(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
30 octobre 2003 (30.10.2003)

PCT

(10) Numéro de publication internationale
WO 03/090465 A1

(51) Classification internationale des brevets[7] : H04N 7/167, 5/00

(21) Numéro de la demande internationale : PCT/IB03/01514

(22) Date de dépôt international : 15 avril 2003 (15.04.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0664/02 19 avril 2002 (19.04.2002) CH

(71) Déposant *(pour tous les États désignés sauf US)* : NAGRAVISION SA [CH/CH]; 22, route de Genève, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : SASSELLI, Marco [CH/CH]; 20, chemin des Roches, CH-1803 Chardonne (CH).

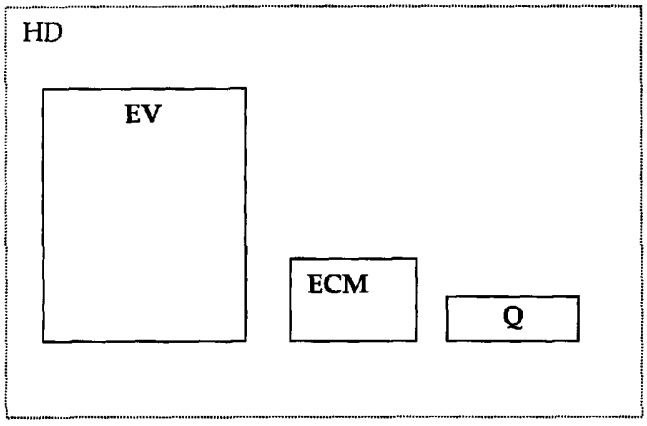
(74) Mandataire : ROULET, Pierre; Leman Consulting SA, 62, route de Clémenty, CH-1260 Nyon (CH).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD FOR MANAGING THE RIGHTS OF AN ENCRYPTED CONTENT STORED ON A PERSONAL DIGITAL RECORDER

(54) Titre : METHODE DE GESTION DES DROITS D'UN CONTENU ENCRYPTE ET STOCKE SUR UN ENREGISTREUR NUMERIQUE PERSONNEL



(57) Abstract: The aim of the invention is to provide a method for storing an event which is encrypted by control words (CW) guaranteeing access to said event at any moment, even if certain modifications occur in the designation of the identifiers of said events between the moment of storage and the moment of visualization.This is achieved by means of a method for storing such an event in a receiving and decrypting unit (STB) connected to a security unit (SC), said control words (CW) and the required rights being contained in control messages (ECM). The inventive method is characterized in that it comprises the following steps: the encrypted event is stored, along with the control messages (ECM), on the storage unit; the control messages (ECM) are transmitted to the security unit (SC); verification occurs as to whether the access rights to said event are contained in the security unit (SC), if this is the case, a receipt (Q) is provided for all or part of the control message (ECM) by means of a secret key (K) which is contained in the security unit (SC) and is proper to each security unit; said receipt (Q) is stored on the storage unit.

(57) Abrégé : Le but de la présente invention est de proposer une méthode de stockage d'un événement encrypté par des mots de contrôle (CW) qui garantisse l'accès à cet événement à n'importe quel moment, même si certaines modifications dans la désignation des identifiants de ces événements sont intervenues entre le moment du stockage et le moment de la visualisation. Ce but est atteint par une méthode de stockage d'un tel événement dans une unité de réception et de décryptage (STB) connectée a une unité de sécurité (SC), ces mots de contrôle (CW) et les droits nécessaires étant contenus dans des messages de contrôle (ECM), caractérisée en ce qu'elle comprend les étapes suivantes: -à stocker l'événement encrypte ainsi que les messages de contrôle (ECM) sur l'unité de stockage, -à transmettre à l'unité de sécurité (SC) les messages de contrôle (ECM), -à vérifier si les droits d'accès a cet événement sont contenus dans l'unité de sécurité (SC), -dans l'affirmative, à déterminer une quittance (Q) sur tout ou partie du message de contrôle (ECM) grâce a une clé secrète (K) contenue dans l'unité de sécurité (SC) et propre a chaque unité de sécurité, -à stocker cette quittance (Q) sur l'unité de stockage.

