



MINISTERE DES AFFAIRES ECONOMIQUES

NUMERO DE PUBLICATION : 1009081A4

NUMERO DE DEPOT : 09500086

Classif. Internat. : H04N

Date de délivrance le : 05 Novembre 1996

Le Ministre des Affaires Economiques,

Vu la Convention de Paris du 20 Mars 1883 pour la Protection de la propriété industrielle;

Vu la loi du 28 Mars 1984 sur les brevets d'invention, notamment l'article 22;

Vu l'arrêté royal du 2 Décembre 1986 relatif à la demande, à la délivrance et au maintien en vigueur des brevets d'invention, notamment l'article 28;

Vu le procès verbal dressé le 06 Février 1995 à 14H00 à l'Office de la Propriété Industrielle

ARRETE:

ARTICLE 1.- Il est délivré à : LE GROUPE VIDEOTRON Ltée
avenue Viger Est 300, MONTREAL, QUEBEC(CANADA)

représenté(e)(s) par : DE PALMENAER Roger, BUREAU VANDER HAEGHEN - K.O.B. S.A., Rue
Colonel Bourg 108A,- B 1030 BRUXELLES.

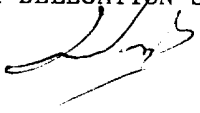
un brevet d'invention d'une durée de 20 ans, sous réserve du paiement des taxes annuelles, pour : METHODE ET SYSTEME DE DISTRIBUTION DE SIGNAUX A DES ABONNES EN REGLE.

INVENTEUR(S) : Garneau Pierre, 157 St-Paul Ouest # 32, Montréal Québec (CA);Corriveau Josée, 8320 Alphonse-Desjardins, St-Léonard, Québec (CA);Dufresne Michel, 1096 Du Perche, Boucherville Québec (CA)

PRIORITE(S) 07.02.94 US USA 193410

ARTICLE 2.- Ce brevet est délivré sans examen préalable de la brevetabilité de l'invention, sans garantie du mérite de l'invention ou de l'exactitude de la description de celle-ci et aux risques et périls du(des) demandeurs(s).

Bruxelles, le 05 Novembre 1996
PAR DELEGATION SPECIALE :


WUYTS L
Directeur

Méthode et système de distribution de signaux à des abonnés en règle

La présente invention concerne une méthode et un système de distribution de signaux à des abonnés qui sont en règle avec leurs abonnement appelés dans la suite "abonnés en règle", la méthode et la système étant employés utilement dans un système de télévision "d'achat à la consommation" ou "avec paiement à la carte".

Les systèmes TV à péage tombent généralement dans une des deux catégories dans lesquelles, ou bien les abonnés paient une redevance mensuelle pour voir tous les signaux transmis sur certaines chaînes ou certains canaux pendant une certaine période de temps, ou bien les abonnés "avec paiement à la carte" où des programmes choisis peuvent être vus par certains abonnés qui paient une redevance pour chaque programme demandé. Dans la première catégorie, des filtres peuvent être supprimés sur les lignes de transmission des abonnés autorisés ou un signal de désembrouillage peut être envoyé par la tête de réseau dans des terminaux d'abonnés. Dans la seconde catégorie, des signaux de décodage limités à des programmes particuliers sont transmis à des décodeurs adressables soit par une ligne téléphonique, soit par le réseau câblé.

Cela revient très cher d'envoyer du personnel pour supprimer ou ajouter des filtres localement à chaque lieu d'abonné dans une grande population chaque fois que des abonnés signent pour un service ou l'annulent, ou négligent de payer pour ce service. De plus, la nécessité d'adresser chaque terminal d'abonné avec une adresse individuelle pour fournir un code de désembrouillage pour des programmes spécifiques ou pour des périodes spécifiques s'est révélée présenter des inconvénients, car elle utilise une largeur de bande que l'on sait déjà encombrée et elle est lente car elle nécessite l'envoi de codes pendant une longue période.

De plus, ces systèmes n'ont pas pu être utilisés avec des réseaux classiques de TV câblée utilisés par plusieurs compagnies de TV par câble car un abonné à une compagnie pouvait téléphoner à une autre et obtenir l'envoi d'un code de désembrouillage recevant ainsi des signaux auxquels il n'avait pas droit, en privant ainsi la première compagnie du paiement de cet abonné.

De plus, étant donné la sécurité faible, ces systèmes ne sont pas utilisables pour fournir d'autres services que ceux du câble, par exemple des services bancaires, un service personnel ou des services de marchandises, etc., dans lesquels des informations sur les comptes, sur

les états des comptes, etc., doivent être affichées sur l'écran de télévision de l'abonné.

La présente invention prévoit un système de paiement à la carte ou un service équivalent qui ne nécessite pas l'envoi d'un code de désembrouillage ou d'activation d'un terminal d'abonné par une tête de réseau, sur une base terminal par terminal, et qui peut être utilisé pour permettre aux fournisseurs de service, comme un service bancaire, un service de commande de marchandises, de stockage et de restitution d'informations personnelles, etc., de les fournir à un groupe d'abonnés. De plus, le système peut faciliter l'utilisation d'un seul réseau par plusieurs opérateurs de câbles sans risque qu'un abonné à l'un puisse commander à un autre une programmation ou des services.

De plus, le système n'a pas besoin d'être lié au système de distribution de réseau câblé, mais peut être utilisé pour commander la fourniture de signaux utiles aux abonnés qui reçoivent des diffuseurs domestiques par voie hertzienne, des diffusions par satellites, etc.

Le système convient aussi à une utilisation de "diffusion proche", c'est-à-dire permettant à des abonnés spécifiquement autorisés de choisir ou de recevoir des données et de les traduire par une machine de facsimilé équipée pour recevoir les signaux en rapports, messages, journaux, états de comptes et bordereaux de confirmation, etc., sans que la tête de réseau ait besoin de transmettre des codes d'activation ou de désembrouillage à des terminaux spécifiquement adressés.

Chaque terminal peut être individuellement activé pour recevoir une séquence spécialement demandée de signaux (désignant un programme, un service, etc.) par l'abonné introduisant un mot de passe dans le terminal. Ce mot de passe est obtenu à une station centrale qui a vérifié un code de requête d'événement qui est reçu, pratiquement par un téléphone à touches, et qui fournit le mot de passe par un système de réponse vocale synthétique. Le code de requête d'événement est visible sur l'écran de télévision de l'abonné, une fois que celui-ci a introduit, dans le terminal, une requête pour un programme ou un service spécial.

Par exemple, dans un système de paiement à la carte, un canal annonceur affiche les programmes et les services disponibles dont chacun porte un numéro. Quand on désire un programme ou un service particulier, le numéro correspondant est introduit dans un terminal par l'abonné. Le terminal, entre temps, a mis en mémoire les codes d'identification des

divers programmes et services, et pointe le numéro introduit en face des numéros en mémoire, afin de vérifier qu'une erreur d'entrée n'a pas été faite.

Puis le terminal restitue une adresse unique logique ou physique
5 (I.D.) qui peut être mise en mémoire dans une mémoire morte (ROM), des contacts DIP, etc., restitue le code d'identification du programme ou du service et, en utilisant un clé d'embrouillage, traite le numéro de programme et l'adresse ID du terminal par un algorithme utilisant la clé d'embrouillage pour former un code embrouillé de requête d'événement qui
10 est affiché sur l'écran de télévision. Dans un exemple réussi de réalisation de l'invention, ce code comporte 14 caractères, y compris un numéro de vérification arithmétique, bien qu'on puisse utiliser d'autres longueurs de code, suivant les besoins de la compagnie de câble. L'abonné peut ensuite initier la réalisation de placer un ordre pour un événement
15 avec paiement à la carte. On peut éventuellement utiliser une identification automatique de numéro (ANI) ce qui permet de réduire le nombre de caractères utilisés.

Pour placer un ordre, le code de requête d'événement qui est affiché sur l'écran de l'abonné est envoyé par téléphone par l'abonné à la
20 station centrale. La station centrale décrypte le code, pointe le numéro du terminal dans la liste des numéros de terminal d'abonnés en règle, vérifie le code du programme et fournit le mot de passe mentionné ci-dessus, par exemple par une réponse vocale engendrée synthétiquement, à l'abonné. Ensuite, l'abonné met le mot de passe dans le terminal, ce
25 qui lui fournit non seulement un code de désembrouillage spécial pour l'événement, le programme, le service requis, etc., mais encore l'autorise à désembrouiller pendant un certain temps de programme pendant lequel le code de désembrouillage doit être invoqué, et, de préférence, lui commande de commuter automatiquement le signal de sortie vers l'écran
30 de télévision et le canal requis qui peut être le canal annonceur, en temps voulu, et pour une période spéciale, de manière à fournir automatiquement le programme à l'abonné.

