprenant un crypteur pour crypter un signal entrant analogique initial en un signal crypté analogique et un décrypteur pour décrypter le signal crypté analogique en un signal décrypté analogique analogue audit signal analogique initial et telle que définie dans le préambule de la revendication 1.

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 heurs 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 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 un selon des séquences de permutation d'un ou plusieurs échantillons.

Une installation de cryptage et de décryptage telle que définie dans le préambule de la revendication 1 est décrite dans le brevet américain US—A—4.100.374. Les moyens de retard du crypteur, resp. du décrypteur, sont constitués par deux véritables mémoires analogiques, bien qu'appelées "registres à décalage analogiques" composées chacune de N cellules d'echantillon adressables individuellement en écriture et lecture. Les entrées des mémoires reçoivent alternativement, pendant une période NT_e sur deux du signal de cryptage, resp. de décryptage, N échantillons en série du signal entrant initial, resp. crypté. Les 2N sorties des cellules des deux mémoires analogiques sont reliées en parallèle 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 parallèle—série. Il est commandé par le signal de cryptage, resp. de décryptage, afin de sélectionner alternativement en lecture, pour deux périodes consécutives NT_e, les N sorties de l'une des mémoires puis les N sorties de l'autre mémoire. Pendant chaque période NT_e, les N cellules d'une mémoire sont adressées en lecture 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 fréquence de lecture que celle d'écriture $1/T_e$. Le signal de cryptage adresse en lecture ainsi les N cellules d'une mémoire 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 mémoires 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.

Un autre procédé de cryptage et de décryptage faisant appel à un échantillonnage du signal analogique entrant et à l'écriture d'échantillons ou portions de signal dans des mémoires analogiques est décrit dans la demande de brevet allemand DE—A—2.412.732. Pendant chaque période NT_e, N portions du signal entrant de durée égale T_e sont mémorisées. Puis dans le crypteur, parmi celles-ci, des portions de signal sont sélectionnées et sont lues avec une vitesse égale à un sous-multiple entier

k de la vitesse d'écriture afin d'occuper par expansion temporelle des fentes temporelles T_e plus grandes dont la somme est égale à NT_e. Ce procédé présente l'inconvénient qu'une partie de l'information est perdue et n'est pas transmise au décrypteur et que les portions de signal initial non transmises sont restituées à la réception par similitude avec les portions véritablement reçues.

On connaît également par le brevet américain US—A—4.099.027 une installation de cryptage et de décryptage dans laquelle le crypteur et le décrypter comprennent chacun une unique ligne à retard analogique ou registre à décalage analogique inséré en série entre l'entrée et la sortie. La ligne à retard enchantillonne le signal entrant et transfère de l'entrée vers la sortie par écriture et lecture successives dans ses différents étages analogiques en série les échantillons sous la commande de signaux logiques complémentaires émanant d'un même signal de modulation. Il y a alors expansion et compression temporelles des échantillons. Dans le crypteur, l'échantillonnage initial n'est pas régulier, c'est-à-dire n'est pas rythmé à période constante, et si le signal entrant initial varie notablement lorsque le retard imposé est grand, c'est'à-dire lorsque l'écart entre deux instants d'échantillonnage successifs est grand, le signal décrypté à la réception peut être corollairement différent. Cette installation présente également le second inconvénient suivant. L'ecriture et la lecture dans la ligne à retard étant rythmées par le même signal de cryptage dans le crypteur, il est alors nécessaire de compenser les retards dans le décrypteur en retardant le signal crypté selon l'ordre inverse des retards dans le crypteur. En d'autres termes, le signal de décryptage est l'inverse du signal de cryptage, cette condition présentant les désavantages déjà mentionnés pour le US—A—4.100.374.

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 sans pertes d'échantillon au moins une compression temporelle pour chaque période du signal de cryptage, lequel est également utilisé en tant que signal de 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 est telle que caractérisée dans la revendication 1.

La fonction de retard ou de compensation 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").

Une première combinaison des deux lignes à retard dans le crypteur, resp. dans le décrypteur est déterminée dans la revendication 2. Chaque période NT_e correspond à la durée de remplissage de tous est étages d'une ligne à retard pendant laquelle sont écrits dans le crypteur, resp. sont lus dans le décrypteur les N échantillons du signal initial, res. décrypté. Pendant chaque période NT_e, 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 décryptage 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 cryptage selon ladite répartition prédeterminée, 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 cryptage, res. de décryptage.

Une seconde combinaison des deux lignes à retard dans le crypteur, resp. le décrypteur est déterminée dans la revendication 3.

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 transmissions des impulsions suivantes jusqu'au début de la période suivante. Par suite, N échantillons du signal crypté sont toujours compresés temporellement pour une période NT_e. Cependant l'intervalle temporel entre deux échantillons successifs d'une même période NT_e peut être plus grand que T_e. En fonction de la modulation sélectionée, 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 clairemont 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 adressage en éciture 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 défaults 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 analogiqe 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 transfer 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 $F_4=1/T_e$ 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 $512\times0,05/2$ ms. Chaque ligne à retard retarde le signal analogique d'une durée qui est inférieur à deux fois la durée dite d'écriture $NT_e=(P\times512/2)\times0,05$ ms de N échantillons, et que 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 égale-

ment 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'echantillonnage 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 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-band 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 évalement, 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 code 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'horloge 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 le sortie 225 du circuit de commutation analogique 222 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 complé-

mentaire 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 le lecture aux instants t_1 à t_N tels que, en général, $t_{i+1}-t_i \neq T_e$ avec $1 \leqslant i < N$. 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'invenion, 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. Cependent, 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'on a 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, de 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 suivant NT_e, il est néessaire d'inhiber les autres impulsions de range 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 sorte 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. Dés 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 pen-

dant une durée NT_e. Les N impulsions de lecture transmises sont représentées en traits pleins sur les lignes a, 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 traverse 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 133_1 et 133_2.