WO 03/090465 A1

(84) États désignés *(régional)* **:** brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

MÉTHODE DE GESTION DES DROITS D'UN CONTENU ENCRYPTÉ ET STOCKE SUR UN ENREGISTREUR NUMÉRIQUE PERSONNEL

La présente demande concerne le domaine des récepteurs/décodeurs de services à accès conditionnel, en particulier des récepteurs disposant d'unité de stockage tels que disques durs.

L'évolution technologique dans le domaine des capacités de stockage et de la rapidité des disques magnétiques (disque dur) a fait qu'il est devenu possible de stocker du contenu vidéo télédiffusé pour l'accéder en différé par l'utilisateur.

De tels enregistreurs sont connus sous la marque ReplayTV® ou Tivo® et proposent des stockages de plusieurs dizaines d'heures de transmission numérique. Ces enregistreurs ne sont toutefois pas directement intégrés aux récepteurs/décodeurs de services à accès conditionnel ; en particulier, le contenu est stocké sans protection particulière sur le disque, ce qui rend impossible la collecte des droits d'auteur associés au contenu, dans le cas où le disque serait ensuite dupliqué à des fins de redistribution commerciale. De plus, l'accès au contenu

A l'inverse, dans un système de télévision numérique à péage, le flux numérique transmis vers ces récepteurs est encrypté afin de pouvoir en contrôler l'utilisation et de définir des conditions pour une telle utilisation. Cette encryption est réalisée grâce à des mots de contrôle (Control Words) qui sont changés à intervalle régulier (typiquement entre 5 et 30 secondes) afin de dissuader toute attaque visant à retrouver un tel mot de contrôle.

Selon un mode de réalisation particulier, les mots de contrôle sont changés à des intervalles beaucoup plus long ce qui signifie que pour un événement considéré, il est encrypté par un seul mot de contrôle.

Pour que le récepteur puisse décrypter le flux encrypté par ces mots de contrôle, ces derniers lui sont envoyés indépendamment du flux dans des messages de contrôle (ECM) encryptés par une clé propre au système de transmission entre le centre de gestion (CAS) et le module de sécurité de l'unité d'utilisateur. En effet, les opérations de sécurité sont effectuées dans une unité de sécurité (SC) qui est généralement sous la forme d'une carte à puce, réputée inviolable. Cette unité peut être soit de type amovible ou directement intégrée au récepteur.

Lors de la décryption d'un message de contrôle (ECM), il est vérifié, dans l'unité de sécurité (SC), que le droit pour accéder au flux considéré est présent. Ce droit peut être géré par des messages d'autorisation (EMM) qui chargent un tel droit dans l'unité de sécurité (SC). D'autres possibilités sont également possibles tels que l'envoi de clés de décryptage.

Pour la suite de l'exposé, on appellera "événement" un contenu vidéo, audio (par exemple MP3) ou données (programme de jeu par exemple) qui est encrypté selon la méthode connue des mots de contrôle, chaque événement pouvant être encrypté par un ou une plusieurs mots de contrôle, chacun ayant une durée de validité déterminée.

La comptabilisation de l'utilisation de tels événements est aujourd'hui basée sur le principe de l'abonnement, de l'achat d'événements ou du paiement par unité de temps.

L'abonnement permet de définir un droit associé à un ou des canaux de diffusion transmettant ces événements et permet à l'utilisateur d'obtenir ces canaux en clair si le droit est présent dans son unité de sécurité.

Parallèlement, il est possible de définir des droits propres à un événement, tel qu'un film ou un match de football. L'utilisateur peut acquérir ce droit (achat par exemple) et cet événement sera

spécifiquement géré par ce droit. Cette méthode est connue sous l'appellation "pay-per-view" (PPV).

Pour ce qui concerne le paiement par unité de temps, l'unité de sécurité comprend un crédit qui est débité en fonction de la consommation réelle de l'utilisateur. Ainsi par exemple, une unité sera débitée chaque minute à ce crédit quelque soit le canal ou l'événement regardé. Il est possible selon les implémentations techniques, de varier l'unité de comptabilisation, soit dans la durée, soit dans la valeur du temps alloué, voire en combinant ces deux paramètres pour adapter la facturation au type d'événement transmis.

Un message de contrôle (ECM) ne contient pas uniquement le mot de contrôle mais également les conditions pour que ce mot soit renvoyé au récepteur/décodeur. Lors du décryptage des mots de contrôle, il sera vérifié si un droit associé aux conditions d'accès énoncées dans le message est présent dans l'unité de sécurité.