Une fois le mot de passe fourni à l'abonné, la commande de paiement à la carte est acceptée et facturée. L'abonné a la faculté d'annuler
35 l'ordre jusqu'au début de l'événement. Le processus d'annulation est semblable à celui qu'on utilise pour requérir l'événement. Les programmes choisis sont listés sur l'écran de télévision quand on sélectionne l'option

"annulation" dans le menu de l'annonceur. On peut choisir le programme à annuler et, une fois fait, un code d'annulation de 14 caractères est affiché et, immédiatement, le programme annulé dans le terminal. Le code à 14 caractères doit être envoyé à la tête de réseau pour annuler la
5 facture avant le démarrage du programme. Une fois obtenu un code d'annulation crypté sur l'écran de télévision, l'abonné le transmet à la station centrale en utilisant un numéro de téléphone différent de celui servant à placer un ordre. Un mot de passe différent est envoyé à l'abonné et est introduit dans le terminal pour clore la transaction
10 d'annulation.

On sait qu'il est virtuellement impossible de décrypter en un temps raisonnable un code crypté engendré en utilisant des techniques de cryptage modernes, ce qui procure pratiquement une sécurité. De plus, les clés de cryptage mises en mémoire dans les divers terminaux peuvent être
15 changées de temps en temps en diffusant par la tête de réseau aux terminaux, chacune étant adressée par l'adresse permanente du terminal, par exemple tous les deux mois. Comme, pour ce cas, chaque terminal n'a pas besoin d'être immédiatement adressé avant un programme ou un service choisi, l'économie en équipement de transmission nécessaire, en largeur
20 de bande pendant les moments de pointe, etc., est évidente.

De plus, comme les codes associés aux divers programmes peuvent être choisis par le fournisseur de service sur câble TV et pratiquement ne sont fournis sur les canaux annonceurs qu'un jour ou deux avant la transmission d'un programme de paiement à la carte, et que le code crypté
25 et le mot de passe, à la fois, dépendent non seulement de la clé de cryptage, mais encore du numéro de programme, il est virtuellement impossible d'engendrer des mots de passe appropriés par des pirates pour pouvoir, à temps, désembrouiller et utiliser frauduleusement les signaux diffusés avec paiement à la carte.

A noter que la clé de cryptage peut être différente pour chacun des opérateurs de câble TV qui distribuent des signaux sur le même réseau de câble TV ou par d'autres média. Ainsi, un terminal d'abonné, qui a mis en mémoire une clé particulière de décryptage associée à l'opérateur de
30 câble TV auquel l'abonné est abonné, engendrera des codes de requête d'événement qui ne seront pas reconnus par l'équipement de stations centrales d'un autre opérateur de câble TV et aucun mot de passe, ni
35 aucun mot de passe valable ne sera donné sur requête d'un abonné à un

autre opérateur de câble TV. Cela provoque une ségrégation des abonnés pour séparer les opérateurs de câble TV qui sont tous connectés à un seul réseau. Ainsi, on a un ensemble où une région entière peut être reliée à un seul réseau ou à un groupement de réseaux uniques, grands ou petits.

5 En outre, il n'y a pas de monopole d'un opérateur pour les abonnés qui peuvent choisir l'opérateur de câble TV qu'ils veulent. Plusieurs opérateurs desservant une grande population n'ont pas besoin de dupliquer un réseau de câble TV, ce qui procure une économie considérable.

10 Suivant une caractéristique de l'invention, une méthode de distribution de signaux à des abonnés en règle comprend la mise en mémoire d'au moins un code d'identification valable pour le terminal d'abonné à la station centrale, la diffusion de promotions de services disponibles pour les abonnés, dont chacun est associé à un code de promotion spécifique, le choix d'un desdits services et l'entrée d'un
15 code choisi de promotion de service dans un terminal là où réside l'abonné, la lecture automatique d'un numéro d'identification associé au terminal en réponse à l'entrée d'un code de promotion choisi, le traitement du numéro d'identification et du code de promotion choisi suivant un algorithme de cryptage, et la génération par celui-ci d'un
20 code crypté de requête d'événement, l'envoi du code de requête d'événement à un centre de vérification, le décryptage au centre de décryptage du code de requête d'événement, la vérification du numéro avec les codes d'identification valables, et l'envoi d'un mot de passe unique au terminal et du code de promotion choisi, l'entrée du mot de passe dans
25 le terminal là où réside l'abonné, et fourniture de l'accès à un service en utilisant l'un des signaux distribués correspondant au code de promotion choisi à l'abonné en réponse à l'entrée du mot de passe.

Suivant une autre caractéristique de l'invention, une méthode de distribution de signaux à des abonnés en règle comprend, au terminal
30 d'abonné, la génération d'un code de requête pour un service utilisant les signaux en accédant à un code enregistré de programme relatif au service et un code d'adresse relatif à une identification du terminal, et le cryptage des codes en utilisant une clé de cryptage pour engendrer un code de requête de service, la requête du service auprès d'un terminal
35 central en envoyant le code de requête de service au terminal central qui décrypte le code de requête de service et vérifie la validité du code d'adresse et du code de programme, et qui engendre un mot de passe,

l'entrée du mot de passe dans le terminal de l'abonné et, en réponse, la fourniture de l'accès aux signaux fournissant le service.

Suivant une autre caractéristique, un système de câble TV comprend des terminaux d'abonnés, chaque terminal d'abonné comprenant un appareil
5 pour mettre en mémoire un code d'identification de terminal, un appareil pour mettre en mémoire un code d'identification de programme, un appareil pour mettre en mémoire une clé de cryptage, un appareil pour traiter les codes et la clé suivant un algorithme de cryptage et ensuite engendrant un code de requête de programme, un dispositif d'affichage pour afficher
10 le code de requête de programme, un appareil pour recevoir un mot de passe et, en réponse, l'activation d'un programme à passer au dispositif d'affichage pour affichage, une tête de réseau et un réseau de câble TV qui lui est relié pour transmettre une représentation cryptée du programme aux terminaux d'abonnés, une station centrale comprenant un
15 appareil pour recevoir le code de requête de programme, un appareil pour décrypter le code de requête de programme et pour en tirer le code d'identification de programme et le code d'identification du terminal, un appareil pour vérifier les codes déterminés d'identification de programme et de terminal, et un appareil pour engendrer un mot de passe en réponse
20 à la vérification de la validité des codes déterminés d'identification de programme et de terminal.

Suivant une autre caractéristique, un système de câble TV comprend un réseau de distribution de TV par câble, une pluralité d'équipements de diffusion de TV par câble prévus pour transmettre des programmes par le
25 réseau destinés à des terminaux d'abonnés autorisés à ne recevoir que des équipements de diffusion individuels, une pluralité de terminaux d'abonnés reliés au réseau, chaque terminal d'abonné comprenant un code de cryptage, chaque code étant unique pour un diffuseur particulier, un appareil dans chaque terminal pour choisir un programme et pour obtenir
30 un code de requête d'événement crypté, un appareil dans les équipements pour engendrer un mot de passe qui est unique pour un événement et unique pour un diffuseur individuel particulier, un appareil pour appliquer le mot de passe au terminal où le programme a été choisi, de manière que des programmes diffusés par d'autres diffuseurs ne puissent pas être affichés
35 dans d'autres terminaux.

Suivant une autre caractéristique, un système de câble TV comprend un réseau, des terminaux d'abonnés reliés au réseau et autorisés à

recevoir des signaux offerts par certains des différents opérateurs, et des appareils pour limiter la réception par des abonnés de signaux à ceux qui sont offerts par ces opérateurs pour lesquels ont été autorisés les terminaux d'abonnés.

5 Suivant une autre caractéristique, une méthode de distribution de signaux à divers abonnés comprend la connexion de plusieurs abonnés à un seul réseau de distribution de programme, la connexion de plusieurs fournisseurs de programme audit réseau, l'envoi vers chacun des divers terminaux d'abonnés d'un code relatif à un fournisseur de programme
10 particulier, et la mise en mémoire dudit code dans les terminaux d'abonnés concernés, la transmission de programmes à partir desdits fournisseurs de programmes au réseau dans des canaux séparés particuliers, et l'activation de la réception des programmes particuliers uniquement provenant des fournisseurs de programmes concernés par des
15 terminaux d'abonnés spécifiques utilisant lesdits codes.

Les caractéristiques de l'invention mentionnées ci-dessus, ainsi que d'autres, apparaîtront plus clairement à la lecture de la description suivante d'un exemple de réalisation, ladite description étant faite en relation avec les dessins joints, parmi lesquels:

20 la Fig. 1 est un bloc-diagramme d'un système utilisé pour mettre en oeuvre l'invention,

la Fig. 1A est un bloc-diagramme d'une variante du système de vérification,

la Fig. 1B est un bloc-diagramme d'une autre variante du système de
25 vérification,

la Fig. 2 est un bloc-diagramme des parties concernées d'un terminal d'abonné, et

la Fig. 3 est un bloc-diagramme d'un système de diffusion de programmes par plusieurs opérateurs.