Le circuit de synchronisation 16 est montré schématiquement à la Fig. 5. Il comprend une double bascule monostable 163 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 transmisses 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 transmission 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 grande 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 que 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 impulsions ou plus simplement un multiplicateur ou un diviseur de 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 rem-

plaçant 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 réalisée, 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 signal crypté est véhiculé dans un canal de fréquence de la voie de transmission 3, le signal de synchronisation peut être mélangé au signal crypté dans ce 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 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 comprenant un crypteur (1) pour crypter un signal entrant analogique initial en un signal crypté analogique et un décrypteur (2) pour décrypter le signal crypté analogique en un signal décrypté analogique analogue audit signal analogique initial, le crypteur (1) comprenant des premiers moyens (12) pour retarder 2N échantillons du signal analogique entrant, des premiers moyens d'écriture (13, 14) pour produire des premières impulsions d'horloge à une période prédéterminée T_e qui commandent l'écriture en série et l'échantillonnage de N échantillons successifs du signal entrant dans les premiers moyens de retard (12) pendant une première période NT_e et des premiers moyens de lecture (13, 15) pour produire un signal de cryptage ayant N impulsions par période égale à NT_e qui commandent la lecture de N échantillons successifs écrits dans les premiers moyens de retard (12) pendant une seconde période NT_e succédant à la première période NT_e afin d'obtenir ledit signal crypté analogique, et le décrypteur (2) comprenant des seconds moyens (22) pour retarder 2N échantillons du signal crypté analogique, des seconds moyens d'écriture (23, 25, 26) pour produire un signal de décryptage qui est synchronisé avec le signal de cryptage et qui est formé par N impulsions par période égale à NT_e qui commandent l'écriture en série de N échantillons successifs du signal crypté dans les seconds moyens de retard (22) pendant ladite première période NT_e et des seconds moyens de lecture (23, 24, 26) pour produire des secondes impulsions d'horloge à ladite période prédéterminée T_e qui sont synchronisées avec les premières impulsions d'horloge et qui commandent la lecture de N échantillons successifs écrits du signal crypté dans les seconds moyens de retard (22) pendant ladite seconde période NT_e afin d'obtenir le signal décrypté analogique, caractérisée en ce que les N impulsions du signal de cryptage sont réparties temporellement selon une répartition prédéterminée dans chacune desdites périodes NT_e afin que les N échantillons du signal crypté soient soumis à au moins une compression temporelle et éventuellement à une expansion temporelle par rapport à la répartition temporelle régulière des N échantillons écrits du signal entrant et en ce que le signal de décryptage est identique au signal de cryptage et a ses N impulsions qui sont réparties temporellement selon ladite répartition prédéterminée dans chacune desdites périodes NT_e.

2. Installation conforme à la revendication 1, dans laquelle les premiers moyens de retard (12) comprennent en entrée deux sous-moyens de retard analogiques (121_1, 121_2) ayant leurs entrées reliées (120) recevant le signal entrant analogique et étant commandées alternativement pendant une période NT_e sur deux, l'un en écriture par les N premières impulsions d'horloge et l'autre en lecture par les N impulsions du signal de cryptage, et en sortie des premiers moyens de commutation analogiques (122) délivrant le signal crypté et dans laquelle les seconds moyens de retard (22) comprennent en entrée deux sous-moyens de retard analogiques (221_1, 221_2) ayant leurs entrées

reliées (220) recevant le signal crypté analogique et étant commandées alternativement pendant une période NT_e sur deux, l'un en écriture par les N impulsions du signal de décryptage et l'autre en lecture par les N secondes impulsions d'horloge, et en sortie des seconds moyens de commutation analogiques (222) délivrant le signal décrypté, caractérisée en ce que les quatre sous-moyens de retard sont quatre lignes à retard analogiques (121_1, 121_2, 221_1, 222_2) et en ce que chacun des premiers et seconds moyens de commutation analogiques (122, 222) commute alternativement pendant une période NT_e sur deux les sorties des derniers étages analogiques des deux lignes à retard respectives (121_1, 121_2; 221_1, 222_2) pour transmettre 2N échantillons en série du signal crypté, resp. décrypté, pendant lesdites première et seconde périodes successives NT_e.

3. Installation conforme à la revendication 1, dans laquelle les premiers moyens de retard (12′) comprennent des premiers et seconds sous-moyens de retard analogiques ($121'_1$, $121'_2$), les premiers sous-moyens de retard ($121'_1$) ayant leur entrée (120′) recevant le signal entrant analogique et étant commandés en écriture par les N premières impulsions d'horloge pendant les premières périodes NT_e et les seconds sous moyens de retard ($121'_2$) étant commandés en lecture par les N impulsions du signal de cryptage pendant les secondes périodes NT_e et dans laquelle les seconds moyens de retard (22′) comprennent des troisièmes et quatrièmes sous-moyens de retard ($221'_1$, $221'_2$), les troisièmes sous-moyens de retard ($221'_1$) ayant leur entrée (220′) recevant le signal crypté analogique et étant commandés en écriture par les N impulsions du signal de décryptage pendant les premières périodes NT_e et les quatrièmes sous-moyens de retard ($221'_2$) étant commandés en lecture par les secondes impulsions d'horloge pendant les secondes périodes NT_e, caractérisée en ce que les sous-moyens de retard sont des première, seconde, troisième et quatrième lignes à retard analogiques ($121'_1$, $121'_2$, $221'_1$, $221'_2$), en ce que les premiers moyens de retard (12′) comprennent des moyens (122′) pour transférer en parallèle N échantillons du signal entrant des N premiers étages de la première ligne à retard ($121'_1$), qui est commandée en écriture par les premières impulsions d'horloge pendant les premières et secondes périodes NT_e, dans les N derniers étages de la seconde ligne à retard ($121'_2$), qui est commandée en lecture par les impulsions du signal de cryptage pendant les premières et secondes périodes NT_e, à la fin de chaque période NT_e, et en ce que les seconds moyens de retard (22′) comprennent des moyens (222′) pour transférer en parallèle N échantillons du signal crypté des N premiers étages de la troisième ligne à retard ($221'_1$), qui est commandée en écriture par les impulsions du signal de décryptage pendant les premières et secondes périodes NT_e, dans les N derniers étages de la quatrième ligne à retard ($221'_2$), qui est commandée en lecture par les secondes impulsions d'horloge pendant les premières et secondes périodes NT_e, à la fin de chaque période NT_e.

4. Installation conforme à l'une des revendications 1 à 3, caractérisée en ce que les premiers moyens de lecture (15) et les seconds moyens d'écriture (25) comprennent chacun des moyens (151) pour produire périodiquement des impulsions pendant chaque période NT_e dont les N premières sont réparties temporellement selon ladite répartition prédéterminée et des moyens (155) pour compter les premières impulsions pendant chaque période NT_e afin d'inhiber les impulsions succédant à la Nième impulsion jusqu'au début de la période NT_e suivante et des moyens de synchronisation (16; 26) recevant un signal d'horloge à période NT_e pour remettre à zéro lesdits moyens de comptage (155) et réinitialiser les moyens de production d'impulsions (151) à la fin d'une période NT_e.

