



DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

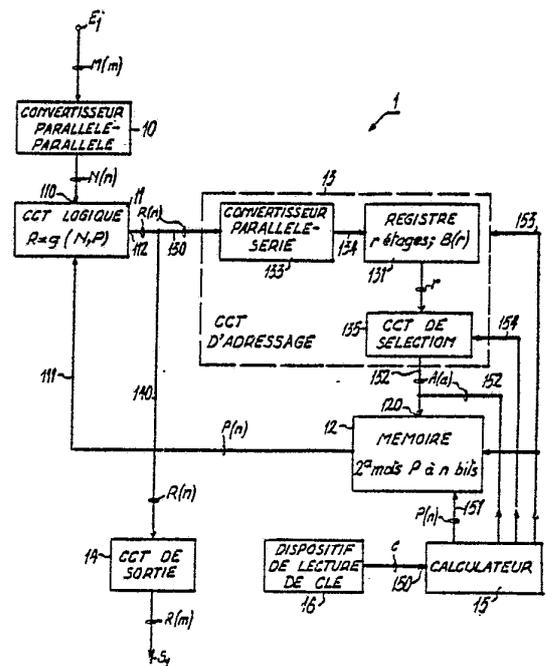
| | | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>(51) Classification internationale des brevets³ : H04L 9/02</p> | <p>A1</p> | <p>(11) Numéro de publication internationale: WO 84/ 04438 (43) Date de publication internationale: 8 novembre 1984 (08.11.84)</p> |
| <p>(21) Numéro de la demande internationale: PCT/FR80/00149 (22) Date de dépôt international: 10 octobre 1980 (10.10.80) (31) Numéro de la demande prioritaire: 79/25256 (32) Date de priorité: 10 octobre 1979 (10.10.79) (33) Pays de priorité: FR (71)(72) Déposants et inventeurs: BERNEDE, Georges, G. [FR/FR]; 106, rue de Malabry, F-92350 Le Plessis Robinson (FR). GREGEOIS, Jean, M. [FR/FR]; 1, avenue Carnot, F-94230 Cachan (FR). (74) Mandataire: CABINET MARTINET; 62, rue des Mathurins, F-75008 Paris (FR). (81) Etat désigné: US.</p> | | <p>Publiée <i>Avec rapport de recherche internationale. En vertu de l'article 64.3.c)ii) après publication d'un brevet résultant de la demande internationale ci-dessus et délivré par l'Office des brevets et des marques des Etats Unis le 14 février 1984 (14.02.84) sous le numéro 4,431,865.</i></p> |

(54) Title: ARRANGEMENT FOR THE ENCRYPTION AND DECRYPTION OF A DIGITAL SIGNAL

(54) Titre: INSTALLATION DE CHIFFREMENT ET DECHIFFREMENT D'UN SIGNAL NUMERIQUE

(57) Abstract

The arrangement comprises the encryption of a digital signal of n-bit words N_i into an encrypted signal of n-bit words R_i . In the encryption device (1), a logic circuit (11) generates each encrypted word R_i from a logic operation g effected on the word N_i and on a stored word P_{i-1} having n bits. An addressing circuit (13) elaborates an a-bit address word A_{i-1} belonging completely or partially at least to the preceding encrypted word R_{i-1} . A store (12) of predetermined 2^a words P_{i-1} is read out for each address word A_{i-1} to provide a corresponding word P_{i-1} to the logic circuit (11) so as to carry out the operation g so that $R_i = g(N_i, P_{i-1})$. The decryption device receives the encrypted words R_i to elaborate the address words A_i controlling the reading of the corresponding words P_i among 2^a stored words. Each decrypted word N_i is obtained by a logic operation h which is opposite to g and which is effected on the encrypted R_i and on the stored word P_{i-1} , so that $N_i = h(R_i, P_{i-1})$. The stores (12) may be programmed by computers (15) which compute according to a predetermined algorithm a table of words P_i for a given key (C). Application particularly to the encryption and decryption of teletexts.



(57) **Abrégé** L'installation consiste à chiffrer un signal numérique de mots N_i à n bits, en un signal chiffré de mots R_i à n bits. Dans le chiffreur (1), un circuit logique (11) produit chaque mot chiffré R_i à partir d'une opération logique g portée sur le mot N_i et sur un mot mémorisé P_{i-1} à n bits. Un circuit d'adressage (13) élabore un mot d'adresse A_{i-1} à a bits appartenant tout ou partie au moins au mot chiffré précédent R_{i-1} . Une mémoire (12) de 2^a mots P_{i-1} prédéterminés est lue par chaque mot d'adresse A_{i-1} pour transmettre un mot correspondant P_{i-1} au circuit logique (11) afin qu'il effectue l'opération g telle que $R_i = g(N_i, P_{i-1})$. Le déchiffreur reçoit les mots chiffrés R_i pour élaborer les mots d'adresse A_i commandant la lecture des mots correspondants P_i parmi 2^a mémorisés. Chaque mot déchiffré N_i est obtenu par une opération logique h dite contraire de g portée sur le mot chiffré R_i et sur le mot mémorisé P_{i-1} , telle que: $N_i = h(R_i, P_{i-1})$. Les mémoires (12) peuvent être programmables par des calculateurs (15) qui calculent, selon un algorithme prédéterminé, une table de mots P_i pour une clé donnée (C). Applications notamment au chiffrement et déchiffrement de télétextes.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

| | | | |
|----|--------------------------------------------|----|-----------------------|
| AT | Autriche | KR | République de Corée |
| AU | Australie | LI | Liechtenstein |
| BE | Belgique | LK | Sri Lanka |
| BG | Bulgarie | LU | Luxembourg |
| BR | Brésil | MC | Monaco |
| CF | République Centrafricaine | MG | Madagascar |
| CG | Congo | MR | Mauritanie |
| CH | Suisse | MW | Malawi |
| CM | Cameroun | NL | Pays-Bas |
| DE | Allemagne, République fédérale d' | NO | Norvège |
| DK | Danemark | RO | Roumanie |
| FI | Finlande | SD | Soudan |
| FR | France | SE | Suède |
| GA | Gabon | SN | Sénégal |
| GB | Royaume-Uni | SU | Union soviétique |
| HU | Hongrie | TD | Tchad |
| JP | Japon | TG | Togo |
| KP | République populaire démocratique de Corée | US | Etats-Unis d'Amérique |

INSTALLATION DE CHIFFREMENT ET DECHIFFREMENT D'UN
SIGNAL NUMERIQUE

La présente invention concerne une installation de chiffrement et déchiffrement d'un signal numérique convoyant des mots N_i à n bits, i désignant le rang du mot N_i dans le signal, en un signal chiffré numérique composé de mots R_i à n bits, comprenant, à l'émission dans un chiffreur, des moyens logiques effectuant une opération logique g appliquée sur chaque mot N_i et un mot prédéterminé P_{i-1} à n bits pour produire le mot correspondant chiffré $R_i = g(N_i, P_{i-1})$ et des moyens, qui comportent, en outre, un registre recevant les mots chiffrés R_i , pour produire les mots P_{i-1} selon un algorithme prédéterminé à partir des mots chiffrés R_i , et, à la réception dans un déchiffreur, des moyens logiques effectuant une opération logique h , dite contraire de l'opération g , appliquée sur chaque mot chiffré R_i et sur le mot prédéterminé P_{i-1} pour produire le mot correspondant déchiffré $N_i = h(R_i, P_{i-1})$ et des moyens de production des mots P_{i-1} analogues à ceux du chiffreur.

Les termes de chiffrement et de déchiffrement sont employés dans la présente description pour l'application particulière à un signal convoyant des caractères alphanumériques, bien que l'invention soit relative, de manière générale, à tout cryptage et décryptage, codage et décodage ou brouillage et débrouillage d'un signal numérique. On se réfère, dans la suite, en tant qu'exemple d'application, au signal numérique fourni par une installation de télétexte et convoyant à travers une voie de transmission d'un réseau de diffusion, par exemple d'images télévisées, des pages d'écriture destinées à être visualisées par des récepteurs de télévision classiques.

Pour une installation de télétexte, les pages d'écriture sont constituées de caractères alphanumériques portant l'information et de caractères nécessaires à la syntaxe, généralement transmis sous forme d'octets. A l'émission, le signal numérique convoyant les caractères est transmis à des moyens de multiplexage qui insèrent conve-

nablement le signal numérique dans le signal vidéo classique, par exemple dans les signaux de suppression et de synchronisation des trames. Après avoir été véhiculé à travers la voie de télévision, le signal composite est reçu dans le terminal de l'abonné et démultiplexé afin de séparer le signal numérique du signal vidéo. Un analyseur syntaxique permet de reproduire les pages d'écriture convoyées par le signal numérique pour les visualiser par le récepteur de télévision.

10 Le dispositif de contrôle d'accès mis en place dans une structure de télétexte est classique. L'abonné demandeur possède un moyen d'accès matérialisé par un support d'information sur lequel sont mémorisées toutes les données caractérisant l'abonné et sa zone accessible. 15 Le dispositif de contrôle acquiert ces informations et les compare, d'une part, aux données d'identification éventuellement présentes à bord du terminal, d'autre part, aux données caractérisant la demande de l'utilisateur. Si cette comparaison est positive, l'installation "donne accès" 20 aux informations.

Dans une installation de télétexte diffusé, les informations peuvent être reçues presque partout et sont donc accessibles par des moyens technologiques simples répandus dans le grand public. Des émissions sur des fréquences affectés spécialement à cet usage ne constitueraient qu'une protection illusoire. Il en est de même pour tout 25 dispositif qui conserverait les informations sous forme directement exploitable. En outre, l'apparition et la diffusion rapide de l'informatique "domestique" met à la disposition d'un nombre croissant de personnes des puissances de calcul non négligeables. Compte tenu de tout ceci, il apparaît indispensable de chiffrer non seulement les codes de commande de l'installation de télétexte, mais le message informatif tout entier. Ceci résoud par ailleurs le problème du secret éventuellement nécessaire pour certaines 30 utilisations institutionnelles des services de télétexte. 35

De manière générale, dans une installation de transmission chiffrée, on distingue :

- une source de messages N appartenant à l'ensemble des messages possibles ;

5 - un organe de chiffrement réalisant une fonction f qui, à un message N donné, fait correspondre un cryptogramme (message chiffré résultant) R appartenant à l'ensemble des cryptogrammes possibles, selon la relation :

$$R = f(N, C) = f_C(N)$$

10 où C est un mot de code appelé clé de chiffrement utilisée ;

- la voie de transmission à travers laquelle transitent les messages chiffrés R ;

15 - un organe de déchiffrement réalisant la fonction inverse f_C^{-1} de la fonction f_C qui fait correspondre au cryptogramme R le message N initial obtenu en dépendance de la clé C selon la relation :

$$N = f_C^{-1}(R) ; \text{ et}$$

- des moyens de distribution "sûrs" de la clé C.