30 La Fig. 1 montre un exemple de bloc-diagramme d'un système destiné à mettre en oeuvre l'invention. A noter que dans le système de distribution de télévision, les parties structurelles qui ne portent pas sur l'invention ne sont pas montrées, car on pense qu'elles sont connues de l'homme du métier.

35 Une tête de réseau 1 engendre des signaux de programmes, tels que des signaux de câble TV ou CATV, et les transmet par un milieu 3. Dans le prototype de l'invention qui a été une réussite et dans un exemple

préférée de l'invention, le milieu 3 est un réseau de distribution TV par câble. Cependant, on comprendra que la tête de réseau pourrait assurer la transmission par un système de distribution par satellite, un système normal de télédiffusion locale, un réseau national, tel qu'un réseau à
5 fibres optiques (autoroute de l'information, etc. Les signaux transmis par la tête de réseau peuvent être des signaux commerciaux, des signaux distribués en clair, des signaux cryptés de télévision, ou d'autres signaux qui procurent des services divers à de nombreux abonnés. La description ci-dessous concerne des signaux distribués en clair, mais
10 aussi surtout ceux qui ont été embrouillés ou cryptés. Donc, on n'a pas montré des éléments de terminal d'abonné qui sont en dérivation sur le décrypteur/convertisseur ou qui donnent des signaux à, par exemple, une entrée de facsimilé, de calculateur, etc. Cependant ces aspects de construction d'un terminal sont connus de l'homme du métier, par exemple
15 par le document US-A-4 623 920.

Les signaux transmis par la tête de réseau 1 sont reçus par le terminal d'abonné 5 et sont envoyés à l'entrée du décrypteur/convertisseur 7. A moins qu'un code de décryptage n'ait été
20 reçu par le décrypteur/convertisseur, les signaux sont bloqués et ne passent pas dans le décrypteur/convertisseur et donc ne sont pas montrés de manière compréhensible sur un moniteur vidéo 9 qui est relié à sa sortie.

En fonctionnement, la tête de réseau transmet, non crypté sur un canal annonceur, un affichage des promotions de services dont disposent
25 les abonnés, chacun étant associé à un code de promotion associé. Les services peuvent comprendre ou comporter des programmes TV cryptés, comme on peut le désirer pour être vus dans un système avec paiement à la carte. La liste est compilée par un fournisseur 2 de service avec paiement à la carte.

30 A un moment approprié, les programmes à choisir sont aussi transmis dans d'autres canaux; par exemple, il peut y avoir deux canaux auxiliaires différents pour le paiement à la carte, cryptés, qui sont transmis par la tête de réseau à des moments prédéterminés.

Le canal annonceur n'est pas crypté et, ou bien passe par une
35 dérivation du décrypteur/convertisseur, ou bien passe par le décrypteur/convertisseur sans nécessiter d'être décrypté, et est affiché

sur le moniteur 9. L'abonné voit le canal annonceur et choisit un service de programmes identifié par un code de programme.

L'abonné peut alors faire entrer le code de programme dans le terminal d'abonné, par exemple au moyen d'une télécommande qui passe dans
5 un processeur de cryptage 11.

Un module 13 d'adresse de terminal est associé au terminal 5 et peut être un groupe de commutateurs à enfoncement (boutons-poussoirs) qui identifient logiquement le terminal, ou une adresse logique mise en mémoire dans une mémoire ROM, une adresse dans un microprogramme, ou une
10 adresse mise en mémoire de manière permanente d'une autre manière.

Le terminal 5 comporte aussi une mémoire 15 qui met en mémoire une clé de cryptage.

Dès que l'abonné fait entrer le code de programme dans le terminal 5 pour un service qu'il veut spécifiquement, comme un programme avec paiement à la carte, l'algorithme de cryptage accède au numéro de série
15 qui identifie le terminal à partir du module 13, à la clé de cryptage à partir de la mémoire 15 et, en utilisant le code de programme, traite les données ci-dessus suivant l'algorithme en engendrant un code de requête d'événement crypté. Dans un exemple de réalisation réussi de l'invention, le code de requête d'événement comporte 14 caractères et sera décrit en
20 détail ci-dessous.

On préfère aussi que les signaux de numéro de programme des services dont la promotion est faite sur le canal annonceur soient en mémoire dans une mémoire de programmes 17 qui est reliée pour pouvoir recevoir ces
25 signaux du décrypteur/convertisseur 7. Avant que le processeur 11 n'engendre le code de requête d'événement, on préfère qu'il ait accès à la mémoire de programmes et qu'il compare les numéros de programme en mémoire au code de programme introduit par l'abonné. Si on ne détecte pas le code de programme introduit, l'abonné a certainement fait une erreur
30 d'enregistrement et le processeur 11 peut envoyer un signal, par la ligne 19, au décrypteur/convertisseur 7 pour le faire afficher un message sur le moniteur 9 avertissant l'abonné qu'un code de programme erroné a été introduit.

Supposant que le code de programme a été trouvé correct, le code de requête d'événement engendré par le processeur 11 passe par la ligne 19
35 vers le décrypteur/convertisseur 7 pour être affiché pour l'abonné sur le moniteur 9, avec un générateur d'affichage vidéo 20 relié au

décrypteur/convertisseur, demandant, par exemple, à l'abonné de communiquer par téléphone le code de requête d'événement affiché à un numéro de téléphone prédéterminé.

5 L'abonné utilise alors son téléphone 21 et appelle une station centrale qui comporte un système de vérification 24 qui sera décrit, composant le code de requête d'événement crypté par un clavier de touches (ou équivalent) et le transmettant par la ligne téléphonique 23 à un poste téléphonique 25, un modem, etc., dans la station centrale 24.

10 A noter qu'au lieu d'utiliser le téléphone de l'abonné, le terminal 5 peut comprendre un modem et, en actionnant une commande au terminal 5, le modem peut être capable d'appeler automatiquement un modem correspondant dans la station centrale. Donc, dans cet exemple, les postes téléphoniques 21 et 25 seraient remplacés par des modems qui communiqueraient automatiquement entre eux.

15 Selon un exemple réussi, le code de 14 caractères est du format général: AAAAAAEEECBBBV, dans lequel:

AAAAAA est un champ de 6 nombres décimaux pris à partir de l'adresse du terminal d'abonné et est l'identification unique du terminal d'où est ordonné un événement et auquel doit être délivré un programme ou un service.

20 EEE est un champ qui contient le numéro du service ou de l'événement d'achat à la commande commandés par l'abonné. Un numéro d'événement différent est donné à chaque événement et à chaque date et chaque moment où l'événement est fourni. Par exemple, pour les mois pairs, le numéro d'événement ira de 001 à 399 pour les films et de 400 à 499 pour des événements spéciaux. Pour les mois impairs, le numéro d'événement ira de 501 à 899 pour les films et de 900 à 999 pour des événements spéciaux.

25 Le champ C contient le numéro de canal sur lequel doit être diffusé l'événement. Les valeurs possibles vont de 0 à 9. Dans un petit système qui utilise le format ci-dessus, par exemple 0 peut être un canal public (appelé canal annonceur), 1 peut être un premier canal de paiement à la carte et 2 un deuxième canal de paiement à la carte. Les canaux logiques sont traduits par le décrypteur/convertisseur en des canaux spéciaux; par exemple, si le canal logique 1 est choisi et peut être décodé, le canal 30 56 peut être désigné comme le premier canal de paiement à la carte qui peut être décodé et montré sur le canal 14, un canal annonceur représentant.

BBB est un code de paiement engendré par un terminal d'abonné. Le code de paiement sert aussi à prouver à la station centrale que l'abonné a utilisé son propre terminal pour engendrer le code. Le code de paiement BBB est créé en utilisant la clé de cryptage située dans la mémoire ROM dans le terminal.

V est un code de validation calculé à partir des numéros 13 précédents et sert à indiquer à la station centrale que l'utilisateur n'a pas fait d'erreur en enregistrant les données pour l'événement.

Revenant maintenant à la Fig. 1, quand le code de requête d'événement a été reçu par le téléphone 25 ou par un modem équivalent, il est détecté dans l'interface 27 du système de vérification 24. Cela est valable quand le code de requête d'événement introduit par l'abonné est validé par la reconstruction du code de validation V en relation avec le système de décryptage 29. S'il est trouvé non valable, un message est en retour envoyé à l'abonné pour restituer son introduction, ce qui peut être un message vocal synthétique si on utilise le téléphone, ou un message à afficher sur l'écran TV de l'abonné si on utilise un modem.