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

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 une 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).

Patentansprüche

1. Einrichtung für die Verschlüsselung und Entschlüsselung mit einem Chiffrierer (1) für das Verschlüsseln eines eingehenden analogen Anfangssignals in ein analoges verschlüsseltes Signal und mit einem Dechiffrierer (2) für das Entschlüsseln des analogen verschlüsselten Signals in ein dem analogen Anfangssignal entsprechendes analoges entschlüsseltes Signal, wobei der Chiffrierer (1) eine erste Verzöge-

rungseinrichtung (12) für die Verzögerung von 2N Abtasungen des eingehenden analogen Signals, erste Schreibeinrichtungen (13, 14) für die Erzeugung von ersten Taktimpulsen mit einer vorbestimmten Periode T_e, welche das serielle Einschreiben und das Abtasten von N aufeinanderfolgenden Abtastungen das eingehenden Signals in der ersten Verzögerungseinrichtung (12) während einer ersten Periode NT_e steuern, und erste Leseeinrichtungen (13, 15) umfaßt, um ein Verschlüsselungssignal mit N Impulsen pro Periode NT_e zu erzeugen, welche das Lesen von N aufeinanderfolgenden, in die erste Verzögerungseinrichtung (12) während einer zweiten, auf die erste Periode NT_e folgenden Periode NT_e eingeschriebenen Abtastungen steuern, um das verschlüsselte analoge Signal zu erhalten, und wobei der Dechiffrierer (2) eine zweite Verzögerungseinrichtung (22) für die Verzögerung von 2N Abtastungen des verschlüsselten analogen Signals, zweite Schreibeinrichtungen (23, 25, 26) für die Erzeugung eines Entschlüsselungssignals, das mit dem Verschlüsselungssignal synchronisiert ist und das von N Impulsen pro Periode NT_e gebildet wird, welche das serielle Einschreiben von N aufeinanderfolgenden Abtastungen des verschlüsselten Signals in die zweite Verzögerungseinrichtung (22) während der ersten Periode NT_e steuern, und zweite Leseeinrichtungen (23, 24, 26) umfaßt, um zweite Taktimpulse mit der vorbestimmten Periode T_e zu erzeugen, die mit den ersten Taktimpulsen synchronisiert sind und die das Lesen der N aufeinanderfolgenden, von dem verschlüsselten Signal in die zweite Verzögerungseinrichtung (22) während der zweiten Periode NT_e geschriebenen Abtastungen steuern, um das entschlüsselte analoge Signal zu erhalten, dadurch gekennzeichnet, daß die N Impulse des Verschlüsselungssignals zeitlich gemäß einer vorbestimmten Verteilung in jeder der Perioden NT_e verteilt werden, damit die N Abtastungen des verschlüsselten Signals mindestens einer zeitlichen Kompression und eventuell einer zeitlichen Expansion im Verhältnis zu der regelmäßigen zeitlichen Verteilung der N eingeschriebenen Abtastungen des eingehenden Signals unterworfen werden und daß das Entschlüsselungssignal mit dem Verschlüsselungssignal identisch ist und seine N Impulse hat, die zeitlich gemäß der vorbestimmten Verteilung in jeder Periode NT_e verteilt sind.

2. Einrichtung nach Anspruch 1, in der die erste Verzögerungseinrichtung (12) an ihrem Eingang zwei analoge Verzögerungsmittel (121_1, 121_2), deren verbundene Eingänge (120) das analoge Eingangssignal aufnehmen und abwechselnd während jeder zweiten Periode NT_e, und zwar eines zum Einschreiben durch die ersten N Taktimpulse und das zweite zum Lesen durch die N Impulse des Verschlüsselungssignals gesteuert werden, und an ihrem Ausgang eine erste analoge Schalteinrichtung (122) aufweist, welche das verschlüsselte Signal liefert, und in der die zweite Verzögerungseinrichtung (22) an ihrem Eingang zwei analoge Verzögerungsmittel (221_1, 221_2), deren verbundene Eingänge (220) das verschlüsselte analoge Signal aufnehmen und die abwechselnd während jeder zweiten Periode NT_e, und zwar eines zum Einschreiben durch die N Impulse des Entschlüsselungssignals und das zweite zum Lesen durch die zweiten N Taktimpulse gesteuert werden, und an ihrem Ausgang eine zweite analoge Schalteinrichtung (222) aufweist, welche das entschlüsselte Signal liefert, dadurch gekennzeichnet, daß die vier Verzögerungsmittel vier analoge Verzögerungsleitungen (121_1, 121_2, 221_1, 222_2) sind und daß jede der ersten und zweiten analogen Schalteinrichtungen (122, 222) abwechselnd während jeder zweiten Periode NT_e jeweils die Ausgänge der letzten analogen Stufen der beiden jeweiligen Verzögerungsleitungen (121_1, 121_2; 221_1, 222_2) für die serielle Übertragung von 2N Abtastungen des verschlüsselten bzw. entschlüsselten Signals während der ersten und zweiten aufeinanderfolgenden Perioden NT_e umschaltet.

3. Einrichtung nach Anspruch 1, in welcher die erste Verzögerungseinrichtung (12′) erste und zweite analoge Verzögerungsmittel ($121'_1$, $121'_2$) umfaßt, wobei das erste Verzögerungsmittel ($121'_1$) an seinem Eingang (120′) das analoge Eingangssignal aufnimmt und zum Scheiben durch die N ersten Taktimpulse während der ersten Perioden NT_e gesteuert wird, und wobei das zweite Verzögerungsmittel ($121'_2$) zum Lesen durch die N Impulse des Verschlüsselungssignals während der zweiten Perioden NT_e gesteuert wird, und in welcher die zweite Verzögerungseinrichtung (22′) dritte und vierte Verzögerungsmittel ($221'_1$, $221'_2$) umfaßt, wobei das dritte Verzögerungsmittel ($221'_1$) mitt seinem Eingang (220′) das verschlüsselte analoge Signal aufnimmt und zum Schreiben durch die N Impulse des Entschlüsselungssignals während der ersten Perioden NT_e gesteuert wird und wobei das vierte Verzögerungsmittel ($221'_2$) zum Lesen durch die zweiten Taktimpulse während der zweiten Perioden NT_e gesteuert wird, dadurch gekennzeichnet, daß die Verzögerungsmittel erste, zweite, dritte und vierte analoge Verzögerungsleitungen ($121'_1$, $121'_2$, $221'_1$, $221'_2$) sind, daß die erste Verzögerungseinrichtung (12′) eine Übertragungseinrichtung (122′) für die parallele Übertragung von N Abtastungen des von N ersten Stufen der ersten Verzögerungsleitung ($121'_1$) eingehenden Signals, die zum Schreiben durch die ersten Taktimpulse während der ersten und zweiten Perioden NT_e gesteuert wird, in die N letzten Stufen der zweiten Verzögerungsleitung ($121'_2$) umfaßt, die zum Lesen durch die Impulse des Verschlüsselungssignals während der ersten und zweiten Perioden NT_e am Ende jeder Periode gesteuert wird, und daß die zweite Verzögerungseinrichtung (22′) eine Übertragungseinrichtung (222′) für die parallele Über-