20 Au regard de cette organisation, deux problèmes fondamentaux sont à résoudre, à savoir le choix d'une fonction f et le choix de la clé C et de sa distribution. La présente invention ne traite que de la résolution du premier problème.

25 Dans les installations de chiffrement et de déchiffrement les plus couramment utilisées, le chiffreur comporte une unité logique ayant deux bus d'entrée. L'un des bus reçoit les mots N_i à n bits du signal numérique à chiffrer et l'autre bus reçoit des mots prédéterminés P_i à n bits. L'opération logique qu'effectue l'unité logique est généralement une addition modulo 2 ; en d'autres termes, cette unité contient un jeu de portes OU - Exclusif
30 parallèles qui reçoivent chacune une paire de bits de même rang des deux mots associés N_i et P_i . La mise en œuvre de cette opération logique OU - Exclusif a l'avantage de
35 permettre son utilisation dans le chiffreur, en appliquant aux entrées d'une unité logique contenue dans le dé-



chiffreur analogue à celle du chiffreur, le mot chiffré correspondant R_i et le mot prédéterminé P_i pour restituer le mot déchiffré N_i .

5 Les moyens pour produire les mots prédéterminés P_i sont identiques dans le chiffreur et le déchiffreur. De manière générale, ils comportent un générateur de mots binaires aléatoires ou quasi-aléatoires qui sont directement représentatifs des mots prédéterminés P_i (brevet américain 4. 133. 974) ou dont les bits sont sélectionnés et subissent
10 des opérations logiques, par exemple au moyen de l'adressage d'une mémoire vive ou morte qui est adressée en lecture par certains bits des mots binaires aléatoires (demandes de brevet français 2.210.307 et 2.265.221).

L'inconvénient majeure de telle installation de
15 chiffrement et déchiffrement est qu'il est nécessaire de rendre synchrone les générateurs pseudo-aléatoires dans le chiffreur et le déchiffreur. En effet, le même mot prédéterminé P_i doit être appliqué en synchronisme avec le mot à chiffrer initial N_i et le mot chiffré R_i correspondant aux entrées des unités logiques du chiffreur et
20 du déchiffreur. En d'autres termes, le déclenchement du chiffrage doit être synchronisé avec le déclenchement du déchiffrage. Afin d'assurer que les deux générateurs pseudo-aléatoires soient déclenchés au même point de départ de
25 leur cycle de fonctionnement, il est connu de générer une séquence de bits connue appelée "donnée première". Cette "donnée première" est utilisée pour commander le déclenchement du fonctionnement du générateur pseudo-aléatoire dans le chiffreur. La "donnée première" est alors trans-
30 mise à travers la voie de transmission vers le déchiffreur afin que celui-ci la détecte pour commander le déclenchement du fonctionnement du générateur pseudo-aléatoire dans le déchiffreur.

Lorsque le déchiffrement est lié à la syntaxe du message,
35 le mot de "donnée première" peut être inséré entre les lignes du message du texte (demande de brevet français 2.210.307). Si le cryptage n'est pas lié à la syntaxe du



message, le mot de "donnée première" est émis en premier avant le message chiffré, Dans tous les cas, les deux générateurs pseudo-aléatoires commencent au même point de départ, par identification préalable d'une même
5 clé de message.

Corrélativement à cet inconvénient de synchronisation, la plupart des chiffreurs transmettent littéralement ce mot de "donnée première" sur la voie de transmission, de sorte qu'une personne non autorisée sera capable de détecter la "donnée première" par branchement en dérivation sur la voie de transmission, d'autant plus que la "donnée première" est exigée pour être transmise sur la voie de transmission antérieurement à l'opération de déchiffrement.
10

Le brevet américain 4, 133, 974 permet d'obvier en partie à cet inconvénient en chiffrant le mot de "donnée première" lui-même. En effet, selon ce brevet, le premier mot de synchronisation dit "donnée première" est transmis intégralement sur la voie de transmission, les autres mots de synchronisation suivants étant chiffrés.
15
20

On notera que d'autres installations de chiffrement et de déchiffrement fondées, non pas sur une opération logique des mots à chiffrer et des mots pseudo-aléatoires, mais sur une permutation et/ou un remplacement des mots chiffrés, nécessitent également la transmission d'un mot de synchronisation du chiffreur vers le déchiffreur. Par exemple, selon la demande de brevet allemand P 26 39 806.1-31, chaque mot à chiffrer est d'abord remplacé par un autre mot obtenu en adressant en lecture une mémoire contenant une table prédéterminée. Puis le mot lu dans cette mémoire subit une permutation simple. Ainsi, le mot chiffré obtenu remplace le mot du signal initial. Là encore, il est nécessaire de synchroniser le cryptage et le décryptage par un mot de synchronisation transmis avant le message chiffré, afin que l'adressage en lecture par chaque mot initial corresponde à l'adressage en lecture par le mot chiffré correspondant du mot initial.
25
30
35

Ainsi, tous les procédés de chiffrement et déchiffrement précités nécessitent la transmission d'un mot de synchronisation, généralement par période constante en dépendance de la syntaxe du message. En d'autres termes, deux messages initiaux identiques correspondent à un même message chiffré, ce qui limite considérablement la préservation contre tout déchiffrement non autorisé du message chiffré.

Pour se prémunir de tous ces inconvénients, l'article de S. JEFFERY et D.K. BRANSTAD, intitulé "Data Encryption", publié dans - Electro Conference Record -, El Segundo, Etat-Unis d'Amérique, 1977, pages 30/4 - 1 à 30/4 - 6, divulgue une installation de chiffrement et déchiffrement du genre décrit dans l'entrée en matière. Les moyens de production des mots prédéterminés P_i sont introduits dans une boucle de circuits logiques entre la sortie de l'unité logique du chiffreur, resp. du déchiffreur, et une entrée de cette unité logique. Dans ces conditions, les mots P_i sont prédéterminés par les mots à chiffrer, resp. chiffrés, eux-mêmes ; en d'autres termes, au début du fonctionnement de l'installation, les moyens de production des mots P_i se synchronisent eux-mêmes, sans nécessiter la transmission d'un mot de synchronisation particulier. En outre, cette autosynchronisation permet à deux messages identiques à chiffrer à des instants différents de faire correspondre deux messages chiffrés différents, du fait que le contenu du registre des moyens de production des mots P_i est, à priori, différent à ces deux instants. Ainsi, le déchiffrement d'un message chiffré obtenu par une telle installation est pratiquement irréalisable, car la personne non autorisée doit connaître non seulement les différentes clés utilisées et l'algorithme utilisé dans les moyens de production des mots P_i mais également le contenu initial des registres de ceux-ci.

Selon l'article précité, les moyens de production des mots P_i comprennent, entre un registre d'entrée relié à la sortie de l'unité logique et un registre de sortie



relié à une entrée de l'unité logique, une pluralité de circuits logiques effectuant des opérations logiques simples, telles que des permutations et des additions modulo 2 entre des groupes de bits du mot contenu dans le registre d'entrée et le mot de clé sélectionné. Ces opérations logiques sont répétées un grand nombre de fois par bouclage de la sortie vers l'entrée de l'ensemble des circuits logiques. Il apparaît alors, que pour un débit numérique donné des messages entrants, la vitesse de traitement des mots dans ces circuits logiques mise en œuvre doit être élevée, et par conséquent, contribue à un coût de l'ensemble de l'installation peu compatible avec des matériels accessibles au grand public.

La présente invention a donc pour but de fournir une installation de chiffrage et de déchiffrage du genre décrite dans l'entrée en matière dans laquelle les moyens de production des mots prédéterminés font appel à des circuits logiques fonctionnant au même débit numérique que les messages entrants. Comme on le verra dans la suite, au lieu que chaque mot prédéterminé soit calculé selon un algorithme déterminé pour chaque mot de message, au fur et à mesure de la transmission des mots du message, les mots prédéterminés selon l'invention sont calculés préalablement avant le chiffrage du message selon un algorithme prédéterminé par la clé, puis sont mémorisés dans une mémoire vive qui est lue à la même vitesse que le débit des mots à chiffrer, resp. chiffré.

A cette fin, l'installation de chiffrement et de déchiffrement est caractérisée en ce que chacun des moyens de production des mots prédéterminés P_{i-1} comprend des moyens ayant leur sortie reliée aux moyens logiques pour mémoriser 2^a mots P_{i-1} prédéterminés rangés à des adresses respectives A_{i-1} à a bits et des moyens reliés au registre pour adresser en lecture les moyens de mémorisation par lesdites adresses A_{i-1} dont les a bits appartiennent tout ou partie au mot contenu dans le registre.



Les fonctions g , dite de chiffrement, et h , dite de déchiffrement, font correspondre à chaque mot R_i d'un message à chiffrer un mot N_i du message chiffré, tous deux à n bits. Cette bijection est définie pour une table de mots mémorisés P_i . Cette table est déterminée par un algorithme convenable ou logiciel d'un ordinateur. Le calculateur reçoit pour un message donné un mot de code correspondant ou clé. Il calcule, selon l'algorithme en fonction de la clé donnée, les mots P_i et les écrit à des adresses respectives d'une mémoire programmable contenant 2^a cellules à n étages chacune. En phase de calcul, préalablement au chiffrement, resp. au déchiffrement, le calculateur du chiffreur, resp. du déchiffreur, commande la déconnexion des moyens d'adressage et de la mémoire programmable.

Selon une variante générale, les nombres n et a sont différents. Les moyens d'adressage peuvent comporter un registre à décalage recevant en série un nombre n de bits des mots R_i . Le contenu d'une adresse A_i dépend alors, non seulement des bits de mots précédemment chiffrés R_{i-1} , mais également des bits des mots chiffrés antérieurement R_{i-1} , R_{i-2} , ... Egalement, les moyens d'adressage peuvent comprendre des moyens commandés par le calculateur pour sélectionner a sorties du registre r , en fonction de la clé donnée. Ceci contribue encore à augmenter le secret du chiffrement.

En outre, le fait que l'adressage A_i dépend des mots chiffrés précédents, confère à l'installation, comme on le verra dans la suite, une propriété d'autosynchronisation. En d'autres termes, aucun mot supplémentaire n'est nécessaire pour synchroniser le chiffreur et le déchiffreur, car lorsqu'un mot chiffré est reçu erroné dans le déchiffreur, seulement un nombre J relativement faible de mots chiffrés suivants seront erronés, le $J+1$ ^{ème} mot chiffré étant assurément convenable. Ce nombre J dépend du rapport r/n .