Dans un exemple de réalisation du système de vérification 24, une table 33 contient en mémoire une liste de tous les numéros de série des abonnés en règle et une table 36 une liste de programmes valables. Un processeur 36 lit la table 33 et détermine si y est entrée une adresse d'abonné en règle. Il vérifie aussi la table 35 pour s'assurer qu'un numéro de programme valable est introduit.

Dans un autre exemple de réalisation monté à la Fig. 1A, un système de vérification 24A comporte un serveur de PPV 31 qui détectent la validité d'un code de requête d'événement et engendre un mot de passe qui est appliqué à l'interface 27. L'interface 27 engendre dans un langage vocal synthétique les numéros et/ou les caractères d'un mot de passe qui est reproduit acoustiquement dans un téléphone 25 de manière à le fournir à l'abonné qui a composé le code de requête d'événement.

En variante, le mot de passe peut être appliqué au modem mentionné ci-dessus et être envoyé directement au terminal 5 de l'abonné pour être appliqué au déc 7 après avoir été localement traduit par un modem local et le récepteur de données 37 en signaux reconnaissables par le déc.

Dans un autre exemple de réalisation, on se passe de table 33. Le code de requête d'événement crypté contient une somme de vérification. En vérifiant d'abord que la somme de vérification est correcte pour le code

de requête d'événement, et, si c'est le cas, en décryptant ensuite le code de requête d'événement, on détermine qu'un abonné en règle a demandé un événement. Si le code n'est pas décrypter, il indique un abonné qui n'est pas en règle ou si la somme de vérification n'est pas correcte, il y a eu une erreur ou un anomalie en transmission. Dans ces cas, l'événement est refusé.

Si le code est décrypté, on accède à la table 35 pour déterminer si un programme valable a été choisi. En variante, la table 35 n'est pas utilisée et on suppose que la validité du programme a été vérifiée à la création du code de requête d'événement au terminal d'abonné.

En supposant que c'est l'abonné qui a entendu le mot de passe du téléphone 25, il l'applique au terminal, par exemple en le composant dans la télécommande de son terminal. Après l'avoir reçu, le processeur de cryptage inverse son fonctionnement et décrypte le mot de passe. On compare le résultat avec le code de requête d'événement original pris au poste de l'abonné pour validation. Quand il n'y a pas conformité, un message de non validité apparaît sur l'écran.

Si le mot de passe est accepté, cela fait afficher le programme désiré au moment approprié et pendant le temps voulu.

Afin de contrôler la validité des abonnés, le système comporte une SMS 30 qui contient une unité de paiement 39, comme le montre la Fig. 1. L'unité de paiement peut être un calculateur personnel que fait fonctionner un opérateur de câble TV. Les abonnés enregistrés par l'opérateur particulier de câble TV qui ont un bon crédit ou qui ont prépayé pour certains programmes sont mis dans l'unité de paiement qui met en mémoire les dresses des terminaux de ces abonnés en règle dans la table 33.

A noter que l'unité 39 peut être associé à un opérateur particulier. La clé de cryptage est diffusée à chaque abonné dans un canal de données, puis mise en mémoire dans la mémoire 15 du terminal 5. De préférence, elle est changée par la tête de réseau 1 suivant des intervalles prédéterminés, par exemple bimensuels, mensuels, etc. Le code de cryptage peut être engendré par l'unité 39 ou par une supervision de réseau (non montrée). A noter qu'une seule clé de cryptage peut être utilisée pour tous les abonnés autorisés à recevoir des programmes ou des services d'un seul opérateur de câble TV.

Des stations centrales différentes 24 peuvent être reliées à la tête de réseau 1, une par opérateur. Cependant tous les terminaux peuvent être reliés au même milieu 3 du réseau de câble TV. Afin de séparer les terminaux associés à chaque opérateur, tous les terminaux qui sont autorisés à recevoir d'un opérateur particulier ont la même clé de cryptage; on utilise différentes clés de cryptage pour les terminaux autorisés à recevoir à partir d'opérateurs différents.

Il en résulte que les codes de requête d'événement ne seront pas reconnus par les stations centrales 24 des opérateurs relatifs aux terminaux qui sont autorisés par des opérateurs différents. Donc plusieurs opérateurs peuvent utiliser le même réseau et peuvent mettre en commun les transmission des canaux en clair et des services sur câble. Cependant à cause des clés de cryptage différentes, leurs abonnés avec paiement à la carte peuvent être tenus totalement séparés. Cela permet une sécurité complète des divers opérateurs qui peuvent signer avec des fournisseurs de services différents pour leurs systèmes respectifs.

Passant à la Fig. 2, on a montré une vue plus détaillée d'un terminal 5 d'abonné.

Une entrée 41 reçoit des signaux du milieu 3 et les applique au convertisseur 43. Pratiquement, le convertisseur 43 convertit le canal du signal d'entrée en, par exemple, le canal 3 pour affichage sur un moniteur vidéo. Pour des signaux normaux, la sortie du convertisseur 43 va par un contact 45 à la ligne de sortie vidéo 45 pour être appliqués à l'entrée vidéo d'un moniteur.

Le contact 45 peut, en variante, appliquer les signaux de sortie du convertisseur 43 au décrypteur 47. Le convertisseur 43, le contact 45 et le décrypteur 47 sont commandés par un microprocesseur 49 par un bus 51.

Un récepteur télécommandé 53 reçoit, par exemple, des signaux infrarouges d'un émetteur de commande à distance utilisé par l'abonné, convertit les signaux sous forme numérique et les applique au bus 51 pour être reçus par le microprocesseur 49. Une mémoire à accès aléatoire RAM 55 enregistre les programmes qui sont utilisés par le microprocesseur 49 pour mettre en oeuvre les fonctions du terminal d'abonné. Le microprocesseur 49 peut aussi accéder aux données de la RAM 55 pour les afficher sur le moniteur 9 et, après avoir formé un affichage en utilisant un générateur d'affichage vidéo 56, applique les signaux par un convertisseur numérique/analogique 57 où les signaux sont convertis sous

une forme qui peut être affichée par le moniteur 9, sont modulés dans un modulateur 58 et appliqués à la ligne de sortie 45.

Le fonctionnement normal ci-dessus est décrit dans le document US-A-4 623 920.

5 Un module d'adresse de terminal 13 est relié au bus 51 de manière que le microprocesseur puisse accéder au numéro de série du terminal. De plus, une mémoire 15 de clé de cryptage peut mettre en mémoire la clé déjà mentionnée et envoyée par la tête de réseau.

10 De plus, un mémoire de programme RAM 17 est reliée au bus 51 pour l'accès du microprocesseur 49.

15 Des programmes sur le canal annonceur, par exemple le canal 14, sont affichés en ne passant pas par le décrypteur 47. Les données transmises sur le canal de données qui peuvent être dans l'intervalle de suppression verticale ou la ligne 21 du canal annonceur sont appliquées par le convertisseur et démodulées dans un démodulateur (non montré) vers le bus 51. Ces données peuvent être, par exemple, les numéros d'identification de programmes associés aux programmes listés sur le canal annonceur. Le microprocesseur 49 commande la mise en mémoire de ces données dans la mémoire de programmes 17.

20 Quand la liste des programmes est vue par un abonné sur le canal annonceur, il choisit un programme en entrant le code de programme associé affiché en utilisant par exemple sa télécommande. Le code de programme est envoyé par l'émetteur de la télécommande dans un récepteur de télécommande 53 (de préférence, préfixé par une marque spéciale, telle qu'un *), où il est traduit en données et temporairement lis en mémoire dans la RAM 55. Le microprocesseur 49 détecte le code de programme et, en utilisant un programme de la RAM 55, en déduit le code d'événement, c.a.d. les caractères qui deviennent EEE, comme défini ci-dessus. Le microprocesseur 49 vérifie alors ces caractères en les comparant aux caractères correspondant de la mémoire de programme 17 et, s'il y a concordance, accède au programme d'algorithme de cryptage en mémoire dans la RAM 55.

35 En faisant fonctionner l'algorithme de cryptage, le microprocesseur 49 accède au numéro de série du module 13 et au numéro de programme choisi, en mémoire temporairement dans la RAM 55, et engendre le code d'événement de préférence à 14 caractères. Il formule le code de requête d'événement sous une forme affichable en utilisant le générateur 56,

ajoute quelques caractères explicatifs, tels qu'un avis de confirmation, une instruction d'appeler un certain numéro de téléphone, en accédant aux données en mémoire dans la RAM 55 et en appliquant les informations pour affichage sur le moniteur. L'abonné, en voyant le code de requête
5 d'événement affiché sur le moniteur, compose les caractères du numéro de téléphone indiqué et, comme on l'a décrit, reçoit le mot de passe de la station centrale 24. L'abonné compose alors le mot de passe dans la télécommande du terminal, mot de passe qui est reçu dans le récepteur 53. Le mot de passe est mis temporairement en mémoire dans la RAM 55. En
10 utilisant un programme qui y est en mémoire, le microprocesseur 49 décode le mot de passe en moment de mis en marche, en période de marche, en code de décryptage et en signal de commande de canal pour le décrypteur 47.