tragung von N Abtastungen des verschlüsselten signals von N ersten Stufen der dritten Verzögerungsleitung ($221'_1$), die zum Scheiben durch die Impulse des Entschlüsselungssignals während der ersten und zweiten Perioden NT_e gesteuert wird, in die N letzten Stufen der vierten Verzögerungsleitung ($221'_2$) umfaßt, die zum Lesen durch die zweiten Taktimpulse während der ersten und zweiten Perioden NT_e am Ende jeder Periode NT_e gesteuert wird.

4. Einrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die erste Leseeinrichtung (15) und die zweite Scheibeinrichtung (25) jeweils Impulserzeuger (151) für die periodische Erzeugung von Impulsen während jeder Periode NT_e, wobei die N ersten zeitlich gemäß der vorbestimmten Verteilung verteilt werden, und Zähler (155) zum Zählen der ersten Impulse während jeder Periode NT_e umfassen, um die auf den N-ten Impuls folgenden Impulse bis zum Anfang der folgenden Periode NT_e zu unterdrücken, und Synchronisationseinrichtungen (16, 26) umfassen, welche ein Taktsignal mit der Periode NT_e empfangen, um den Zähler (155) auf Null zurückzustellen und den Impulserzeuger (151) am Ende einer Periode NT_e neu anzustoßen.

5. Einrichtung nach Anspruch 4, dadurch gekennzeichnet, daß der Chiffrierer (1) und der Dechiffrierer (2) jeweils mehrere Impulserzeugungsmittel (1510), deren vorbestimmte Verteilungen von N ersten Impulsen während jeder Periode NT_e unterschiedlich sind, und Adressiereinrichtungen (152, 153, 154) umfassen, welche die Impulserzeugungsmittel (1510) adressieren, um eine der vorbestimmten Verteilungen auszuwählen.

6. Einrichtung nach Anspruch 4, dadurch gekennzeichnet, daß der Impulserzeuger (151) des Dechiffrierers (2) in dem Gestell des Dechiffrierers (2) einsteckbar ist.

7. Einrichtung nach Anspruch 5, dadurch gekennzeichnet, daß mindestens eins der Impulserzeugungsmittel (1510) ein Frequenzteiler oder -multiplizierer ist, der durch die Adressiereinrichtungen (152, 153, 154) programmierbar (Fig. 2a) ist.

8. Einrichtung nach Anspruch 5, dadurch gekennzeichnet, daß mindestens eins der Impulserzeugungsmittel (1510) ein Impulsmodulator eines Signals ist, der mit Positionsmodulation (Fig. $2b_1$; $2c_1$) oder Frequenzmodulation (Fig. $2b_2$; $2c_2$) arbeitet, dessen Frequenz unter Steuerung durch die Adressiereinrichtungen (152, 153, 154) programmierbar ist.

Claims

1. Encrypting and decrypting arrangement comprising an encrypter (1) for encrypting an initial analog incoming signal into an analog encrypted signal and a decrypter (2) for decrypting the analog encrypted signal into an analog decrypted signal analogous to said initial incoming signal, the encrypter (1) comprising first means (12) for time delaying 2N samples of the analog incoming signal, first writing means (13, 14) for producing first clock pulses at a predetermined period T_e which control the in series writing and samples of N successive samples of the incoming signal in the first time delaying means (12) during a first period NT_e and first reading means (13, 15) for producing an encrypting signal having N pulses per period equal to NT_e that control the reading of N written successive samples in the first time delaying means (12) during a second period NT_e following the first period NT_e thereby obtaining said analog encrypting signal, and the decrypter (2) comprising second means (22) for time delaying 2N samples of the analog encrypted signal, second writing means (23, 24, 25) for producing a decypting signal that is synchronized with the encrypting signal and that is formed by N pulses per period equal to NT_e that control the in series writing of N successive samples of the encrypted signal in the second time delaying means (22) during said first period NT_e and second reading means (23, 24, 26) for producing second clock pulses at said predetermined period T_e that are synchronized with the first clock pulses and that control the reading of N written successive samples of the encrypted signal in the second time delaying means (22) during said second period NT_e thereby obtaining the analog decrypted signal, characterized in that the N pulses of the encrypting signal are time distributed according to a predetermined distribution in each of said periods NT_e whereby the N samples of the encrypted signal undergo at least a time compression and eventually a time expansion with regard to the regular time distribution of the N written samples of the incoming signal and in that the decrypting signal is identical to the encrypting signal and has its N pulses that are time distributed according to said predetermined distribution in each of said periods NT_e.

2. Arrangement according to claim 1, wherein the first time delaying means (12) comprise on the input side two analog time delaying sub-means (121_1, 121_2) having their connected inputs (120) receiving the analog incoming signal and being alternately controlled during every other period NT_e, one in writing by the N clock pulses and the other in reading by the N first pulses of the encrypting signal, and on the output side, first analog switching means (122) delivering the encrypted signal and wherein the second time delaying means (22) comprise on the input side two analog time delaying sub-means (221_1, 221_2) having their connected inputs (220) receiving the analog encrypted signal and being alternately controlled during every other period NT_e, one in writing by the N pulses of the decrypting signal and the other in reading by the N second clock pulses, and on the output side, second analog switching means (222) delivering the decrypted signal, characterized in that the four

time delaying sub-means are four analog delay lines (121_1, 121_2, 221_1, 221_2) and in that each of the first and second analog switching means (122, 222) alternately switches over the outputs of the last analog stages of the two respective delay lines (121_1, 121_2; 221_1, 222_2) during every other period NT_e to transmit 2N series-samples of the encrypted signal, respectively the decrypted signal, during said successive first and second periods NT_e.