Par ailleurs, afin d'accroître les propriétés de transparence de l'installation, le chiffreur et le déchiffreur peuvent comprendre à leurs entrées un convertisseur parallèle-parallèle convertissant le signal numérique à chiffrer à mots de m bits ($m \neq n$), respectivement chiffré et convoyé à travers la voie de transmission, en



un signal numérique à mots de n bits qui seront traités selon ce format dans le chiffreur et le déchiffreur, sans changement de débit numérique dans la voie de transmission. Aux sorties du chiffreur et du déchiffreur est alors prévu un convertisseur parallèle-parallèle effectuant la conversion inverse. La propriété d'universalité de l'installation est ainsi améliorée, car le chiffrement et le déchiffrement s'effectuent indépendamment du format des mots du signal numérique initial, et, bien entendu, du contenu et de la syntaxe de l'information transmise.

Un chiffreur élémentaire et un déchiffreur élémentaire tels que définis ci-dessus possèdent avantageusement la propriété d'être itérables à volonté, sans dégradation notable des propriétés inhérentes à l'installation. A cet égard, pour une installation comportant K couples de chiffreur et déchiffreur élémentaires, dont les fonctions logiques g et h sont dites contraires selon les relations précédentes, les chiffreurs élémentaires sont reliés en série selon leur indices croissants, de l'entrée vers la sortie du chiffreur global et les déchiffreurs élémentaires sont reliés en série selon leurs indices décroissant de l'entrée vers la sortie du déchiffreur. Une telle structure à au moins deux couples de chiffreur et déchiffreur élémentaires accroît considérablement la protection du secret, rendant quasi-impossible le déchiffrage par tout tiers ne connaissant pas les deux tables de mots P affectées aux deux couples.

Enfin, un autre avantage du chiffreur (resp. du déchiffreur) conforme à l'invention est que son entrée recevant le signal numérique à chiffrer et sa sortie délivrant le signal numérique chiffré sont de même nature. Ceci permet d'insérer le chiffreur, resp. le déchiffreur, dans une chaîne de circuits déjà existants.

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



- la Fig. 1 représente schématiquement le bloc-diagramme d'un chiffreur élémentaire conforme à l'invention ;
- la Fig. 2 représente schématiquement le bloc-diagramme d'un déchiffreur conforme à l'invention ; et
- 5 - les Figs. 3A et 3B représentent schématiquement une installation ayant une pluralité de couples de chiffreur et déchiffreur élémentaires analogues à ceux des Figs. 1 et 2.

La Fig. 1 représente schématiquement un chiffreur 10 1 conforme à l'invention. On notera dès maintenant que les liaisons entre les différents blocs de la Fig. 1 et également des Figs. 2, 3A et 3B sont des bus de fils parallèles, sauf indication contraire. Chaque bus est répertorié conjointement aux types de mots à bits parallèles qu'il 15 convoie.

L'entrée E_1 du chiffreur 1 reçoit un signal numérique sous forme de mots binaires $M(m)$ à m bits parallèles. Eventuellement, un convertisseur parallèle-parallèle 10 peut être prévu pour convertir le signal à mots $M(m)$ en un signal numérique à mots $N(n)$ ayant n bits parallèles, où n est différent de m . Les mots $N(n)$ sont transmis à n premières entrées parallèles 110 d'un circuit 20 logique 11 qui effectue une opération logique g . Cette opération porte sur deux mots $N_i(n)$ et $P_{i-1}(n)$, chacun ayant n bits parallèles. Le mot $P_{i-1}(n)$ est sélectionné en fonction de mots $N(n)$ ayant un rang inférieur à $i-1$ et transmis précédemment au mot $N_i(n)$. Le mot $P_{i-1}(n)$ est 25 délivré par une mémoire programmable 12 vers n secondes entrées parallèles 111 du circuit 11, comme on le verra dans la suite. Le bus de sortie 112 du circuit 11 transmet des mots résultant $R_i(n)$ à n bits parallèles, tels que :

$$R_i = g(N_i, P_{i-1})$$

L'opération g est une fonction combinatoire possédant les propriétés souhaitées au point de vue statistique.

Le mot R_i est fourni, à travers un bus à n fils 130, à un circuit d'adressage 13 et, à travers un bus à n fils

140, à un circuit de sortie 14. Le circuit de sortie 14 est composé d'un registre tampon précédant la sortie S_1 du chiffreur. Il comporte dans la cas où le convertisseur 10 est utilisé, un convertisseur parallèle-parallèle convertissant la suite des mots $R(n)$ en une suite de mots $R(m)$. Autrement, le circuit de sortie n'est pas indispensable.

Le circuit d'adressage 13 comprend un registre 131 à r étages. Le bus de sortie 132 du circuit d'adressage 13 transmet un mot d'adresse de lecture $A(a)$ à a bits ($a \leq r$), chaque fois qu'un mot entrant $R(n)$ est reçu sur le bus 130. Le bus de sortie 132 est relié à l'entrée d'adressage 120 de la mémoire 12 qui contient 2^a mots $P(n)$ à n bits. Ainsi, à chaque mot d'adressage $A(a)$ reçu à l'entrée 120, la mémoire 12 délivre par son bus de sortie 121 un mot $P(n)$ vers l'entrée 111 du circuit 11.

De manière générale, les nombres n , r et a sont différents. Dans ce cas, le circuit d'adressage 13 comprend ; par exemple, un convertisseur parallèle-série 133 qui convertit chaque mot parallèle $R(n)$ transmis par le bus 130 en un mot série qui est mémorisé, à travers le fil d'entrée 134 du registre, dans les premiers étages du registre à décalage 131 à r étages. Le contenu 131 évolue n bits par n bits en fonction des mots $R(n)$ entrants. Si on a $r < n$, seuls r bits de poids prédéterminés du mot $R(n)$ sont enregistrés et serviront à composer le mot d'adressage $A(a)$. Par contre, si on a $r > n$, tous les bits du mot $R(n)$ sont enregistrés dans le registre 131. Ceux-ci serviront, conjointement avec les $(r-n)$ bits précédemment enregistrés et provenant des mots précédents $R(n)$ et, éventuellement, du contenu initial du registre 131, à composer les mots d'adresse $A(a)$. Selon une troisième variante, si on a $n = r$ ou $n > r$, le convertisseur 133 n'est pas nécessaire et le registre 131 est un simple registre tampon recevant en parallèle les n bits ou r bits de chacun des mots $R(n)$.

Egalement dans le cas général, r est différent de a ,



mais, bien entendu, supérieur à a . Un circuit 135 sélectionne a sorties du registre à décalage 131 parmi r . Ce circuit 135 est composé classiquement de portes ET parallèle, et transmet sur le bus 132 un mot $A(a)$ chaque fois qu'un mot $R(n)$ est émis par le bus de sortie 112 du circuit logique 11. Cependant, selon la variante où $r = a$, le circuit de sélection de sortie 135 est supprimé, et les r sorties du registre 131 sont reliées directement aux entrées d'adressage 120 de la mémoire 12.

Ainsi, il apparaît que, pour un mot entrant $N_i(n)$ dans le circuit logique 11, le circuit d'adressage 13 transmet un mot $A_{i-1}(a)$, qui est déduit du contenu du registre 131 et qui est constitué par certains bits des mots résultants précédents $R_{i-1}(n)$, $R_{i-2}(n)$, Un mot $P_{i-1}(n)$ est lu dans la cellule de la mémoire 12 à l'adresse $A_{i-1}(a)$ et est combiné au mot $N_i(n)$ dans le circuit 11 pour donner le mot résultant $R_i = g(N_i, P_{i-1})$. Au rythme des mots $N(n)$, resp. $M(m)$, des mots sortants $R(n)$, resp. $R(m)$, sont transmis à la sortie S_1 du chiffreur.

Préalablement à la phase de traitement du message entrant $M(m)$ ou $N(n)$ dans le chiffreur 1, on procède à l'écriture de la table de chiffrement dans la mémoire 12, qui est une mémoire programmable. On rappelle que cette table est constituée de 2^a mots $P(n)$ de n bits, certains pouvant être égaux. L'établissement de cette table est effectué par un calculateur 15 composé essentiellement par un micro-processeur associé à un logiciel. L'utilisation de la table ne fait ensuite appel qu'à de la circuiterie et est donc rapide et simplement limité par la technologie des circuits utilisés. Le logiciel représente un algorithme établi une fois pour toutes. En fonction d'un mot de code ou clé C reçu à l'entrée 150 du calculateur, l'algorithme permet de calculer des mots $P(n)$ qui sont transmis sur un bus de sortie 151 du calculateur et qui sont écrits respectivement dans des cellules de la mémoire 12 préalablement adressées par le calculateur 15 sous forme de mots $A(a)$, à travers un bus de sortie 152 relié à l'entrée d'adressage

120 de la mémoire. En outre, dès que le calculateur 15 reçoit sur son entrée 150 une clé C, celui-ci émet sur un fil de sortie 153 un signal d'ordre vers le circuit d'adressage 13, en particulier vers le registre 131, et vers la mémoire 12. Le circuit d'adressage 13 est alors déconnecté de la mémoire 12, c'est-à-dire présente une résistance élevée sur un bus 132, et la mémoire programmable 12 est en phase d'écriture ou d'écriture-lecture si le calculateur 15 est conçu pour vérifier si un mot $P(n)$ a bien été écrit à la cellule correspondant à l'adresse fournie. Dès que le calculateur 15 a terminé la phase de calcul et de mémorisation des 2^a mots $P(n)$, la boucle des circuits 12, 11 et 13 est de nouveau fermée et le chiffreur traite le signal numérique entrant $N(n)$ resp. $M(m)$.

Complémentairement, le circuit de sélection 135 sélectionne les r sorties du registre 131 peut être prévu programmable. Dans ce cas, pour une clé C donnée, le calculateur 15 adresse, à travers un bus 154, pendant la phase initiale de calcul et de mémorisation, a mots d'adresses sélectionnant a sorties parmi r .

La transmission de la clé C à l'entrée 150 du calculateur est commandée par un dispositif de lecture de clé 16 dépendant du support d'enregistrement de la clé. En général, pour le chiffreur 1 qui est inclus dans les moyens d'émission du signal à chiffrer destiné à être transmis vers différents usagers, le dispositif de lecture 16 comporte un clavier ou des roues codeuses au moyen duquel un mot alphanumérique représentant la clé convenablement codée, par exemple, en code décimal codé binaire, est attribué à chaque signal numérique, qu'il convient de chiffrer, pour rendre sélective sa détection chez les usagers. En outre, deux voyants à diodes électroluminescentes peuvent être prévus afin de signaler au programmeur que le calculateur 15 est en phase de calcul de la table des mots $P(n)$ ou a terminé celle-ci, auquel cas le programmeur déclenchera la transmission du message.

La Fig. 2 représente schématiquement le bloc-diagramme du déchiffreur 2 associé à celui du chiffreur 1 de la Fig. 1. Le déchiffreur 2 est localisé dans les moyens de réception de chaque usager.