On comprendra qu'un modem 61 peut être relié au bus 51 et, au lieu de composer le code de requête d'événement au téléphone par l'abonné, le
15 modem 61 sous la commande du microprocesseur 49 peut appeler un modem dans la station centrale 24, lui appliquer automatiquement le code de requête d'événement et en recevoir le mot de passe pour l'appliquer au bus pour mise en mémoire dans la RAM 55 et pour pouvoir l'utiliser ensuite par le microprocesseur 49.

Au moment approprié indiqué par une horloge 59, le microprocesseur
20 commute le contact 45 pour envoyer le signal de sortie du convertisseur 43 vers l'entrée du décrypteur 47, applique le code enregistré de décryptage au décrypteur 47 et commute un tuner contenu dans le convertisseur 43 pour recevoir du canal crypté spécifique défini par le
25 canal logique indiqué par le mot de passe, et fait sortir par le convertisseur 43 le signal vers le canal annonceur ou vers un autre canal prédéterminé quelconque. Le canal demandé est ainsi converti, décrypté et appliqué à la ligne de sortie 45 pour affichage sur le moniteur.

Après la période désignée du programme, le microprocesseur 49
30 supprime le code de cryptage 47, commute le convertisseur 43 à nouveau vers le canal sur lequel il était accordé, et commute le contact 45 pour dériver le décrypteur 47 permettant au moniteur d'afficher des canaux généralement en clair.

On comprendra que les mémoires décrites en se référant à l'exemple
35 de la Fig. 2 peuvent être éventuellement combinées d'une manière efficace. De plus, il est préférable qu'une batterie soit utilisée pour préserver les données en mémoire pour le cas d'une panne de courant.

La Fig. 3 est un bloc-diagramme montrant un réseau à plusieurs opérateurs. Plusieurs systèmes de commande d'opérateur 70A à 70N transmettent chacun des programmes par un réseau commun 72 à son propre jeu d'abonnés dont chacun est relié au même réseau commun. Chaque abonné a un terminal de contrôle de réception, tel que celui qui a été décrit en relation avec la Fig. 2. Chacun reçoit des signaux d'une tête de réseau principale par des jonctions câblées, une liaison hertzienne 74 ou un autre moyen de recevoir des signaux. Chaque système d'opérateur a son propre système d'autorisation et de vérification d'abonnés et de programme formé de SMS 30A à 30N et de serveurs 31A à 31N. Chaque système d'autorisation et de vérification de programme a son propre numéro de téléphone pour la ligne téléphonique 25. Ainsi, chaque système d'opérateur peut fournir des codes de terminaux d'abonné et de codage pour son propre groupe d'abonnés, fournir ses propres codes de programme sur son canal annonceur et autoriser ses propres abonnés à recevoir des programme en fournissant ses propres mots de passe. A noter également que les opérateurs individuels de câble peuvent être d'accord avec l'opérateur de la tête de réseau pour faire fonctionner un SMS 30 et un serveur 31 pour son propre compte. Afin de s'assurer que les différents opérateurs n'utilisent pas des codes qui interfèrent ou se recouvrent, on préfère que l'opérateur de la tête de réseau affecte des codes uniques individuels à chacun des systèmes d'opérateurs. Les systèmes fonctionnent dans le réseau commun comme on l'a déjà décrit. A noter qu'avec chacun des nombreux terminaux mettant en mémoire un code commun unique qui est spécifique à un système d'opérateur particulier, même pour des programmes qui ne s'achètent pas à la commande, la réception des programmes par chacun des terminaux peut être limitée à ceux envoyés par un système d'opérateur associé, car le code peut commander le décryptage de signaux normaux de programme qui sont transmis avec un code de cryptage unique par chacun des nombreux systèmes d'opérateurs. D'autres programmes peuvent être acceptés à partir de la tête de réseau 72 et ne sont pas cryptés par tous les systèmes d'opérateurs et sont transmis en commun par les systèmes d'opérateurs pour être vus par tous les abonnés sans restriction. Le réseau ne nécessite pas d'être un système de câble TV, mais peut être de toute forme de système de diffusion de programmes à une audience de masse qui transporte toute forme de signaux destinés à être reçus par une audience de masse.

Revendications

1) Méthode de distribution de signaux à des abonnés en règle caractérisée en ce qu'elle comprend:

5 (a) la mise en mémoire d'au moins un code d'identification valable pour le terminal d'abonné à la station centrale,

(b) la diffusion de promotions de services disponibles pour les abonnés dont chacun est associé à un code de promotion spécifique,

10 (c) le choix d'un desdits services et l'entrée d'un code choisi de promotion de service dans un terminal là où réside l'abonné,

(d) la lecture automatique d'un numéro d'identification associé au terminal en réponse à l'entrée d'un code de promotion choisi,

15 (e) le traitement du numéro d'identification et du code de promotion choisi suivant un algorithme de cryptage, et la génération par celui-ci d'un code crypté de requête d'événement,

20 (f) l'envoi du code de requête d'événement à un centre de vérification,

(g) le décryptage au centre de décryptage du code de requête d'événement, la vérification du numéro avec les codes d'identification valables, et l'envoi d'un mot de passe unique au terminal et du code de promotion choisi,

25

(h) l'entrée du mot de passe dans le terminal là où réside l'abonné, et

30 (i) la fourniture de l'accès à un service en utilisant l'un des signaux distribués correspondant au code de promotion choisi à l'abonné en réponse à l'entrée du mot de passe.

2) Méthode suivant la revendication 1, caractérisée en ce qu'elle comprend la distribution desdits services par le réseau câblé auxdits abonnés.

35

3) Méthode suivant la revendication 1, caractérisée en ce que ledit numéro d'identification est fixé et enregistré dans une mémoire ROM et un groupe de commutateurs de chaque terminal.

5 4) Méthode suivant la revendication 2, caractérisée en ce que ledit numéro d'identification est variable et est enregistré dans une RAM, de plus comprenant une adresse fixée à chaque terminal, le numéro d'identification étant reçu par le câble adressé à l'abonné identifié par l'adresse fixée.

10 5) Méthode suivant la revendication 2, caractérisée en ce qu'elle comprend la transmission d'une clé de cryptage de chacun desdits terminaux et la mise en mémoire de ladite clé de cryptage dans chaque terminal.

15 6) Méthode suivant la revendication 1, caractérisée en ce qu'elle comprend, chaque terminal ayant une adresse fixée, la transmission de clés de cryptage auxdits terminaux identifiés par lesdites adresses fixées et la mise en mémoire d'une clé de cryptage courante sur chaque
20 terminal.

7) Méthode suivant la revendication 5, caractérisée en ce qu'elle comprend la transmission de codes de programme en relation avec les codes de promotion de chacun desdits terminaux, et le cryptage et l'encodage
25 d'un code de programme comme code de promotion et d'un code d'identification du terminal utilisant une clé de cryptage enregistrée pour générer ledit code de requête d'événement.

8) Méthode suivant la revendication 6, caractérisée en ce que chaque
30 numéro d'identification fixé est enregistré dans une mémoire ROM dans chaque terminal.

9) Méthode suivant la revendication 7, caractérisée en ce qu'au
moins l'un desdits services est un signal de télévision "d'achat à la
35 consommation".

10) Méthode suivant la revendication 9, caractérisée en ce que ledit signal de télévision est brouillé, et en ce que la phase de la fourniture

de l'accès comprend le désembrouillage du signal vers l'entrée du mot de passe.

5 11) Méthode de distribution de signaux à des abonnés en règle caractérisée en ce qu'elle comprend:

10 (a) au terminal d'abonné, la génération d'un code de requête pour un service utilisant les signaux en accédant à un code enregistré de programme relatif au service et un code d'adresse relatif à une identification du terminal, et le cryptage des codes en utilisant une clé de cryptage pour engendrer un code de requête de service,

15 (b) la requête du service auprès d'un terminal central en envoyant le code de requête de service,

(c) au terminal central qui décrypte le code de requête de service et vérifie la validité du code d'adresse et du code de programme, et qui engendre un mot de passe,

20 (d) l'entrée du mot de passe dans le terminal de l'abonné et, en réponse, la fourniture de l'accès aux signaux fournissant le service.

25 12) Méthode suivant la revendication 11, caractérisée en ce qu'elle comprend le déchargement d'une clé de cryptage de la tête de réseau audit terminal d'abonné.

30 13) Méthode suivant la revendication 12, caractérisée en ce que les clés d'encryptage du distributeur de câble ou opérateur sont déchargées vers une pluralité de terminaux d'abonnés chacun identifié par l'adresse du terminal.