3. Arrangement according to claim 1, wherein the first time delaying means (12′) comprise first and second time delaying sub-means ($121'_1$, $121'_2$), the first time delaying sub-mes ($121'_1$) having its input (120′) receiving the analog incoming signal and being controlled in writing by the N first clock pulses during the first periods NT_e and the second time delaying sub-means ($121'_2$) being controlled in reading by the N pulses of the encrypting signal during the second periods NT_e and wherein the second time delaying means (22′) comprise third and fourth time delaying sub-means ($221'_1$, $221'_2$), the third time delaying sub-means ($221'_1$) having its input (220′) receiving the analog encrypted signal and being controlled in writing by the N pulses of the decrypting signal during the first periods NT_e and the fourth time delaying sub-means ($221'_2$) being controlled in reading by the second clock pulses during the second periods NT_e, characterized in that the time delaying sub-means are first, second, third and fourth analog delay lines ($121'_1$, $121'_2$, $221'_1$, $221'_2$), in that the first time delaying means (12′) comprise means for transferring in parallel N samples of the incoming signal from the N first stages of the first delay line ($121'_1$) that is controlled in writing by the first clock pulses during the first and second periods NT_e, into the N last stages of the second delay line ($121'_2$) that is controlled in reading by the pulses of the encrypting signal during the first and second periods NT_e, at the end of each period NT_e, and in that the second time delaying means (22′) comprise means (222′) for transferring in parallel N samples of the encrypted signal from the N first stages of the third delay line ($221'_1$) that is controlled in writing by the pulses of the decrypting signal during the first and second periods NT_e, into the N last stages of the fourth delay line ($221'_2$) that is controlled in reading by the second clock pulses during the first and second periods NT_e, at the end of each period NT_e.

4. Arrangement according to any one of claims 1 to 3, characterized in that the first reading means (15) and the second writing means (25) each comprise means (151) for periodically producing pulses during each period NT_e, the N first of which being time distributed according to said predetermined distribution, and means (155) for counting the first pulses during each period NT_e thereby inhibiting the pulses succeeding the N^{th} pulse until the start of the following period NT_e, and synchronizing means (16, 26) receiving the clock signal at the period NT_e for resetting to zero said counting means (155) and for triggering said pulse producing means at the end of a NT_e.

5. Arrangement according to claim 4, characterized in that the encrypter (1) and the decrypter (2) each comprise a plurality of pulse producing means (1510) whose predetermined time distributions of N first pulses during each period NT_e are different and means (152, 153, 154) for addressing said pulse producing means (1510) thereby selecting one of the predetermined time distributions.

6. Arrangement according to claim 4, characterized in that the pulse producing means (151) of the decrypter (2) are plugged in the frame of the decrypter.

7. Arrangement according to claim 4, characterized in that at least one of the pulse producing means (1510) is a frequency divider or multiplier programmable by said addressing means (152, 153, 154).

8. Arrangement according to claim 5, characterized in that at least one of said pulse producing means (1510) is a pulse modulator for a signal according to a position (Figs. $2b_1$; $2c_1$) or frequency (Figs. $2b_2$; $2c_2$) modulation whose frequency may be programmable under the control of the addressing means (152, 153, 154).