5 Il comporte, comme le chiffreur 1 et identiquement quant à leurs structures, respectivement par rapport aux circuits 10, 12, 13, 14 et 15, un convertisseur parallèle-parallèle 20, une mémoire programmable 22, un circuit d'adressage 23, un circuit de sortie 24 et un calculateur
10 25. Les différentes variantes déterminées par les rapports entre les nombres \underline{n} , \underline{r} et \underline{a} correspondent respectivement à des structures des circuits 20, 22, 23, 24 et 25 identiques à celles décrites précédemment pour les circuits 10, 12, 13, 14 et 15 du chiffreur. On notera, à cet égard, que
15 les circuits et liaisons équivalents dans le chiffreur 1 et le déchiffreur 2 sont repérés par un même nombre à deux chiffres précédé par un 1 pour le chiffreur et par un 2 pour le déchiffreur. On considérera ci-après le cas général pour lequel les entiers \underline{n} , \underline{r} et \underline{a} sont différents.

20 L'entrée E_2 du déchiffreur 2 reçoit un message numérique à déchiffrer qui est composé de mots $R(m)$ à \underline{m} bits parallèles, tels que ceux transmis par la sortie S_1 du chiffreur 1. Le convertisseur parallèle-parallèle 20 convertit les mots $R(m)$ en des mots $R(n)$ à \underline{n} bits
25 parallèles transmis de son bus de sortie 200 vers les bus d'entrée 210, 230 d'un circuit logique 21 et du circuit d'adressage 23. Comme dans le chiffreur 1, le circuit d'adressage 23 du déchiffreur transmet un mot d'adresse $A(a)$ sur son bus de sortie 232 vers l'entrée d'adressage
30 220 de la mémoire 22, chaque fois qu'il reçoit un mot $R(n)$. Le registre 231 du circuit d'adressage 23 comporte également \underline{r} étages. Lorsque sont prévus des circuits de sélection figés 135 et 235, ces derniers sélectionnent toujours des sorties de mêmes rangs prédéterminés des registres 131 et 231, respectivement. Si les circuits d'adressage 135 et 235 sont programmables par les calculateurs respectifs 15 et 25 à travers les bus 154 et 254,

15.

ils sélectionnent des sorties des registres 131 et 231 dont les rangs sont programmés en fonction d'une même clé C reçue à l'entrée 150, 250 des calculateurs 15, 25. Pour une même clé C, le calculateur 25, soumis à un logiciel
 5 identique à celui du calculateur 15, fournit, à travers le bus 251, des mots $Q(n)$ à la mémoire 22, qui sont respectivement identiques aux mots $P(n)$ et qui correspondent à des adresses $A(a)$ transmises à travers le bus 252 vers
 10 l'entrée d'adressage 220 de la mémoire 22. Ainsi, la phase de calcul du calculateur 25 est identique à celle du calculateur 15 et, après cette phase, la table contenue dans la mémoire 22 est identique à celle contenue dans la mémoire 12, pour une même clé, c'est-à-dire que chaque couple (A, Q) est identique à un couple (A, P) .

15 Le dispositif de lecture de clé 26 du déchiffreur 2 transmet la clé C à l'entrée 250 du calculateur et peut être différent de celui 16 du chiffreur 1. En particulier, le dispositif 26 peut être constitué par un appareil du genre à tête magnétique qui lit la clé C enregistrée sur
 20 une carte permettant à l'organisme de diffusion des programmes ou messages transmis sous la forme de signaux numériques chiffrés $R(m)$ de contrôler la télédistribution chez les usagers.

Le circuit logique 21 reçoit en synchronisme à
 25 ses entrées 210, 211 deux mots $R(n)$ et $Q(n)$ à n bits chacun. Il réalise une fonction logique h dite "contraire" - ainsi appelée parce qu'elle ne peut être définie comme fonction réciproque ou inverse au sens mathématique propre - telle que le mot résultant R' à n bits transmis à la sortie 212
 30 - du circuit 21 est donné par la relation suivante :

$$R'_i = N_i = h(R_i, Q_{i-1}) \text{ lorsque } R_i = g(N_i, P_{i-1})$$

avec $Q_{i-1} = P_{i-1}$

Ces relations sont vérifiées lorsque la synchronisation est établie entre le chiffreur 1 et le déchiffreur
 35 2, c'est-à-dire lorsque le contenu du registre 231 devient identique à celui du registre 131. Lorsque le registre 231 a enregistré dans ses premiers étages tout $(r > n)$ ou



partie ($r < n$) d'un mot $R_i(n)$ de rang i , le circuit d'adresse 23 sélectionne l'adresse $A_i(a)$ afin que le mot $Q_i(n)$ tel que $Q_i(n) = P_i(n)$ soit lu dans la mémoire 22. Le circuit logique 21 reçoit alors simultanément

5 sur ses entrées 210 et 211 les mots $R_{i+1}(n)$ et $Q_i(n)$ et produit à sa sortie le mot $R'_{i+1} = h(R_{i+1}, Q_i) = h(R_{i+1}, P_i)$. Or, d'après la propriété précédemment énoncée de la fonction h "contraire" de g et la relation $R_{i+1} = g(N_{i+1}, P_i)$, on obtient :

$$10 \quad R'_{i+1}(n) = N_{i+1}(n)$$

Il reste cependant à montrer que la synchronisation est atteinte et à calculer le délai nécessaire, c'est-à-dire le nombre de mots requis devant être reçus par le déchiffreur 2 pour obtenir la synchronisation. Il apparaît,

15 à cet égard, que cette propriété peut être qualifiée d'autosynchronisation et qu'il n'est exigé aucun signal supplémentaire précédant le message à chiffrer à l'émission dans le chiffreur 1 et devant être déchiffré à la réception dans le chiffreur 2.

20 A l'initialisation, c'est-à-dire lors de la phase de calcul et de mémorisation commandée par le calculateur 15 du chiffreur 1, resp. le calculateur 25 du déchiffreur 2, les contenus des registres 131 et 231 sont $B_0(r)$ et $D_0(r)$, quelconque et a priori différents.

25 Le premier mot $N_1(n)$ est appliqué à l'entrée 110 du circuit logique 11 du chiffreur qui transmet le mot résultant

$$R_1(n) = g(N_1, P [B_0])$$

sur le bus 112 pour son chargement dans le registre 131 et, à travers éventuellement le circuit 14, le mot correspondant

30 $R_1(m)$. Le mot $P [B_0]$ correspond à celui lu dans la mémoire 12 à l'adresse correspondant au contenu B_0 du registre 131 après sélection par le circuit 135. Après que le mot $R_1(m)$ et éventuellement, en partie ses suivants $R_2(m), R_3(m), \dots$,

35 si $\underline{m} \neq \underline{n}$, soit convoyé par la voie de transmission convenable entre le chiffreur 1 et le déchiffreur 2, l'entrée 210 du circuit 21 du déchiffreur reçoit le mot $R_1(n)$. Le

circuit 21 calcule $R'_1(n) = h(R_1, Q [D_0])$ où $Q [D_0]$ correspond au mot lu dans la mémoire 22 à l'adresse correspondant au contenu D_0 du registre 231 après sélection par le circuit 235. On a, bien entendu, $R'_1(n) \neq N_1(n)$, car le déchiffrement n'a pas été réalisé avec le contenu ($D_0 \neq B_0$) du registre d'adresse 131. Par ailleurs, $R_1(n)$ a été mémorisé (tout ou partie) dans les registres 131 et 231 dont les contenus sont devenus $B_1(r)$ et $D_1(r)$. Dans ce cas, on constate que les contenus B_1 et D_1 ont au plus n bits identiques appartenant au mot $R_1(n)$. Si $r \leq n$, la suite des mots $N_2(n), N_3(n) \dots$ reçus par le chiffreur 1 et la suite des mots $R'_2(n), R'_3(n) \dots$ calculés dans le déchiffreur 2 deviennent alors égales. Par contre, si $r > n$, les contenus des registres 131 et 231 ne sont pas identiques, tant qu'il reste dans les étages de poids faible des registres 131 et 231 des bits de poids fort appartenant respectivement aux mots $B_0(r)$ et $D_0(r)$. Le déchiffrement devient correct quand les contenus de ces registres sont identiques, c'est-à-dire lorsque tous les bits des mots B_0 et D_0 ont été chassés et remplacés par des bits de mots $R(n)$. Ceci nécessite l'envoi de J mots sur la voie de transmission, où l'entier J est défini par :

$$J = \text{ENT} \left[\frac{r}{n} \right] \text{ si } r = 0 \text{ modulo}(n)$$

$$\text{ou } J = \text{ENT} \left[\frac{r}{n} \right] + 1 \text{ si } r \neq 0 \text{ modulo}(n)$$

où ENT désigne la fonction partie entière.

Le mot $R_{J+1}(n)$ de rang $J+1$ est ensuite déchiffré correctement. J sera nommé délai d'autosynchronisation.

Par ailleurs, on remarquera que, pour une même clé C et un même message $M(m)$, resp. $N(n)$, à chiffrer, deux chiffrements de ce message produisent a priori deux messages chiffrés $R(m)$, resp. $R(n)$, qui sont différents, puisque, à deux instants donnés, les contenus initiaux $B_0(r)$ du registre 131 sont a priori différents. Cette propriété accroît avantageusement le secret de l'information à transmettre.

L'autosynchronisation a une conséquence importante sur la propagation des erreurs dues à la voie de transmission entre le chiffreur et le déchiffreur. On suppose



qu'un mot $R_i(n)$ chiffré par le chiffreur donne, après
 convoyage à travers la voie de transmission, un mot $R_i^*(n)$
 sur le bus 200 du déchiffreur. Dans ces conditions, le
 mot $N_i^*(n)$ résultant du déchiffrement du mot $R_i^*(n)$ est
 5 erroné ($N_i^*(n) \neq N_i(n)$). Par ailleurs, le déchiffrement
 des J mots suivants non erronés $R_{i+1}(n)$ à $R_{i+J}(n)$ sera
 faux puisque, d'après l'autosynchronisation, J mots sont
 nécessaires pour que les contenus des registres 131 et
 231 redeviennent identiques. Si l'on généralise le cas
 10 particulier précédent, au cas où des erreurs sont trans-
 mises / dans un paquet composé de I mots erronés $R_i^*(n)$ à
 $R_{i+I}^*(n)$, alors à la réception dans le déchiffreur 2, il
 faudra déchiffrer $I+J$ mots $R_i^*(n)$ à $R_{i+I+J}^*(n)$ pour que
 le déchiffrement redevienne correct. Dans tous les cas,
 15 la propagation d'erreurs est limitée à J mots.