35 14) Méthode suivant la revendication 13, caractérisée en ce qu'elle comprend la fourniture desdits signaux par une pluralité de diffuseurs, et en déchargeant la même clé de cryptage à tous les abonnés enregistrés vers chaque diffuseur respectif, les clés de cryptage différentes étant prévues aux abonnés enregistrés vers les différents diffuseurs.

15) Méthode suivant la revendication 14, caractérisée en ce que les signaux sont distribués par un réseau câblé commun utilisé par tous ladite pluralité de diffuseurs.

16) Méthode suivant la revendication 11, caractérisée en ce que le code de requête est affiché sur un écran de télévision pour être noté par un abonné au moyen duquel ledit service peut être demandé.

5 17) Système de câble TV, caractérisé en ce qu'il comprend:

 (a) des terminaux d'abonnés, chaque terminal d'abonné comprenant:

 (i) un appareil pour mettre en mémoire un code d'identification de
10 terminal,

 (ii) un appareil pour mettre en mémoire un code d'identification de
programme,

15 (iii) un appareil pour mettre en mémoire une clé de cryptage,

 (iv) un appareil pour traiter les codes et la clé suivant un
algorithme de cryptage et ensuite engendrant un code de requête de
programme,

20 (v) un dispositif d'affichage pour afficher le code de requête de
programme,

 (vi) un appareil pour recevoir un mot de passe et, en réponse,
25 l'activation d'un programme à passer au dispositif d'affichage pour
affichage,

 (b) une tête de réseau et un réseau de câble TV qui lui est relié
pour transmettre une représentation cryptée du programme aux terminaux
30 d'abonnés,

 (c) une station centrale comprenant:

 (i) un appareil pour recevoir le code de requête de programme,

35 (ii) un appareil pour décrypter le code de requête de programme et
pour en tirer le code d'identification de programme et le code
d'identification du terminal,

(iv) un appareil pour vérifier les codes déterminés d'identification de programme et de terminal, et

5 (v) un appareil pour engendrer un mot de passe en réponse à la vérification de la validité des codes déterminés d'identification de programme et de terminal.

10 18) Système suivant la revendication 17, caractérisé en ce que le moyen de réception à la station central comprend un circuit de détection d'un signal de tonalité automatique couplé à une ligne téléphonique détectant chaque caractère dudit code de requête de programme envoyé sur une ligne téléphonique par un abonné, et une unité de réponse vocale pour engendrer synthétiquement une représentation vocale dudit mot de passe et
15 en l'envoyant à ladite ligne téléphonique pour la réception par ledit abonné.

20 19) Système suivant la revendication 17, caractérisé en ce qu'elle comprend une pluralité de stations centrales, chacune fonctionnant avec un opérateur différent de câble TV dont tous distribuent des programmes sur le même réseau à un groupe de terminaux d'abonnés, des clés cryptées dans les terminaux d'abonnés autorisés à recevoir d'un unique opérateur par câble tout en étant les mêmes, mais différents des clés cryptées dans les terminaux d'abonnés autorisés à recevoir à partir d'autres opérateurs
25 par câble.

20) Système de câble TV, caractérisé en ce qu'il comprend:

(a) un réseau de distribution de TV par câble,

30 (b) une pluralité d'équipements de diffusion de TV par câble prévus pour transmettre des programmes par le réseau destinés à des terminaux d'abonnés autorisés à ne recevoir que des équipements de diffusion individuels,

35 (c) une pluralité de terminaux d'abonnés reliés au réseau, chaque terminal d'abonné comprenant un code de cryptage, chaque code étant unique pour un diffuseur particulier,

(d) un appareil dans chaque terminal pour choisir un programme et pour obtenir un code de requête d'événement crypté dérivé de la clé cryptée,

5 (e) un appareil dans les équipements pour engendrer un mot de passe qui est unique pour un événement et unique pour un diffuseur individuel particulier, et

10 (f) un appareil pour envoyer le mot de passe au terminal où le programme a été choisi, pour commander l'affichage d'un programme choisi dans le terminal dans lequel le programme a été choisi,

de manière que des programmes diffusés par d'autres diffuseurs ne puissent pas être affichés dans d'autres terminaux.

15 21) Système de câble TV, caractérisé en ce qu'il comprend un réseau, des terminaux d'abonnés reliés au réseau et autorisés à recevoir des signaux offerts par certains des différents opérateurs, et des appareils pour limiter la réception, par des abonnés, de signaux à ceux qui sont offerts par ces opérateurs pour lesquels ont été autorisés les terminaux
20 d'abonnés.

22) Système suivant la revendication 21, caractérisé en ce que le moyen de réduire est un code de désembrouillage activé par un mot de passe pour le désembrouillage desdits programmes, le mot de passe fourni
25 par un opérateur spécifique pour un terminal spécifique étant inactif pour un autre terminal spécifique.

23) Système suivant la revendication 22, caractérisé en ce que l'autre terminal spécifique est l'un de ceux qui a été autorisé à
30 recevoir des signaux par un autre opérateur spécifique.

24) Méthode de distribution de signaux à divers abonnés caractérisée en qu'elle comprend:

(a) la connexion de plusieurs abonnés à un seul réseau de
35 distribution de programme,

(b) la connexion de plusieurs fournisseurs de programme audit réseau,

(c) l'envoi vers chacun des divers terminaux d'abonnés d'un code relatif à un fournisseur de programme particulier, et la mise en mémoire dudit code dans les terminaux d'abonnés concernés,

5 (d) la transmission de programmes à partir desdits fournisseurs de programmes au réseau dans des canaux séparés particuliers, et

(c) l'activation de la réception des programmes particuliers uniquement provenant des fournisseurs de programmes concernés par des terminaux d'abonnés spécifiques utilisant lesdits codes.

25) Méthode suivant la revendication 24, caractérisé en ce qu'elle comprend la distribution desdits signaux par un transmetteur satellite depuis la terre.

15 26) Méthode suivant la revendication 24, caractérisé en ce qu'elle comprend la distribution desdits signaux par un transmetteur local.

27) Méthode suivant la revendication 24, caractérisé en ce qu'elle comprend la distribution desdits signaux par un réseau de fibres optiques sur un grand territoire.

28) Méthode de distribution de signaux à des abonnés en règle connectés au réseau, caractérisée en ce qu'elle comprend la requête d'un programme à partir d'un fournisseur de programme basé sur un code de promotion de programme, portant un unique mot de passe vers un seul terminal relié au réseau et au programme, et envoyant le mot de passe audit terminal pour activer le programme choisi pour fonctionner.

29) Méthode de distribution de signaux à des abonnés en règle connectés au réseau, caractérisée en ce qu'elle comprend la requête d'un programme à partir d'un fournisseur de programme envoyant ledit programme sur un serveur "d'achat à la consommation" basé sur un code de promotion de programme, portant un unique mot de passe vers un seul terminal relié au réseau et audit serveur "d'achat à la consommation", et en envoyant le mot de passe audit terminal en activant le programme choisi pour fonctionner.

30) Méthode suivant la revendication 29, caractérisée en ce que le mot de passe est également unique audit programme.

31) Méthode de distribution de signaux à des abonnés en règle,
5 caractérisée en ce qu'elle comprend:

(a) la mise en mémoire de codes d'identification valable pour le terminal d'abonné à la station centrale,

10 (b) la diffusion de promotions de services disponibles pour les abonnés dont chacun est associé à un code de promotion spécifique,

(c) le choix d'un desdits services et l'entrée d'un code choisi de promotion de service dans un terminal là où réside l'abonné,

15 (d) la lecture automatique d'un numéro d'identification associé au terminal en réponse à l'entrée d'un code de promotion choisi,

(e) le traitement du numéro d'identification et du code de promotion choisi suivant un algorithme de cryptage, et la génération par celui-ci
20 d'un code crypté de requête d'événement,

(f) l'envoi du code de requête d'événement à un centre de vérification,

25 (g) le décryptage au centre de décryptage du code de requête d'événement, la vérification du numéro avec les codes d'identification valables, et l'envoi d'un mot de passe unique au terminal et du code de promotion choisi,

30 (h) l'entrée du mot de passe dans le terminal là où réside l'abonné, et

(i) la fourniture de l'accès à un service en utilisant l'un des signaux distribués correspondant au code de promotion choisi à l'abonné
35 en réponse à l'entrée du mot de passe.