Le mot de contrôle n'est retourné à l'unité d'utilisateur que lorsque la comparaison est positive. Ce mot de contrôle est contenu dans un message de contrôle ECM qui est encrypté par une clé de transmission TK.

Pour que le droit soit présent dans l'unité de sécurité, il est généralement chargé dans cette unité par un message de gestion de droit (EMM) qui pour des raisons de sécurité, est généralement encrypté par une clé différente dite clé de droit (RK).

Selon une forme connue de diffusion de télévision à péage, les trois éléments suivants sont nécessaires pour décrypter un événement à un moment donné:

- l'événement encrypté par un ou une pluralité de mots de contrôle (CW),

- le ou les messages de contrôle ECM contenant les mots de contrôle (CW) et les conditions d'accès (AC)

- le droit correspondant stocké dans l'unité de sécurité permettant de vérifier les dites conditions d'accès.

Selon un schéma connu, l'événement encrypté qui est stocké sur une unité de stockage telle qu'un disque dur, est accompagné au moins du ou des messages de contrôle ECM.

Du fait que le décryptage à posteriori des messages ECM peut poser un problème, en particulier à cause du changement de la clé de transmission, une première solution est proposée dans le document EP 0 912 052, solution qui implique la décryption de ces messages dans l'unité de sécurité et la ré-encryption avant le stockage sur le disque.

Cette solution résout le problème de la durée de vie de la clé de transmission (changement de clés) mais charge grandement l'unité de sécurité au moment de l'enregistrement, sans savoir si le contenu enregistré sera un jour utilisé. De plus, une des règles fondamentales du système de sécurité est de ne retourner à l'unité d'utilisateur les mots de contrôle que si les droits existent. Dans ce cas, il se peut fort que ces droits n'existent pas si l'on considère un achat par événement. Le droit sera acquis lors de l'achat qui peut se faire bien plus tard au moment où l'utilisateur décide de visualiser cet événement.

Ce document EP 0 912 052 ne résout pas le problème de l'accès au droit car au moment de l'achat, le message de droit EMM doit être toujours diffusé pour qu'il soit chargé dans l'unité de sécurité.

Ainsi, la solution décrite dans ce document n'est applicable que pour des événements diffusés pour lesquels le droit est déjà présent dans l'unité de sécurité afin d'autoriser la décryption et la ré-encryption des ECM.

Un autre aspect est la conservation des droits d'un titulaire. Prenons l'exemple où un titulaire A dispose des droits de réception des canaux M, N, P. Il a donc le droit de visualiser ces canaux et donc d'enregistrer et de visualiser à volonté les événements se trouvant sur son unité de stockage. A chaque utilisation d'un tel événement, l'unité de sécurité va être sollicitée pour décrypter les messages ECM et retourner les mots de contrôle. Il est dès lors important que les droits liés à cet événement soient présents dans l'unité de sécurité.

Dans le cas d'un événement obtenu grâce à un abonnement, l'identification de cet événement est associée au canal de l'abonnement, par exemple M. Ainsi tous les événements portant l'identifiant M sont autorisés et les mots de contrôle retournés au décodeur.

Ces droits sont donc associés à un canal particulier défini par un identifiant tel que M. Lorsque l'abonné résilie son abonnement, ou le modifie pour d'autres canaux, il est résulte que les événements enregistrés sur l'unité de stockage seront inaccessibles car l'unité de sécurité refusera de renvoyer les mots de contrôle, le droit correspondant n'étant plus présent.

Cette situation peut se produire également si le canal M se voit attribuer un nouvel identifiant. Il est ainsi possible que la réorganisation des canaux fasse que ce canal se retrouve avec l'identifiant J4 au lieu de M. Du point de vu des droits de diffusion, l'unité de sécurité en est informée en temps utile et aucun désagrément n'est constaté par l'utilisateur.

Par contre, les conséquences pour un événement enregistré sont plus dramatiques. Cette réassignation aura tout simplement pour conséquence que l'événement enregistré sera inaccessible car le droit correspondant n'est plus présent dans l'unité de sécurité.

Le but de la présente invention est de proposer une méthode de stockage d'un événement encrypté par des mots de contrôle (CW) qui garantisse l'accès à cet événement à n'importe quel moment, même si certaines modifications dans la désignation des identifiants de ces événements sont intervenues entre le moment du stockage et le moment de la visualisation.