En se reportant aux Figs. 3A et 3B, on a repré-
 senté schématiquement les structures d'un chiffreur et
 d'un déchiffreur déduites de celles 1, 2 des Figs. 1, 2
 par réitération. Ils comportent respectivement K chiffreurs
 20 élémentaires 1_1 à 1_K selon la Fig. 1 et K déchiffreurs
 élémentaires 2_1 à 2_K selon la Fig. 2.

A la Fig. 3A, on retrouve dans chaque chiffreur
 élémentaire 1_k ($1 \leq k \leq K$) une boucle constituée par un cir-
 cuit 11_k qui effectue l'opération logique g_k , un circuit
 d'adressage 13_k qui comprend un registre r_k étages et
 25 transmet des mots d'adresse $A(a_k)$ où $a_k \leq r_k$, et une mémoire
 12_k qui possède 2^{a_k} cellules enregistrant chacune un mot
 P_k à n bits. Le bus d'entrée 110_1 du premier chiffreur
 élémentaire 1_1 est relié à l'entrée E_1 du chiffreur glo-
 30 bal, éventuellement à travers le convertisseur parallèle-
 parallèle 10 qui reçoit le message à chiffrer $M(m)$. Le
 dernier chiffreur élémentaire 1_K a son bus de sortie 140_K
 qui est relié au circuit de sortie 14 qui transmet par
 la sortie S_1 du chiffreur global le message chiffré $R(m)$
 35 vers la voie de transmission. Le bus d'entrée $110_2, \dots, 110_K$
 du circuit logique $11_2, \dots, 11_K$ d'un chiffreur élémentaire
 1_2 à 1_K est reliée au bus de sortie $140_1 \dots 140_{K-1}$ du chif-
 freur élémentaire précédent $1_1 \dots 1_{K-1}$ respectivement.

Chaque chiffreur élémentaire, tel que 1_1 ou 1_K , par exemple, peut inclure un calculateur, tel que 15_1 ou 15_K , associé à une mémoire programmable, telle que 12_1 ou 12_K . Le calculateur reçoit par son entrée, telle que
5 150_1 ou 150_K , un mot codé ou clé élémentaire, telle que C_1 ou C_K , qui lui est propre pour un message à chiffrer donné, au moyen d'un dispositif de lecture commun 17, du genre de celui déjà décrit 16. Le support d'enregistrement du dispositif de lecture 17 (resp. 27 du déchiffreur)
10 contient une clé C composé par la suite des clés élémentaires et des adresses des calculateurs des chiffreurs élémentaires (resp. des déchiffreurs élémentaires). Cependant, certains chiffreurs élémentaires, tels que 1_2 , ne comportent pas de calculateur. La mémoire, telle que
15 12_2 , de ces chiffreurs est alors une mémoire morte contenant à chaque adresse $A_i(a_k)$ le mot correspondant $P_{i,k}(n)$. Le circuit de sélection d'adresses de celle-ci, tel que 135_2 , s'il existe, n'est pas programmable.

Les déchiffreurs élémentaires 2_K à 2_1 du déchiffreur
20 de la Fig. 3B comprennent chacun également une boucle fermée analogue à celle 2 de la Fig. 2. Pour un déchiffreur élémentaire 2_k ($1 \leq k \leq K$), on y retrouve un circuit d'adressage 23_k et une mémoire 22_k identiques à ceux 13_k et 12_k du chiffreur élémentaire 1_k . Si les mémoires 12_k
25 et 22_k sont programmables, le déchiffreur 2_k comprend également un calculateur 25_k dont le logiciel et le microprocesseur sont identiques à ceux du calculateur 15_k et qui est commandé par un dispositif de lecture commun 27, du genre de celui 26 montré à la Fig. 2. Comme déjà
30 dit, une clé commune est composée de clés élémentaires C_k qui sont adressées par le dispositif 27 respectivement aux entrées 250_k des calculateurs 25_k des déchiffreurs élémentaires correspondants 2_k .

Afin d'assurer convenablement le déchiffrement,
35 par correspondance deux à deux d'un chiffreur élémentaire 1_k et d'un déchiffreur élémentaire 2_k , les déchiffreurs élémentaires sont reliés successivement, suivant leur



indice décroissant K à 1 , à partir de l'entrée E_2 du déchiffreur global. Le bus d'entrée 200_K du déchiffreur 2_K est relié à l'entrée E_2 , éventuellement à travers le convertisseur parallèle-parallèle 20 si le chiffreur global effectue une conversion de mots $M(m)$ en mots $N(n)$.
 5 Le bus de sortie 212_1 du circuit logique 21_1 du déchiffreur élémentaire 1_1 est relié à travers le circuit de sortie 24 à la sortie S_2 . Le bus de sortie $212_K \dots$
 10 212_2 , du circuit logique $21_K, \dots, 21_2$ de chaque déchiffreur élémentaire $2_K \dots 2_2$, est relié au bus d'entrée $200_{K-1}, \dots, 200_1$ du déchiffreur élémentaire suivant $2_{K-1}, \dots, 2_1$, respectivement.

Chaque déchiffreur élémentaire 1_k réalise, en outre, au moyen de son circuit logique 21_k , la fonction
 15 "contraire" h_k de celle g_k du circuit logique 11_k du chiffreur correspondant 1_k . Le secret obtenu par un tel couple de chiffreur et déchiffreur globaux est considérablement accru au prix d'une plus grande complexité de la circuiterie.

20 Par ailleurs, si on désigne J_k le délai d'auto-synchronisation d'un déchiffreur élémentaire 2_k , le délai d'autosynchronisation J du déchiffreur global composé de K déchiffreurs élémentaires 2_1 à 2_K est donné par la somme suivante :

$$25 \quad J = \sum_{k=1}^K j_k$$

dans laquelle $j_k = \text{ENT} \left[\frac{r_k}{n} \right]$ si $r_k = 0 \text{ modulo}(n)$
 ou $j_k = \text{ENT} \left[\frac{r_k}{n} \right] + 1$ si $r_k \neq 0 \text{ modulo}(n)$

A titre d'exemple on limitatif, deux applications du chiffrement et du déchiffrement conformes à l'invention sont décrites ci-après.

30 La première application concerne un message transmis selon les prescriptions de l'installation de télétexte français dit ANTIOPE (Acquisition Numérique et Télévisualisation d'Images Organisées en Pages d'Écritures). Dans



Dans le cas où l'utilisateur n'a pas introduit dans le dispositif de lecture 26 la clé correspondant au chiffrement du message transmis, c'est-à-dire du magazine qu'il désire visualiser, les images transmises après déchiffrement sont complètement illisibles. Eu égard au chiffrement complexe mis en oeuvre selon l'invention, l'utilisateur, quand bien même il serait un homme du métier, est incapable de déchiffrer les pages visualisées. En effet, il doit connaître la table des mots $P = Q$ dans les mémoires 12 et 22, mais également connaître l'état initial $C_0(8)$ du registre 131 avant le chiffrement, lequel diffère à priori pour chaque transmission de message. Si l'utilisateur détermine la table des mémoires 12 et 22 pour un message, il ne pourra pas néanmoins la réutiliser pour un autre message, puisque, à chaque clé identifiant un message, correspond une table $P = Q$ déterminée par l'algorithme inhérent aux calculateurs 15 et 25.

Selon une réalisation préférée, les opérations logiques g et h sont le "OU" exclusif de l'algèbre de Boole portant sur chacune des 8 paires de bits de même poids des mots $N(8)$ et $P(8)$ dans le chiffreur et des mots $R(8)$ et $Q(8)$ dans le déchiffreur. Chaque circuit logique 11, 21 comprend ainsi 8 portes logiques OU exclusif, chacune d'elles ayant une entrée reliée à un fil du bus 110, 210 et une entrée reliée à un fil du bus 121, 221. Il apparaît que les relations définissant la fonction h dite "contraire" de g

$N = h(R, Q = P)$ lorsque $R = g(N, P)$
sont applicables aux fonctions OU exclusif $g = h$, désignées ci-après par le signe \oplus :

$$N = R \oplus P \quad \text{lorsque } R = N \oplus P$$

Une seconde application est relative à toute installation de télévision cryptée basée sur des transformations des tensions électriques représentatives d'une partie d'image télévision (ligne, point, etc.), commandées par un message binaire caractéristique de l'émission reçue.



cette installation, le message est composé de pages destinées à être visualisées par les récepteurs de télévision classiques chez les usagers. Chaque page est organisée en rangées de caractères. Le contenu d'une page est ainsi constitué, d'une part de caractères nécessaires à la mise en page et constituant la syntaxe, c'est-à-dire la position du début de page, de ligne, le numéro de ligne, etc... Chacun de ces caractères alphanumériques est transmis sous la forme d'un mot à 8 bits N(8) ou octets. L'ensemble de ces caractères constituant le message est directement transmis à l'entrée 110 du circuit logique 11 du chiffreur. Tous les mots N, R, A et P sont des octets et les chiffreur et déchiffreur ont une structure suivant la variante simple où $m = n = r = a = 8$. Les convertisseurs 10 et 20 sont supprimés et les circuits d'adressage 13, 23 ne comporte chacun qu'un simple registre tampon 131, 231 à 8 étages. Le bus 140 sortant du chiffreur est ensuite transmis à un multiplexeur vidéo qui est destiné à insérer le signal numérique chiffré R(8) dans certaines lignes appartenant au signal de suppression et de synchronisation de trames d'un signal de télévision en couleurs classique, ce signal conservant son contenu propre. Selon une autre variante, le signal numérique chiffré R(8) peut occuper la totalité de la voie télévision (utilisation "plein canal"). Le chiffreur est interconnecté entre la source de message ANTIOPE et le multiplexeur, en prenant les précautions d'usage d'adaptation électrique.

A la réception dans le local de l'utilisateur, un terminal comporte un démultiplexeur vidéo afin de séparer le signal de télévision classique transmis vers le récepteur de télévision et le signal numérique chiffré R(8). Ce dernier est reçu par l'entrée 200 du déchiffreur qui délivre le signal N(8) déchiffré à un analyseur de syntaxe ANTIOPE. L'analyseur syntaxique fournit des ordres à un dispositif de visualisation qui élabore les pages du message ANTIOPE présentées ensuite sur le tube cathodique du récepteur.



Une telle installation est par exemple l'installation de télévision cryptée française dite DISCRET (DISpositif de CRyptage pour Emission de Télévision) qui est destiné à la transmission d'émissions strictement
5 assignées à un groupe de téléspectateurs particuliers. Le procédé mis en oeuvre par cette installation est fondé sur l'inversion et le décalage, par lignes de retard, des lignes du signal vidéo, ces opérations étant commandées par un générateur pseudo-aléatoire classique à bascules
10 bistables et rebouclages par portes logiques du genre OU exclusif. Deux mots informatifs numériques sont nécessaires pour le fonctionnement du générateur pseudo-aléatoire. Un premier mot dit de configuration indique les rebouclages effectués et, par suite, identifie la séquence
15 générée. Un second mot dit de synchronisation est chargé dans les bascules à des instants prédéterminés et indique le début de la séquence.