32) Méthode de distribution de signaux à des abonnés en règle, caractérisée en ce qu'elle comprend:

(a) au terminal d'abonné, la génération d'un code de requête pour un service utilisant les signaux en accédant à un code enregistré de programme relatif au service et un code d'adresse relatif à une identification du terminal, et le traitement desdits pour engendrer un
5 code de requête de service,

(b) la requête du service auprès d'un terminal central en envoyant le code de requête de service,

(c) au terminal central qui décrypte le code de requête de service
10 et vérifie la validité du code d'adresse et du code de programme, et qui engendre un mot de passe,

(d) l'entrée du mot de passe dans le terminal de l'abonné et, en réponse, la fourniture de l'accès aux signaux fournissant le service.

15 33) Méthode suivant la revendication 32, caractérisée en ce que le code de programme est unique au seul serveur dudit service.

34) Méthode suivant la revendication 33, caractérisée en ce que ledit service est la provision d'un signal de programme "d'achat à la
20 consommation".

35) Système de câble TV, caractérisé en ce qu'elle comprend:

(a) des terminaux d'abonnés, chaque terminal d'abonné comprenant:

25 (i) un appareil pour mettre en mémoire un code d'identification de terminal,

(ii) un appareil pour mettre en mémoire un code d'identification de programme,

30 (iii) un appareil pour le traitement desdits codes et générant un code de requête de programme,

(iv) un dispositif d'affichage pour afficher les programmes et l'affichage dudit code de requête de programme,

(v) un appareil pour recevoir un mot de passe et, en réponse, l'activation d'un programme à passer au dispositif d'affichage pour affichage,

5 (b) une tête de réseau et un réseau de câble TV qui lui est relié pour transmettre une représentation cryptée du programme aux terminaux d'abonnés,

(c) une station centrale comprenant:

10 (i) un appareil pour recevoir le code de requête de programme, et la détermination du code d'identification du programme et le code d'identification du terminal,

15 (iv) un appareil pour vérifier la validité du programme déterminé et les codes déterminés d'identification, et

(v) un appareil pour engendrer un mot de passe en réponse à la vérification de la validité des codes déterminés d'identification de programme et de terminal.

20 36) Système de câble TV, caractérisé en ce qu'elle comprend:

(a) un réseau de distribution de TV par câble,

25 (b) une pluralité d'équipements de diffusion de TV par câble prévus pour transmettre des programmes par le réseau destinés à des terminaux d'abonnés autorisés à ne recevoir que des équipements de diffusion individuels,

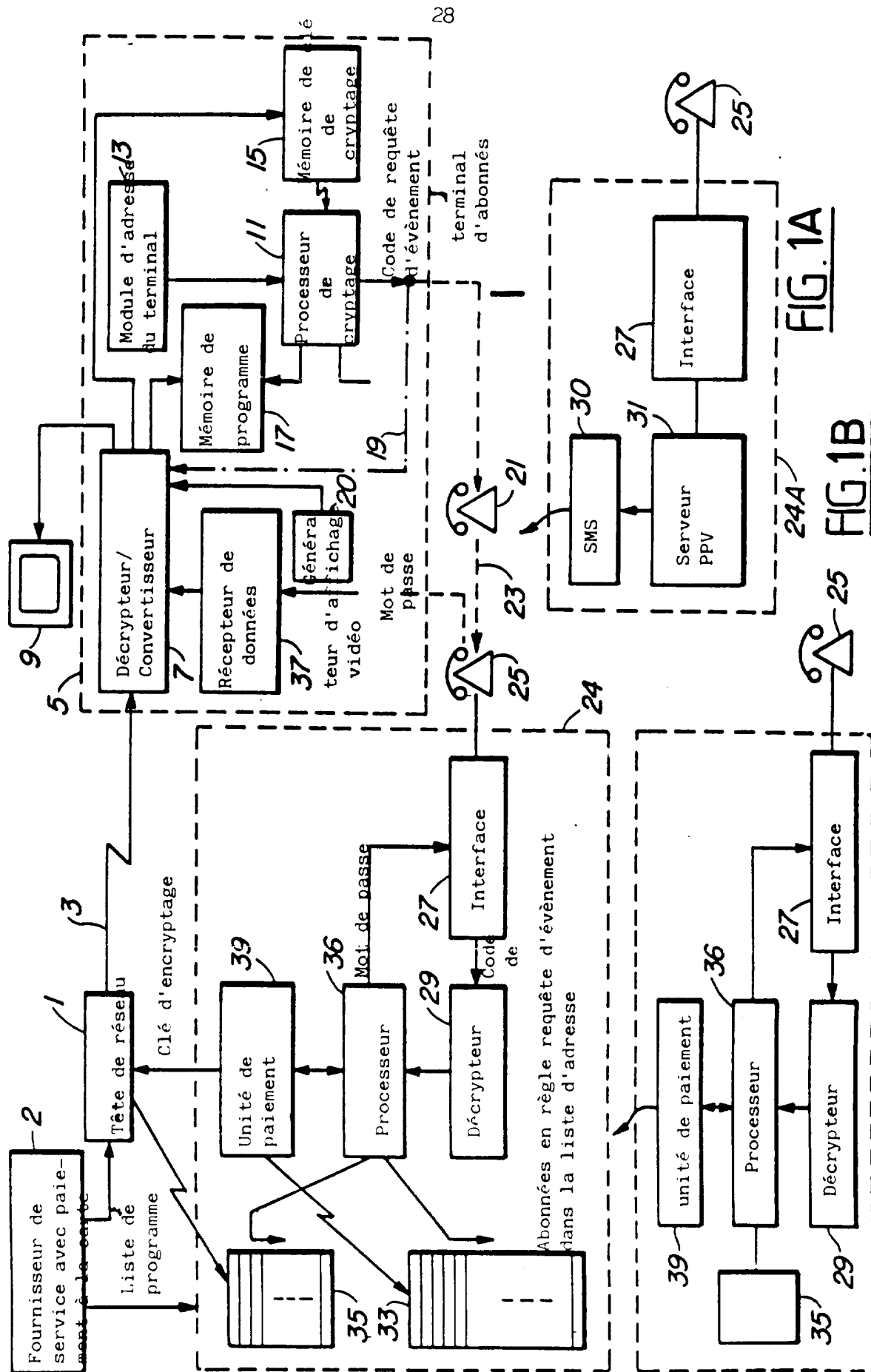
30 (c) une pluralité de terminaux d'abonnés reliés au réseau, chaque terminal d'abonné comprenant un code de cryptage, chaque code étant unique pour un diffuseur particulier,

35 (d) un appareil dans chaque terminal pour choisir un programme et pour obtenir un code de requête d'événement crypté dérivé du premier code,

(e) un appareil dans les équipements pour engendrer un mot de passe qui est unique pour un événement et unique pour un diffuseur individuel particulier, et

5 (f) un appareil pour envoyer le mot de passe au terminal où le programme a été choisi, pour commander l'affichage d'un programme choisi dans le terminal dans lequel le programme a été choisi,

10 de manière que des programmes diffusés par d'autres diffuseurs ne puissent pas être affichés dans d'autres terminaux.