Ce but est atteint par une méthode de stockage d'un événement encrypté par un ou des mots de contrôle (CW) dans une unité de réception et de décryptage (STB) connectée à une unité de sécurité (SC), ces mots de contrôle (CW) et les droits nécessaires étant contenus dans des messages de contrôle (ECM), caractérisée en ce qu'elle comprend les étapes suivantes:

- à stocker l'événement encrypté ainsi que les messages de contrôle (ECM) sur l'unité de stockage,

- à transmettre à l'unité de sécurité (SC) les messages de contrôle (ECM),

- à vérifier si les droits d'accès à cet événement sont contenus dans l'unité de sécurité (SC),

- à déterminer une quittance (Q) sur tout ou partie du message de contrôle (ECM) grâce à une clé secrète (K) contenue dans l'unité de sécurité (SC) et propre à chaque unité de sécurité,

- à stocker cette quittance (Q) sur l'unité de stockage.

Selon une première variante de l'invention, cette quittance est constituée par une signature sur tout ou partie du message de contrôle et constitue un super droit qui permettra lors de l'utilisation subséquente de l'événement, de vérifier prioritairement cette quittance avant de vérifier les droits usuels dans l'unité de sécurité. La présence de cette

quittance, une fois reconnue pour un message de contrôle donné, permet d'ignorer les conditions d'accès.

Selon une deuxième variante de l'invention, lors de la génération de la quittance, en plus de la signature, une nouvelle partie est ajoutée qui décrit comment traiter ce message de contrôle lorsqu'il sera présenté à l'unité de sécurité. Cette condition peut être d'ignorer toutes les conditions énoncées dans ce message (ce qui revient à la solution précédente) ou énoncer d'autres conditions telles que de disposer d'un droit de reproduction ou définir une fenêtre en temps pour autoriser une telle reproduction.

Pour déterminer la signature, on va de préférence prendre une partie qui est inchangée pour tout l'événement. En effet, le message ECM comprend schématiquement deux parties:

a. le mot de contrôle pour le décryptage (ou les mots pair et impair)

b. le droit nécessaire pour retourner ce mot de contrôle.

Cette quittance permet de marquer un message de contrôle et donc d'ajouter d'autres informations destinées au traitement en mode reproduction. Le but est donc d'identifier un message de contrôle d'une manière indubitable. Dans la pratique, on constate que la partie b, soit le droit nécessaire, change moins fréquemment que le mot de contrôle. C'est pourquoi on choisira de préférence cette partie pour calculer la signature. Néanmoins, il n'est pas exclu de déterminer la signature sur le mot de contrôle, ou l'ensemble des deux parties.

Pour le calcul de cette signature, on détermine une image unique de la partie considérée par une fonction unidirectionnelle et sans collision sur ces données. Il est admis qu'il n'existe pas d'ensemble de données différent qui donne le même résultat que cette fonction. Cette image H est produite par une fonction de type Hash. L'algorithme utilisé peut être

de type SHA-1 ou MD5 et cette image exprime l'ensemble des données d'une manière unique.

L'opération suivante consiste à encrypter ces données grâce à une clé d'encryption K.

Avant l'opération d'encryption, par la clé K, il est possible d'ajouter un champ de données CD qui décrit des nouvelles conditions d'accès. L'ensemble de ces données (H et CD) constituant le quittance est ensuite encrypté par la clé de signature K.

Dans l'esprit de l'invention, le terme quittance signifie que l'on détermine un ensemble de données représentatif des conditions d'accès (par exemple dans le cas le plus simple) et unique à une unité de sécurité concernée grâce à la clé d'encryption K. Selon une forme de réalisation, il est possible d'encrypter directement les conditions d'accès du message de contrôle ECM par cette clé sans passer par l'opération de Hash. Selon une autre forme de réalisation, il est possible de déterminer cette image unique (fonction Hash) sur les conditions d'accès puis de crypter cette image par une première clé K1, ajouter les nouvelles conditions d'accès CD et d'encrypter le tout avec la même clé K1 ou une seconde clé K2.