Dans l'installation DISCRET, le mot de synchronisation est modifié périodiquement en transportant son contenu binaire à l'aide d'une procédure selon l'installation française DIDCN (DIffusion de DONnées) identique à celle du transport selon l'installation ANTIOPE. Conformément à l'invention, le chiffrement et le déchiffrement par un chiffreur et un déchiffreur selon les Figs. 1 et 2
25 s'applique, en tant que mots $M(m)$ ou $N(n)$, aux mots de synchronisation de l'installation DISCRET.

Selon une autre application complémentaire de la précédente, le chiffreur selon la Fig. 1 a son entrée E_1 reliée à la sortie du générateur pseudo-aléatoire de
30 l'installation DISCRET. Sa sortie S_1 délivre la séquence pseudo-aléatoire chiffrée. A la réception, le déchiffreur selon la Fig. 2 est connecté en amont du générateur pseudo-aléatoire et délivre par sa sortie S_2 la séquence déchiffrée. Le mot de configuration, qui ne subit pas de
35 chiffrement et déchiffrement, peut être utilisé comme clé C et, par suite, peut être transmis aux entrées 150, 250 des calculateurs 15, 25.



De manière générale, on notera qu'un signal numérique quelconque du genre pseudo-aléatoire, mais également un signal de bruit, peut être retransmis sans perte d'information à la sortie du déchiffreur, après
5 avoir subi un chiffrement et un déchiffrement conformes à l'invention.



REVENDICATIONS

1 - Installation de chiffrement et déchiffrement d'un signal numérique convoyant des mots N_i à n bits, i désignant le rang du mot N_i dans le signal, en un signal chiffré numérique composé de mots R_i à n bits, comprenant, à l'émission dans un chiffreur (1), des moyens logiques (11) effectuant une opération logique g appliquée sur chaque mot N_i et un mot prédéterminé P_{i-1} à n bits pour produire le mot correspondant chiffré $R_i = g(N_i, P_{i-1})$ et des moyens (12, 13), qui comportent, en outre, un registre (131) recevant les mots chiffrés R_i , pour produire les mots P_{i-1} selon un algorithme prédéterminé à partir des mots chiffrés R_i , et, à la réception dans un déchiffreur (2), des moyens logiques (21) effectuant une opération logique h , dite contraire de l'opération g , appliquée sur chaque mot chiffré R_i et sur le mot prédéterminé P_{i-1} pour produire le mot correspondant déchiffré $N_i = h(R_i, P_{i-1})$ et des moyens de production des mots P_{i-1} (22, 23) analogues à ceux (12, 13) du chiffreur, caractérisée en ce que chacun des moyens de production des mots prédéterminés P_{i-1} (12, 13 ; 22, 23) comprend des moyens (12 ; 22) ayant leur sortie reliée aux moyens logiques (11 ; 21) pour mémoriser 2^a mots P_{i-1} prédéterminés rangés à des adresses respectives A_{i-1} à a bits et des moyens (135 ; 235) reliés au registre (131 ; 231) pour adresser en lecture les moyens de mémorisation (12 ; 22) par lesdites adresses A_{i-1} dont les a bits appartiennent tout ou partie au mot contenu dans le registre (131 ; 231).

2 - Installation conforme à la revendication 1, dans laquelle chaque registre est un registre à décalage à r étages, caractérisée en ce que chaque registre à décalage (131 ; 231) reçoit en série, à travers un convertisseur parallèle-série (133 ; 233), les mots chiffrés R_i .

3 - Installation conforme à la revendication 1, caractérisée en ce que chaque registre comporte un nombre r d'étages inférieur ou égal à n qui reçoivent en parallèle des bits des mots chiffrés R_i .



4 - Installation conforme à la revendication 2 ou 3, caractérisée en ce que chacun des moyens d'adressage (13 ; 23) comprend des moyens (135, 235) pour sélectionner a sorties dudit registre (131 ; 231) parmi r afin de transmettre auxdits moyens de mémorisation (12 ; 22) lesdites adresses A_i à a bits.

5 - Installation conforme à l'une des revendications 1 à 4, caractérisée en ce que chacun des moyens de mémorisation (12, 22) est une mémoire programmable par un calculateur (15 ; 25) qui, initialisé en phase de calcul, commande la déconnexion des moyens d'adressage (13 ; 23) et de la mémoire (12, 22) afin de calculer selon un algorithme prédéterminé et sélectivement en fonction d'un mot de code prédéterminé (C) lesdits mots P_i et afin d'écrire lesdits mots P_i auxdites adresses respectives A_i dans la mémoire programmable (12 ; 22).

6 - Installation conforme aux revendications 4 et 5, caractérisée en ce que les moyens de sélection (135 ; 235) sont commandés par le calculateur (15, 25) afin de sélectionner a sorties dudit registre (131, 231) parmi r en fonction dudit mot de code prédéterminé (C).

7 - Installation conforme à l'une des revendications 1 à 4, caractérisée en ce que les moyens de mémorisation (12 ; 22) sont une mémoire morte contenant à chaque adresse A_i le mot correspondant P_i .

8 - Installation de chiffrement et déchiffrement d'un signal numérique convoyant des mots N_i à n bits en un signal chiffré numérique composé de mots R_i à n bits, caractérisée en ce qu'il comprend, à l'émission dans le chiffreur, un nombre K de chiffreurs élémentaires (1_k) en série tels que celui de l'installation conforme à l'une des revendications 1 à 7, la sortie (140_k) à mots chiffrés des moyens logiques (11_k) d'un chiffreur élémentaire (1_k) de rang k ($1 \leq k \leq K$) étant reliée à l'entrée (110_{k+1}) à mots à chiffrer des moyens logiques (11_{k+1}) du chiffreur élémentaire (1_{k+1}) de rang suivant k + 1,



et en ce qu'il comprend, à la réception dans le chiffreur, un nombre K de déchiffreurs élémentaires (2_k) en série tels que celui de l'installation conforme à l'une des revendications 1 à 7, la sortie (212_k) à mots déchiffrés des moyens logiques 5 (21_k) d'un déchiffreur élémentaire (2_k) de rang k effectuant l'opération h_k contraire de l'opération g_k effectuée par le chiffreur élémentaire de rang k étant reliée à l'entrée (200_{k-1}) à mots à déchiffrer des moyens logiques (21_{k-1}) du déchiffreur élémentaire (2_{k-1}) de rang précédent $k-1$ effectuant l'opération $10h_{k-1}$ contraire de l'opération g_{k-1} effectuée par le chiffreur élémentaire de rang $k-1$.

9 - Installation conforme à la revendication 8, caractérisée en ce que les chiffreurs $(1_1, 1_K)$, Fig. 3A), resp. déchiffreurs élémentaires $(2_1, 2_K)$, Fig. 3B), qui possèdent un calculateur (15, 25), sont reliés à un dispositif de lecture (17, 27) dudit mot de code prédéterminé (C), ledit mot de code comprenant des mots de code élémentaires (C_1, C_K) assignés respectivement auxdits chiffreurs, déchiffreurs élémentaires.

20 10 - Installation conforme à l'une des revendications 1 à 9, caractérisée en ce que le chiffreur, resp. le déchiffreur, comprend à son entrée un convertisseur parallèle-parallèle (10 ; 20) pour convertir un signal numérique de mots à chiffrer 25M (m), resp. chiffrés R (m) à m bits en ledit signal numérique à mots N (n), resp. R (n) à n bits, et à sa sortie un convertisseur parallèle-parallèle (14, 24) pour convertir le signal à mots chiffrés R (n), resp. déchiffrés N (n) à n bits, en ledit signal numérique à mots chiffrés R (m), resp. déchiffrés M (m), 30 à m bits.