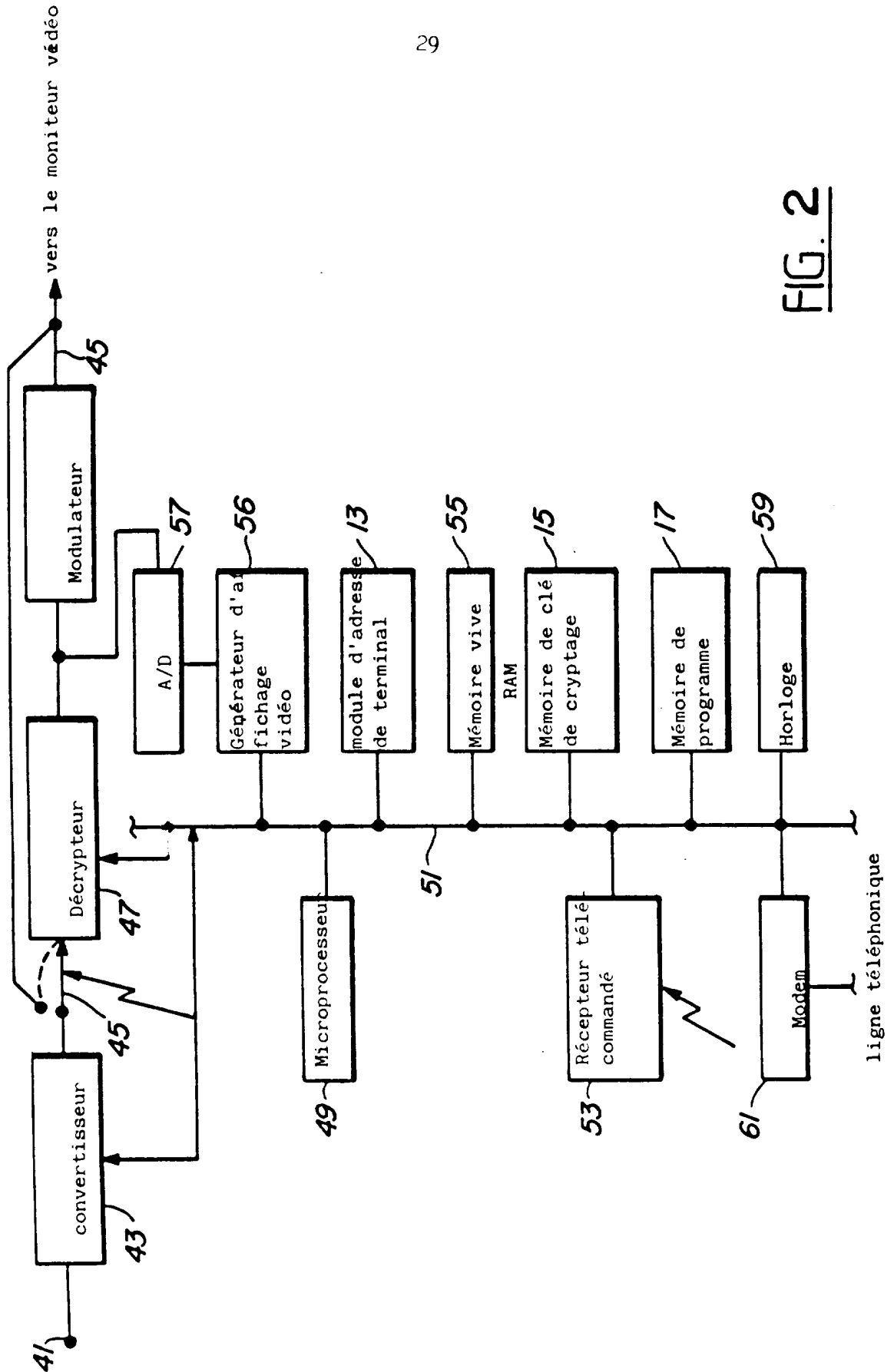


FIG. 2

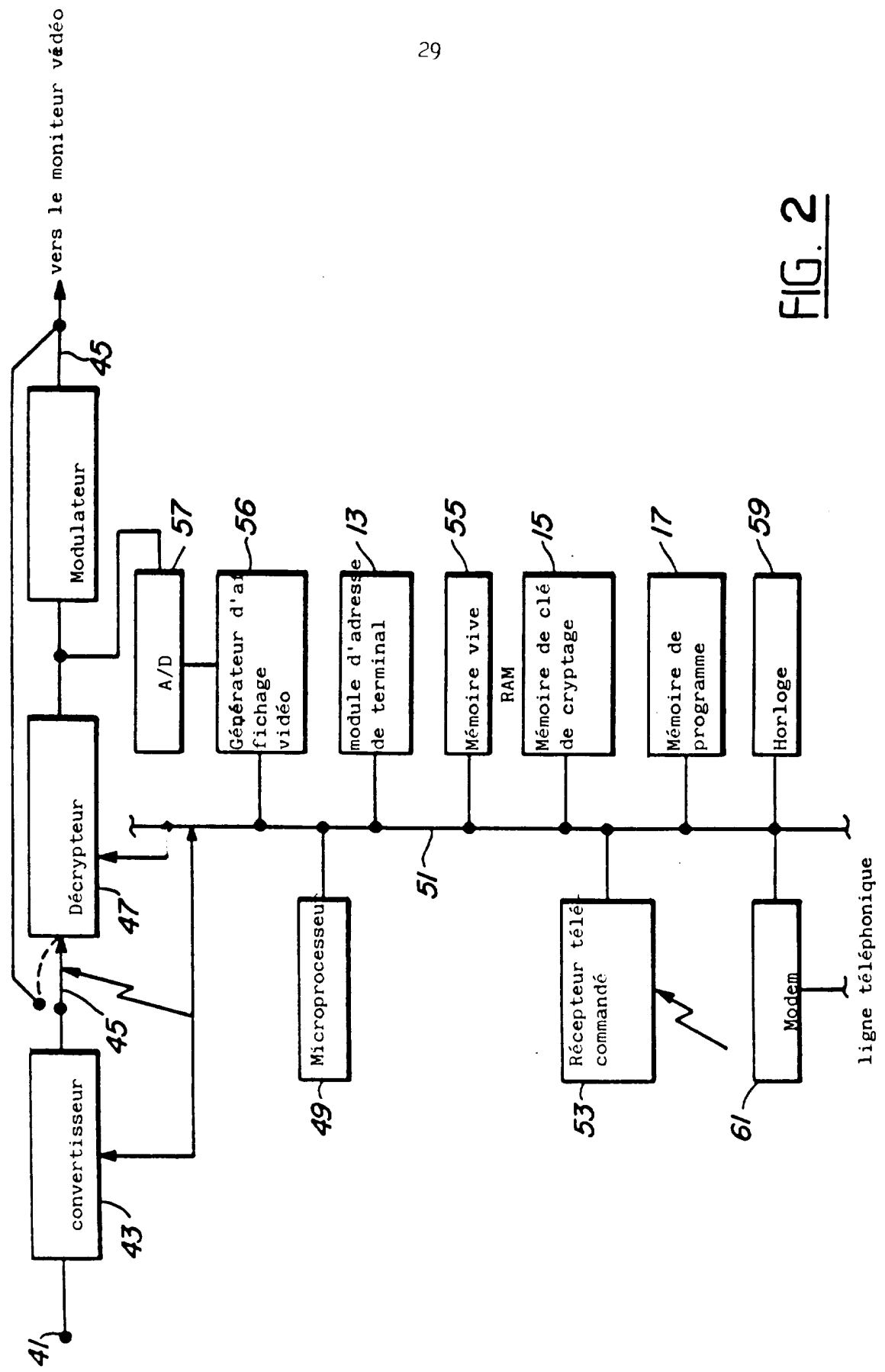


FIG. 2



Office européen
des brevets

RAPPORT DE RECHERCHE

établi en vertu de l'article 21 § 1 et 2
de la loi belge sur les brevets d'invention
du 28 mars 1984

Numero de la demande
nationale

B0 5574
BE 9500086

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.6)
Y	WO-A-85 03830 (AMERICAN TELEPHONE & TELEGRAPH) 29 Août 1985	1,11,17, 20,21, 24,28, 29,31, 32,35,36	H04N7/167 H04N7/16
A	* page 8, ligne 18 - page 10, ligne 16 *	2-10, 12-16, 18,19, 22,23, 25-27, 30,33,34	
	* page 11, ligne 2 - page 11, ligne 17 *		
	* page 15, ligne 35 - page 16, ligne 37 *		
Y	US-A-4 947 429 (BESTLER CHARLES B ET AL) 7 Août 1990	1,11,17, 20,21, 24,28, 29,31, 32,35,36	
A	* colonne 5, ligne 65 - colonne 6, ligne 68 *	2-10, 12-16, 18,19, 22,23, 25-27, 30,33,34	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6) H04N
A	US-A-4 893 248 (PITTS W HAMPTON ET AL) 9 Janvier 1990 * abrégé *	1-36	
A	US-A-4 755 872 (BESTLER CHARLES B ET AL) 5 Juillet 1988 * abrégé *	1-36	
A,D	GB-A-2 118 750 (TELECABLE VIDEOTRON LTD) 2 Novembre 1983 * le document en entier *	1-36	
Date d'achèvement de la recherche		Examineur	
22 Avril 1996		Greve, M	
CATEGORIE DES DOCUMENTS CITES			
X : particulièrement pertinent à lui seul		T : théorie ou principe à la base de l'invention	
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie		E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date	
A : arrière-plan technologique		D : cité dans la demande	
O : divulgation non-écrite		L : cité pour d'autres raisons	
P : document intercalaire		& : membre de la même famille, document correspondant	

**ANNEXE AU RAPPORT DE RECHERCHE
RELATIF A LA DEMANDE DE BREVET BELGE NO.**

B0 5574
BE 9500086

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche visé ci-dessus.
Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

22-04-1996

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO-A-8503830	29-08-85	BE-A- 901801	17-06-85
		CA-A- 1229385	17-11-87
		DE-T- 3590072	15-05-86
		FR-A- 2560473	30-08-85
		GB-A,B 2173379	08-10-86
		JP-T- 61501301	26-06-86
		NL-T- 8520023	02-01-86
		SE-A- 8504939	21-10-85
		US-A- 4890322	26-12-89

US-A-4947429	07-08-90	AUCUN	

US-A-4893248	09-01-90	AUCUN	

US-A-4755872	05-07-88	AUCUN	

GB-A-2118750	02-11-83	CA-A- 1177558	06-11-84
		DE-A- 3312723	27-10-83
		FR-A,B 2525420	21-10-83
		JP-A- 59015348	26-01-84
		NL-A,B 8301010	01-11-83
		US-A- 4623920	18-11-86