FIG.1

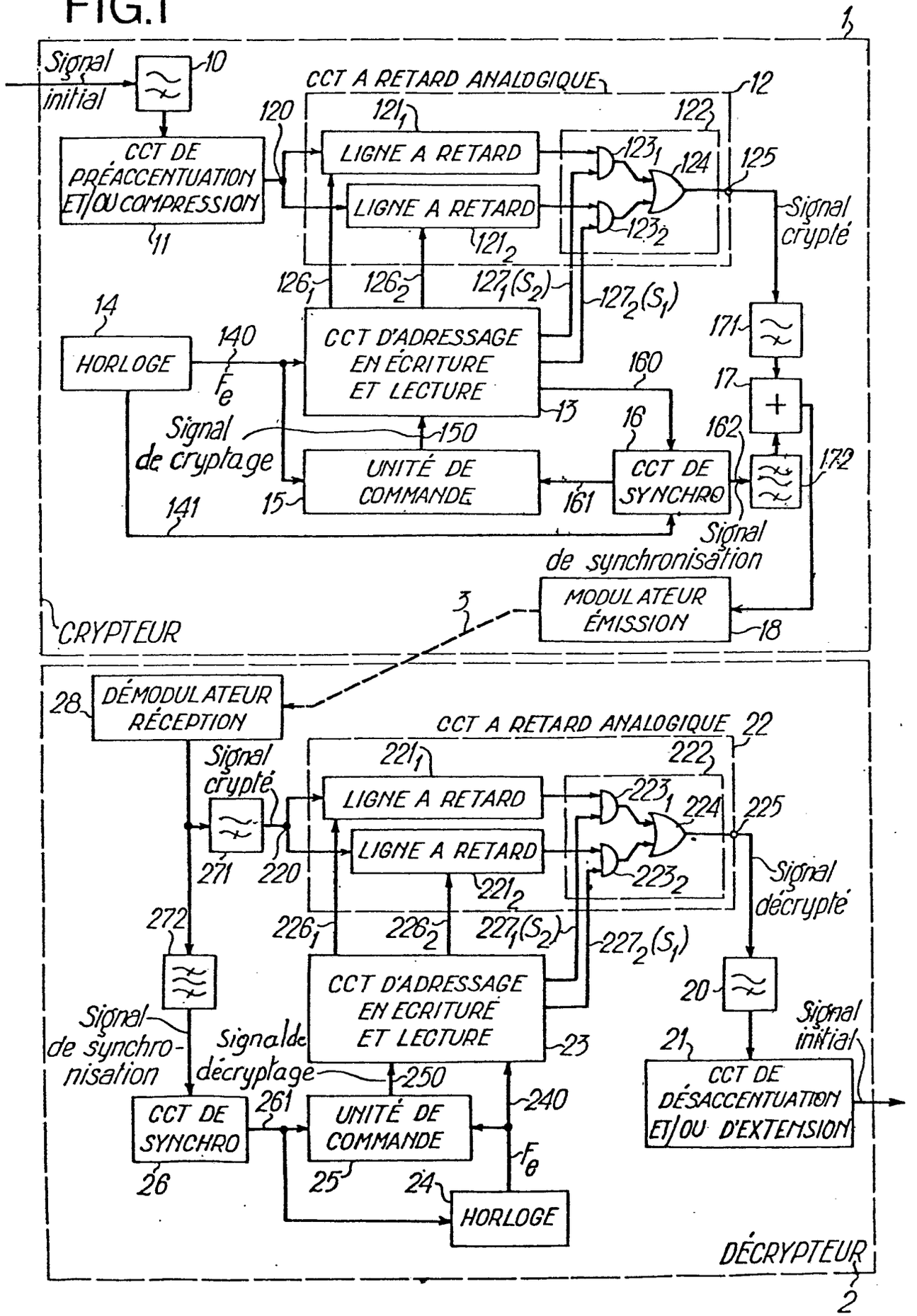

1
Signal initial
10
CCT A RETARD ANALOGIQUE
12
120
121 1
122
CCT DE PRÉACCENTUATION ET/OU COMPRESSION
11
LIGNE A RETARD
123 1
124
125
LIGNE A RETARD
121 2
123 2
Signal crypté
126 1
126 2
127 1 (S2)
127 2 (S1)
14
HORLOGE
140
Fe
CCT D'ADRESSAGE EN ÉCRITURE ET LECTURE
160
13
171
17
16
162
Signal de cryptage
150
UNITÉ DE COMMANDE
CCT DE SYNCHRO
172
15
161
141
Signal de synchronisation
MODULATEUR ÉMISSION
18
3
CRYPTEUR
28
DÉMODULATEUR RÉCEPTION
CCT A RETARD ANALOGIQUE
22
Signal crypté
221 1
222
LIGNE A RETARD
223 1
224
225
271
220
LIGNE A RETARD
221 2
223 2
Signal décrypté
272
226 1
226 2
227 1 (S2)
227 2 (S1)
CCT D'ADRESSAGE EN ECRITURE ET LECTURE
20
Signal de synchro-nisation
Signal de décryptage
23
Signal initial
21
250
240
CCT DE SYNCHRO
261
UNITÉ DE COMMANDE
CCT DE DÉSACCENTUATION ET/OU D'EXTENSION
26
25
24
Fe
HORLOGE
DÉCRYPTEUR
2

FIG.2

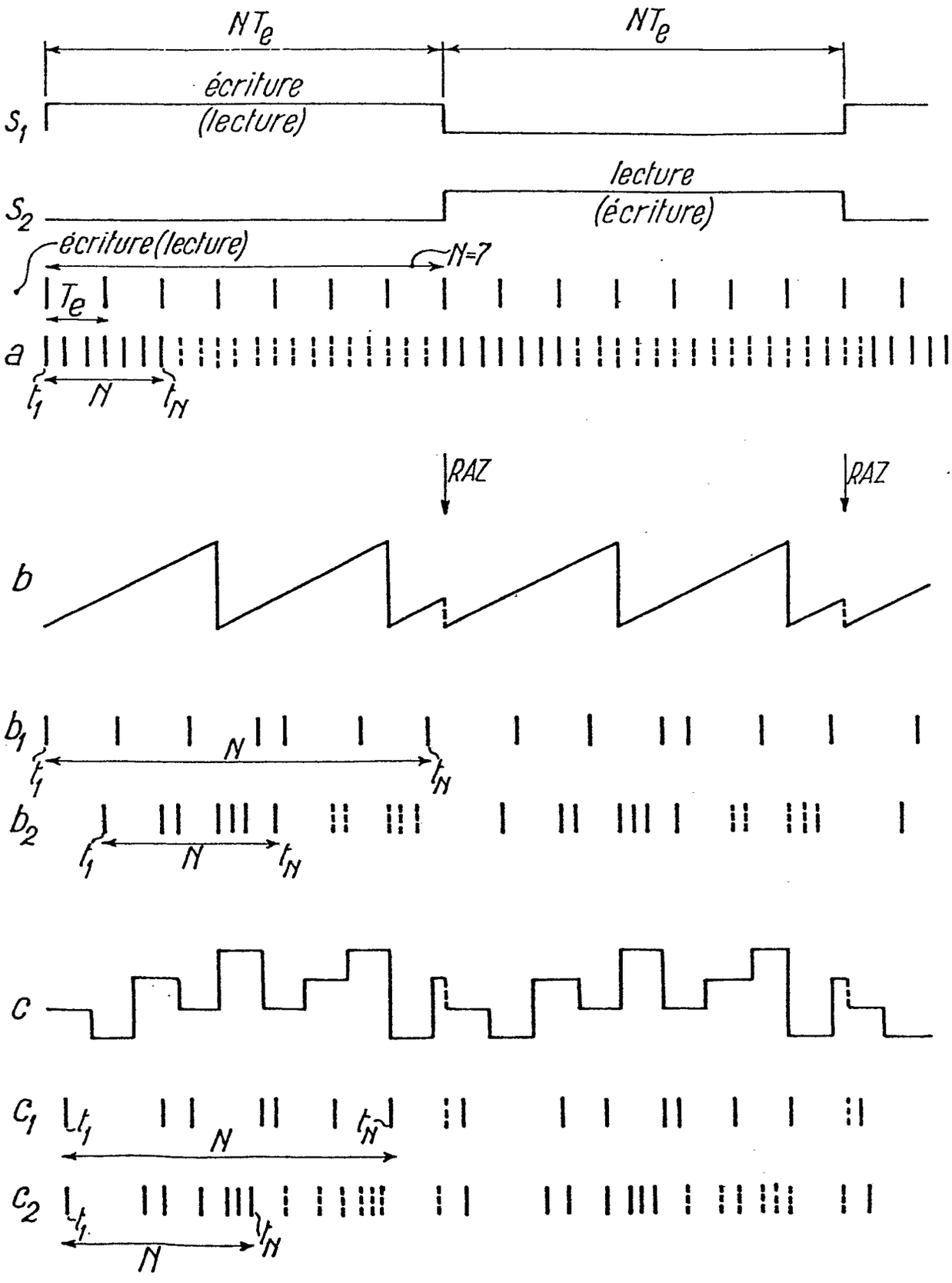

NTe
NTe
écriture
(lecture)
S1
lecture
(écriture)
S2
écriture (lecture)
N=7
Te
a
t1
N
tN
RAZ
RAZ
b
b1
N
t1
tN
b2
t1
N
tN
c
c1
t1
N
tN
c2
t1
N
tN