FIG.1

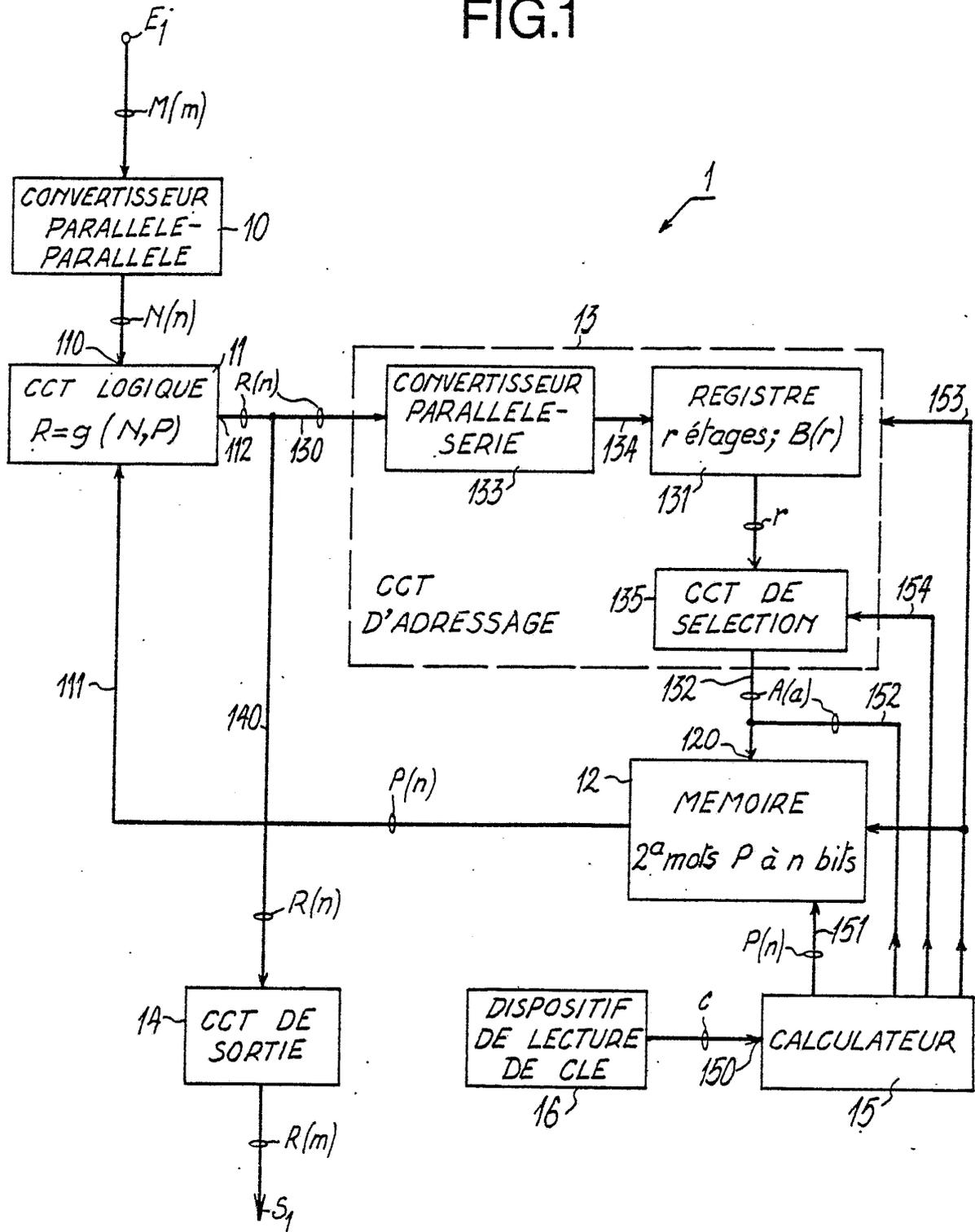


FIG. 2

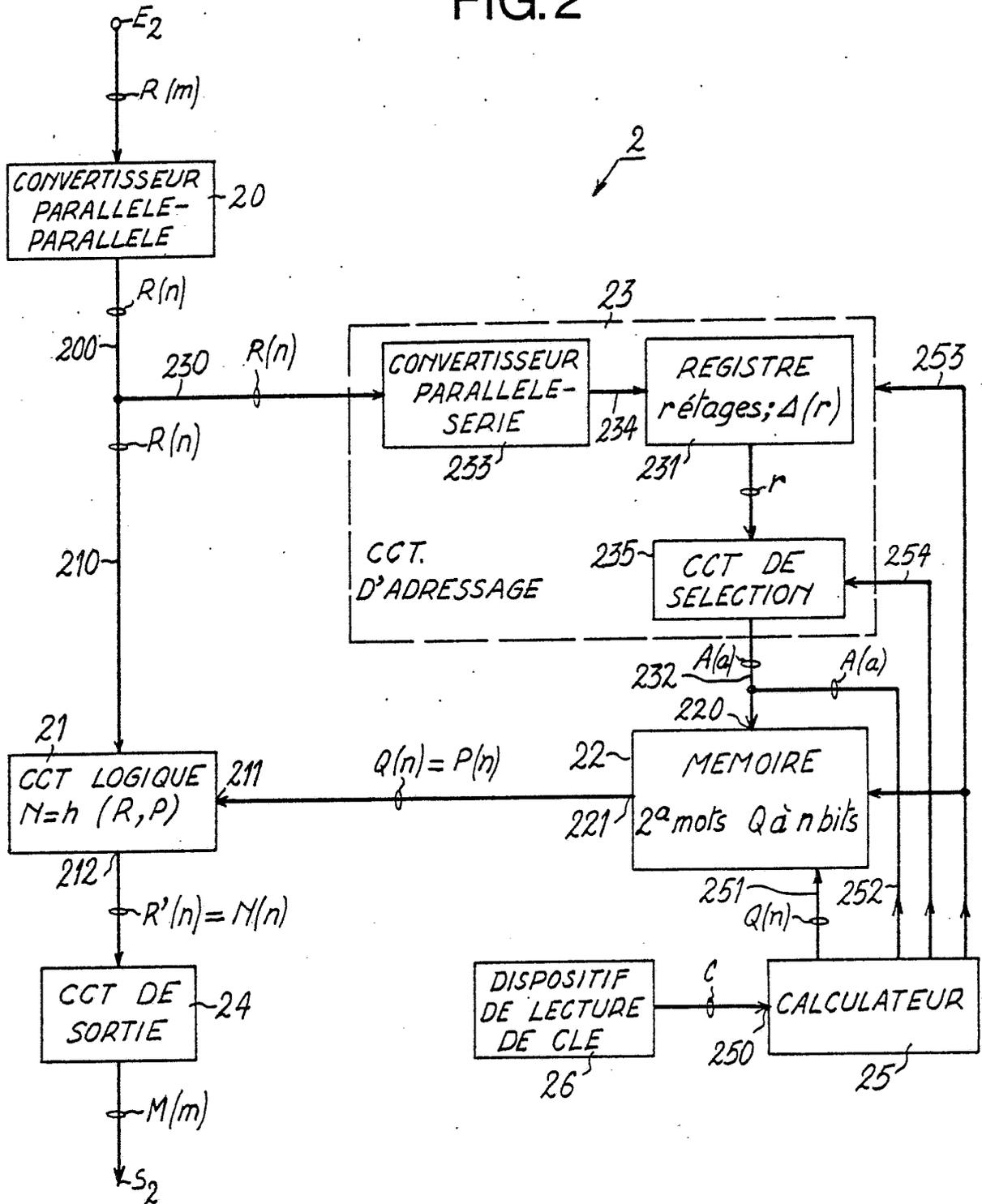
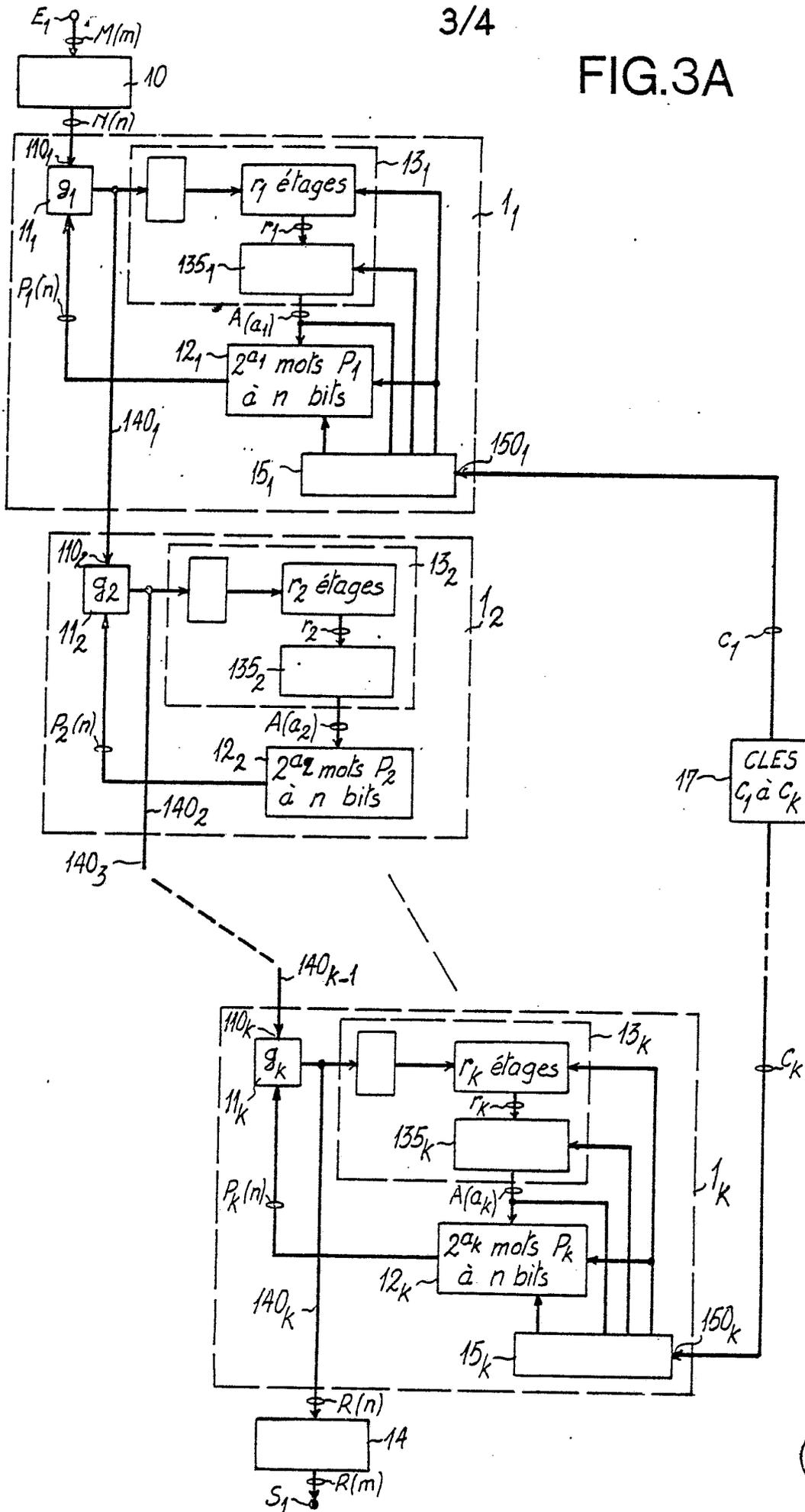
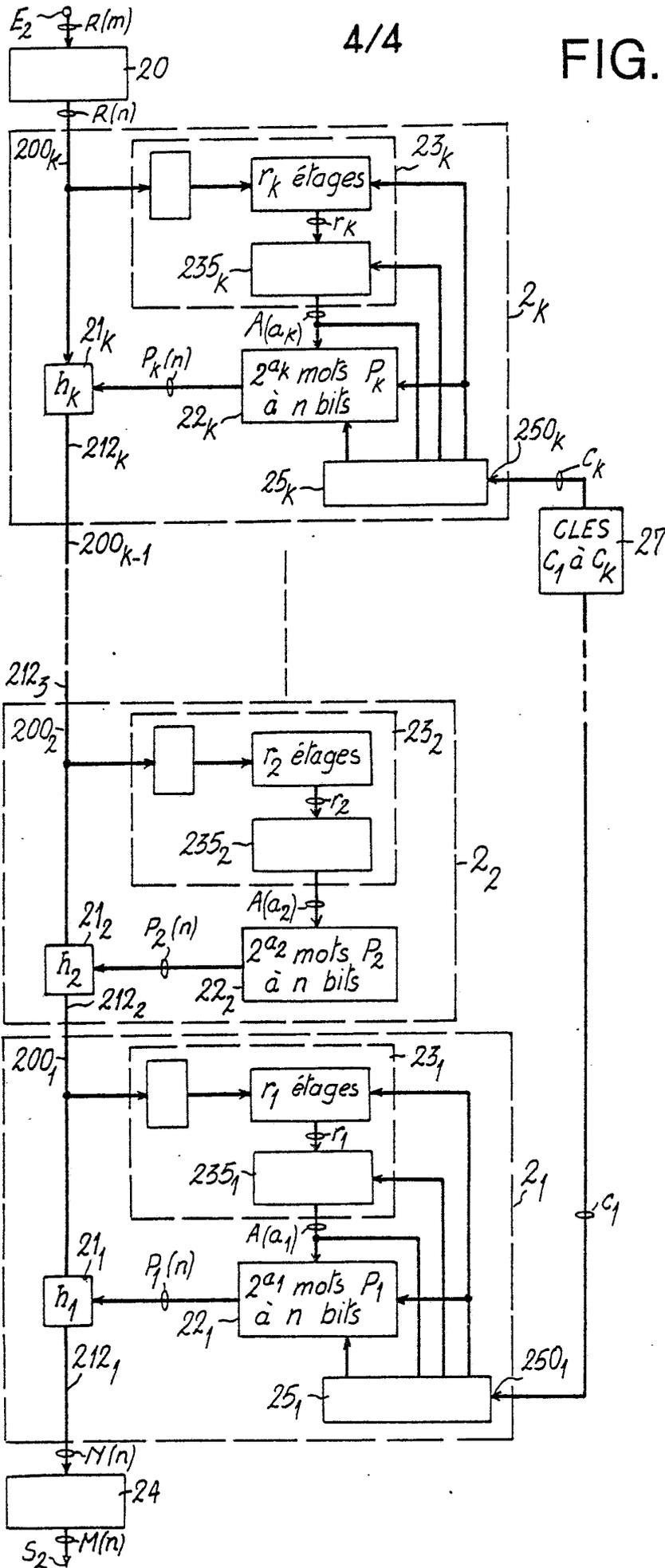