FIG.3

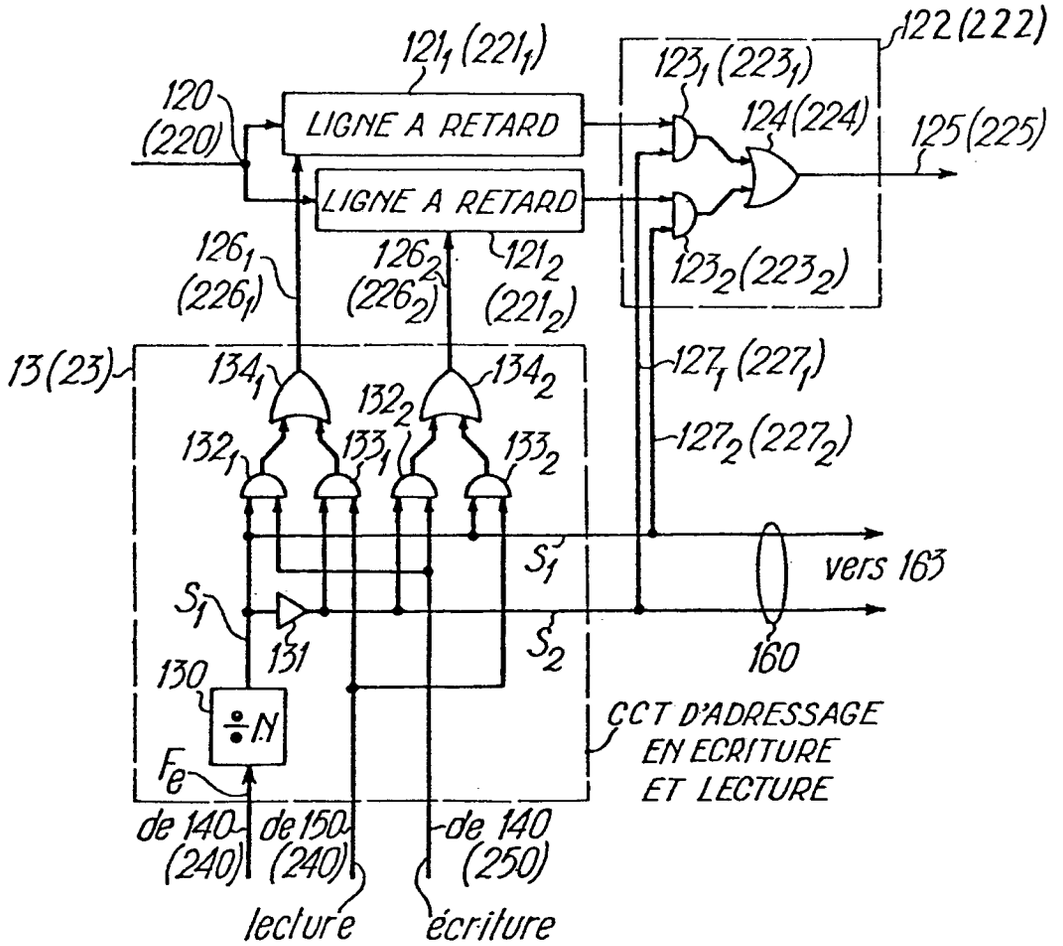

121₁ (221₁)
122 (222)
123₁ (223₁)
120 (220)
LIGNE A RETARD
124 (224)
125 (225)
LIGNE A RETARD
123₂ (223₂)
126₁ (226₁)
126₂ (226₂)
121₂ (221₂)
13 (23)
134₁
134₂
132₂
127₁ (227₁)
132₁
133₁
133₂
127₂ (227₂)
S₁
vers 163
S₁
131
S₂
160
130
÷N
CCT D'ADRESSAGE EN ECRITURE ET LECTURE
Fe
de 140 (240)
de 150 (240)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

FIG.4

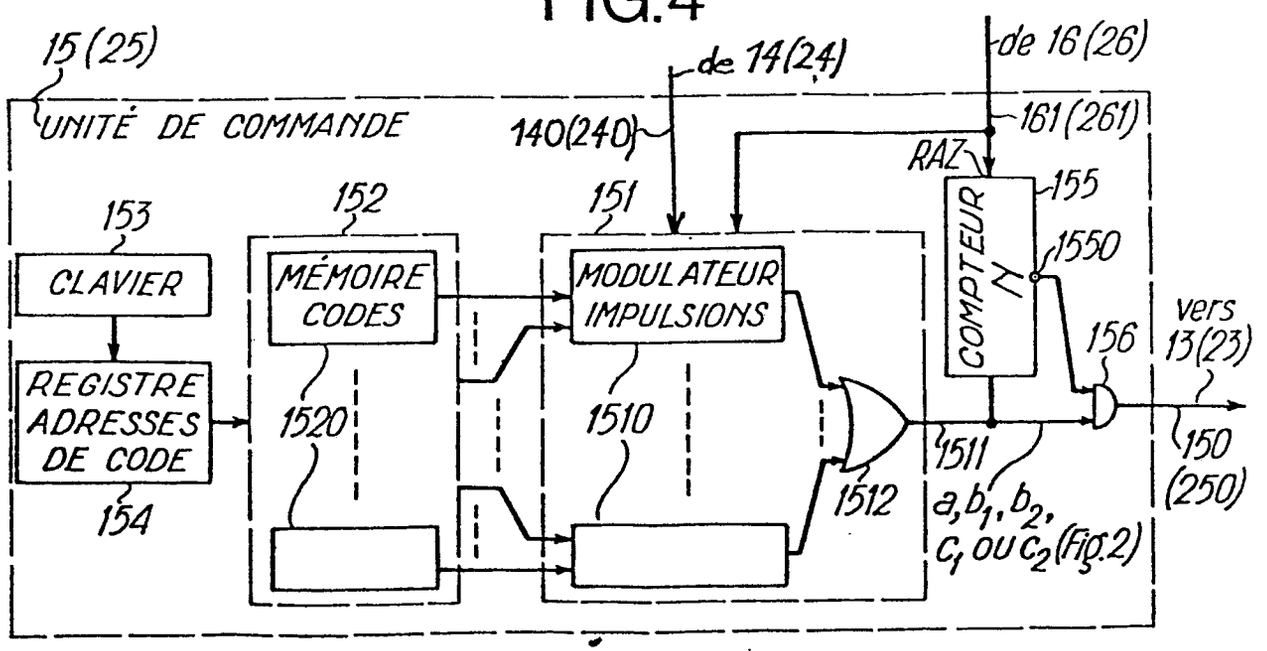

15 (25)
de 14 (24)
de 16 (26)
UNITÉ DE COMMANDE
140 (240)
161 (261)
RAZ
155
153
152
151
COMPTEUR N
1550
CLAVIER
MÉMOIRE CODES
MODULATEUR IMPULSIONS
vers 13 (23)
156
REGISTRE ADRESSES DE CODE
1520
1510
1511
1512
150 (250)
154
a, b₁, b₂, c₁ ou c₂ (Fig.2)

FIG.5

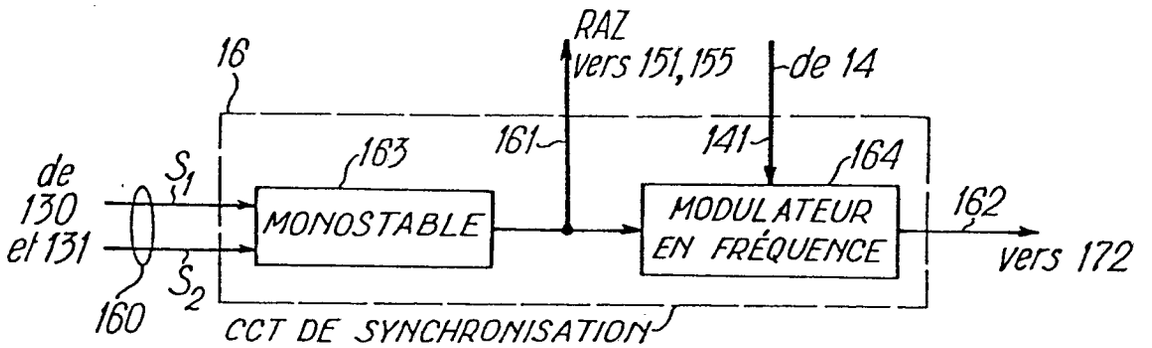
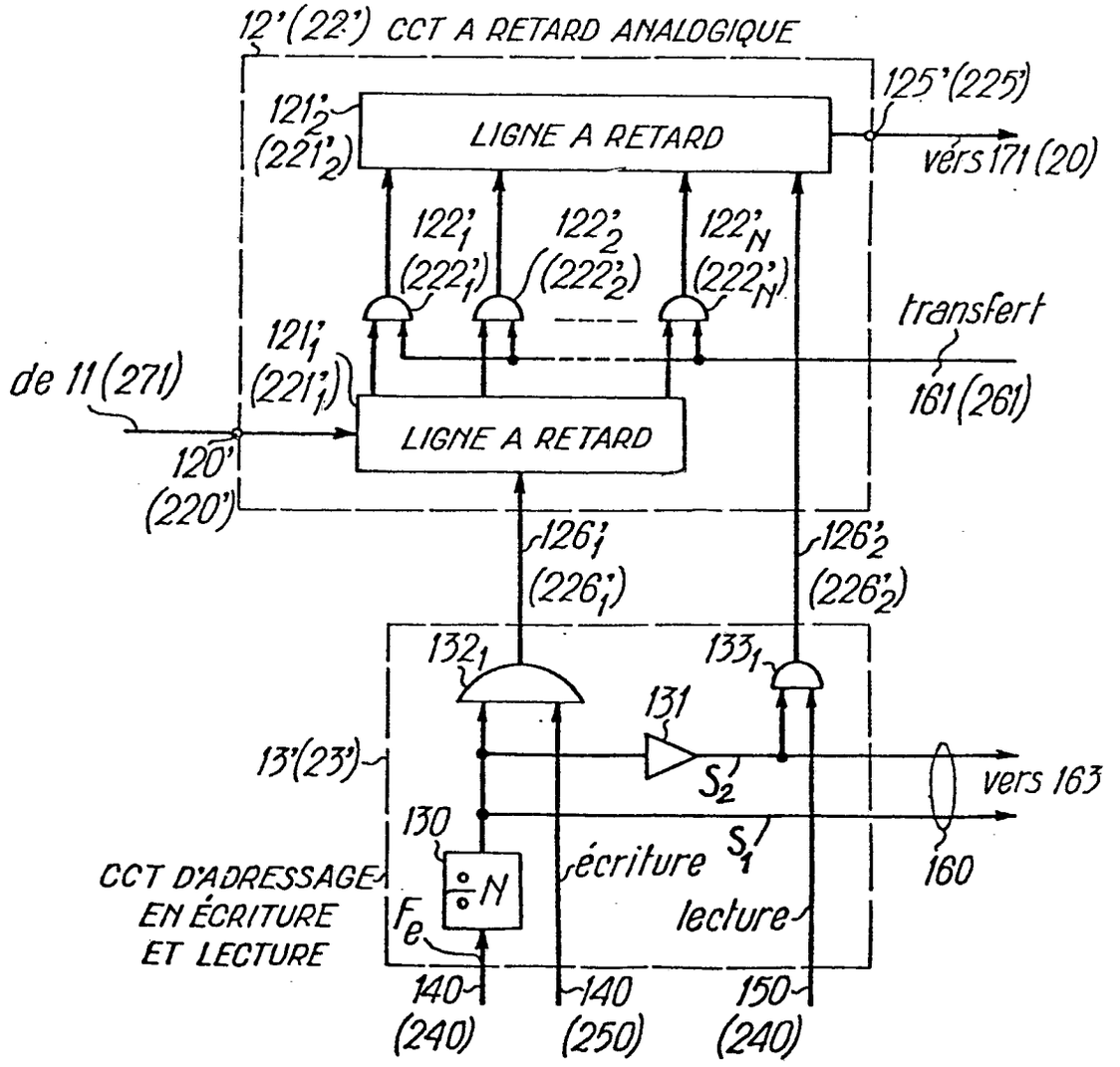

16
RAZ
vers 151, 155
de 14
161
141
163
164
de
130
et 131
S1
S2
MONOSTABLE
MODULATEUR
EN FRÉQUENCE
162
vers 172
160
CCT DE SYNCHRONISATION

FIG.6


12'(22') CCT A RETARD ANALOGIQUE
125'(225')
121'2
(221'2)
LIGNE A RETARD
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
Fe
lecture
140
(240)
140
(250)
150
(240)