FIG.3A



4/4

FIG.3B



INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR80/00149

| | | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) ³ | | |
| According to international Patent Classification (IPC) or to both National Classification and IPC | | |
| Int.Cl. ³ : H04L 9/02 | | |
| II. FIELDS SEARCHED | | |
| Minimum Documentation Searched ⁴ | | |
| Classification System | Classification Symbols | |
| Int.Cl. ³ | H04L 9/02; H04L 9/00; H04L 9/04 | |
| Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched ⁵ | | |
| III. DOCUMENTS CONSIDERED TO BE RELEVANT ¹⁴ | | |
| Category * | Citation of Document, ¹⁶ with indication, where appropriate, of the relevant passages ¹⁷ | Relevant to Claim No. ¹⁸ |
| | FR, A, 2210307, published on July 5, 1974, see page 4, lines 2 to 13, 25 to 36; page 5, lines 18 to 22, 29 to 36; I.B.M. Cited in the application --- | 1 |
| | Electro Conference Record 1977, published in April 1977 (El Segundo, US), S. Jeffery et al. "Data Encryption", pages 30/4-1 to 30/4-6, see page 30/4-5, left-hand column line 52 to right-hand column, line 18 Cited in the application --- | 2 |
| | DE, B, 2639806, published on October 13, 1977 see column 4, lines 8 to 30; column 5, lines 34 to 65, Siemens Cited in the application --- | 1,5 |
| | FR, A, 2265221, published on October 17, 1975, see page 2, lines 7 to 31; page 8, line 8 to page 9, line 5, Philips Cited in the application --- | 1,2 |
| | --- |/.. |
| <p>* Special categories of cited documents: ¹⁵</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"&" document member of the same patent family</p> | | |
| IV. CERTIFICATION | | |
| Date of the Actual Completion of the International Search ² | Date of Mailing of this International Search Report ² | |
| 9 January 1981 (09.01.81) | 19 January 1981 (19.01.81) | |
| International Searching Authority ¹ | Signature of Authorized Officer ²⁰ | |
| European Patent Office | | |

FURTHER INFORMATION CONTINUED FROM THE SECOND SHEET

A US, A, 4133974, published on January 9, 1979, see column 4, lines 23 to 65; column 5, lines 28 to 64; Morgan Cited in the application

1,7

V. OBSERVATIONS WHERE CERTAIN CLAIMS WERE FOUND UNSEARCHABLE ¹⁰

This international search report has not been established in respect of certain claims under Article 17(2) (a) for the following reasons:

1. Claim numbers, because they relate to subject matter ¹² not required to be searched by this Authority, namely:

2. Claim numbers, because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out ¹³, specifically:

VI. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING ¹¹

This International Searching Authority found multiple inventions in this international application as follows:

1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims of the international application.

2. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims of the international application for which fees were paid, specifically claims:

3. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim numbers:

4. As all searchable claims could be searched without effort justifying an additional fee, the International Searching Authority did not invite payment of any additional fee.

Remark on Protest

The additional search fees were accompanied by applicant's protest.

No protest accompanied the payment of additional search fees.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale N° PCT/FR 80/00149

| | | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I. CLASSEMENT DE L'INVENTION (si plusieurs symboles de classification sont applicables, les indiquer tous) ³ | | | | |
| Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB | | | | |
| Int.Cl. ³ H 04 L 9/02 | | | | |
| II. DOMAINES SUR LESQUELS LA RECHERCHE A PORTÉ | | | | |
| Documentation minimale consultée ⁴ | | | | |
| Système de classification | Symboles de classification | | | |
| Int.Cl. ³ | H 04 L 9/02; H 04 L 9/00; H 04 L 9/04 | | | |
| Documentation consultée autre que la documentation minimale dans la mesure où de tels documents font partie des domaines sur lesquels la recherche a porté ⁵ | | | | |
| | | | | |
| III. DOCUMENTS CONSIDÉRÉS COMME PERTINENTS ¹⁴ | | | | |
| Catégorie * | Identification des documents cités, ¹⁶ avec indication, si nécessaire, des passages pertinents ¹⁷ | N° des revendications visées ¹⁸ | | |
| | FR, A, 2210307, publié le 5 juillet 1974, voir page 4, lignes 2 à 13, 25 à 36; page 5, lignes 18 à 22, 29 à 36, I.B.M. cité dans la demande | 1 | | |
| | -- | | | |
| | Electro Conference Record 1977, publié en avril 1977 (El Segundo, US) S. Jeffery et al. "Data Encryption", pages 30/4-1 à 30/4-6, voir page 30/4-5, colonne de gauche, ligne 52 à colonne de droite, ligne 18 cité dans la demande | 2 | | |
| | -- | | | |
| | DE, B, 2639806, publié le 13 octobre 1977, voir colonne 4, lignes 8 à 30; colonne 5, lignes 34 à 65, Siemens cité dans la demande | 1,5 | | |
| | -- | | | |
| | FR, A, 2265221, publié le 17 octobre 1975, voir page 2, lignes 7 à 31; page 8, ligne 8 à page 9, ligne 5, Philips cité dans la demande | 1,2 | | |
| | -- | | | |
| | ./. | | | |
| <p>* Catégories spéciales de documents cités: ¹⁵</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; border: none;"> <p>« A » document définissant l'état général de la technique</p> <p>« E » document antérieur, mais publié à la date de dépôt international ou après cette date</p> <p>« L » document cité pour raison spéciale autre que celles qui sont mentionnées dans les autres catégories</p> <p>« O » document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens</p> </td> <td style="width: 50%; border: none;"> <p>« P » document publié avant la date de dépôt international mais à la date de priorité revendiquée ou après celle-ci</p> <p>« T » document ultérieur publié à la date de dépôt international ou à la date de priorité, ou après, et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention</p> <p>« X » document particulièrement pertinent</p> </td> </tr> </table> | | | <p>« A » document définissant l'état général de la technique</p> <p>« E » document antérieur, mais publié à la date de dépôt international ou après cette date</p> <p>« L » document cité pour raison spéciale autre que celles qui sont mentionnées dans les autres catégories</p> <p>« O » document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens</p> | <p>« P » document publié avant la date de dépôt international mais à la date de priorité revendiquée ou après celle-ci</p> <p>« T » document ultérieur publié à la date de dépôt international ou à la date de priorité, ou après, et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention</p> <p>« X » document particulièrement pertinent</p> |
| <p>« A » document définissant l'état général de la technique</p> <p>« E » document antérieur, mais publié à la date de dépôt international ou après cette date</p> <p>« L » document cité pour raison spéciale autre que celles qui sont mentionnées dans les autres catégories</p> <p>« O » document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens</p> | <p>« P » document publié avant la date de dépôt international mais à la date de priorité revendiquée ou après celle-ci</p> <p>« T » document ultérieur publié à la date de dépôt international ou à la date de priorité, ou après, et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention</p> <p>« X » document particulièrement pertinent</p> | | | |
| IV. CERTIFICATION | | | | |
| Date à laquelle la recherche internationale a été effectivement achevée ² | Date d'expédition du présent rapport de recherche internationale ³ | | | |
| 9 janvier 1981 | 19 janvier 1981 | | | |
| Administration chargée de la recherche internationale ¹ | Signature du fonctionnaire autorisé ²⁰ | | | |
| Office Européen des Brevets | G.L.M. Kruidenberg | | | |

SUITE DES RENSEIGNEMENTS INDIQUÉS SUR LA DEUXIÈME FEUILLE

| | | |
|---|-------------------------------------------------------------------------------------------------------------------------------------------|-----|
| A | US, A, 4133974, publié le 9 janvier 1979, voir colonne 4, lignes 23 à 65; colonne 5, lignes 28 à 64, Morgan cité dans la demande | 1,7 |
|---|-------------------------------------------------------------------------------------------------------------------------------------------|-----|

V. OBSERVATIONS LORSQU'IL A ÉTÉ ESTIMÉ QUE CERTAINES REVENDICATIONS NE POUVAIENT PAS FAIRE L'OBJET D'UNE RECHERCHE ¹⁰

Selon l'article 17.2) a) certaines revendications n'ont pas fait l'objet d'une recherche pour les motifs suivants:

1. Les revendications numéros se rapportent à un objet à l'égard duquel la présente administration n'a pas l'obligation de procéder à la recherche, ¹² à savoir:

2. Les revendications numéros se rapportent à des parties de la demande internationale qui ne remplissent pas les conditions prescrites dans une mesure telle qu'une recherche significative ne peut être effectuée, ¹³ précisément:

VI. OBSERVATIONS LORSQU'IL Y A ABSENCE D'UNITÉ DE L'INVENTION ¹¹

L'administration chargée de la recherche internationale a trouvé plusieurs inventions dans la présente demande internationale, c'est-à-dire:

1. Comme toutes les taxes additionnelles demandées ont été payées dans les délais, le présent rapport de recherche internationale couvre toutes les revendications de la demande internationale pouvant faire l'objet d'une recherche.
2. Comme seulement une des parties taxes additionnelles demandées ont été payées dans les délais, le présent rapport de recherche internationale couvre seulement celles des revendications de la demande pour lesquelles les taxes ont été payées, c'est-à-dire les revendications:
3. Aucune taxe additionnelle demandée n'a été payée dans les délais par le déposant. En conséquence, le présent rapport de recherche internationale est limité à l'invention mentionnée en premier dans les revendications; elle est couverte par les revendications numéros:

Remarque quant à la réserve

- Les taxes additionnelles de recherche étaient accompagnées d'une réserve du déposant.
- Aucune réserve n'a été faite lors du paiement des taxes additionnelles de recherche.