L'invention sera mieux comprise grâce à la description détaillée qui va suivre et qui se réfère aux dessins annexés qui sont donnés à titre d'exemple nullement limitatif, à savoir:

- la figure 1 décrit une unité d'utilisateur STB avec unité de stockage,

- la figure 2, décrit l'ensemble des données stockées sur l'unité de stockage,

- la figure 3 décrit la structure d'un message de contrôle ECM.

Le décodeur STB illustré à la figure 1 reçoit des données en entrée sous forme encryptées. Ces données sont stockées dans l'unité de stockage HD et comprennent notamment l'événement considéré EV et les messages de contrôle ECM.

Ainsi, selon l'invention, ces deux ensemble de données sont accompagnés par un nouvel ensemble qui est illustré sur la figure 2 par le bloc de quittance Q.

La taille des différents blocs est donnée ici pour exemple. On peut néanmoins considérer que l'événement EV occupe la majeure partie, les messages de contrôle ECM une petite partie et selon une forme de réalisation, une seule quittance suffit pour l'ensemble de ces données.

En effet, si cette signature est effectuée sur la partie des conditions d'accès du message de contrôle, elle ne va pas varier pour tout l'événement considéré.

Sur la figure 3 est illustré la structure d'un message de contrôle ECM. Ce message contient, comme décrit précédemment, le mot de contrôle CW et les conditions d'accès. Ces conditions sont divisées en deux parties, une partie propre aux conditions de diffusion ACB et une partie propre aux conditions de reproduction ACR. Ce message comprend également une marque temps TP.

Parmi ces conditions, on peut trouver :

- numéro du canal (ou services), particulièrement utile pour l'abonnement,

- le thème de l'événement (par ex. sport, nouvelles, adulte)

- le niveau (prime time, après-midi, rediffusion)

- un numéro pour achat impulsif.

La duplication des conditions ouvre des possibilités à la gestion de l'événement lors de la reproduction. La quittance Q peut signifier qu'il est nécessaire de se conformer simplement aux conditions de reproduction ou alors signifier au contraire ignorer ces conditions.

Prenons l'exemple d'une fonction de blocage géographique. Cette fonction permet de bloquer la réception d'un événement sportif par exemple dans les 30 km autour du stade. Si ce blocage à un sens au moment de l'événement, par contre quelque jours plus tard, il n'a plus de raison d'être.

Dans les conditions de diffusion ACB, l'on trouvera les conditions du blocage par tranche de numéros d'unité de sécurité ou par code postal. Pour ce qui concerne les conditions de reproduction ACR, l'on trouvera une simple autorisation pour tous à partir d'une certaine date (pour autant que les autres conditions tels qu'abonnement, soient remplies).

Lors de la reproduction, la quittance Q est chargée en premier et décryptée par la clé secrète K, pour obtenir la signature SGN et les nouvelles conditions d'accès CD.

La signature SGN est ensuite conservée dans la mémoire de l'unité de sécurité avec les nouvelles conditions CD. Lorsque l'on présente un message de contrôle ECM à l'unité de sécurité, elle détermine par la fonction Hash une image unique H' sur la partie des droits AC selon cet exemple et compare cette valeur H' avec la signature SGN.

Si les deux valeurs sont identiques, l'unité de sécurité applique les conditions énoncées dans la partie conditions CD de la quittance. Si cette condition CD signifie "accès libre", cela permet de ne plus vérifier les conditions contenues dans le message de contrôle ECM et donc permet de s'affranchir de tous les changements structurels des canaux de diffusion.

Selon un autre exemple d'application, la nouvelle condition CD renvoie aux conditions de reproduction ACR. Dans ces conditions l'on ne trouve plus de référence à des canaux, ou autres éléments qui pourraient varier dans le temps (conditions structurelles) mais des conditions sur le temps durant lequel cet accès est accordé ou un nombre de fois. On sous-entend dans ce cas que les conditions d'accès liés à un abonnement ou autres ont été vérifiées lors de la formation de la quittance.

La quittance peut être évolutive. Dans certain cas il peut être intéressant de stocker une nouvelle quittance plus favorable que l'ancienne. Ceci est le cas notamment lors d'un achat impulsif. Dans ce cas une première quittance est générée lors du stockage sans que l'utilisateur n'aie acheté cet événement.

Les conditions contenues dans cette quittance vont renvoyer aux conditions contenues dans le message de contrôle ECM.

Au moment où l'utilisateur décide d'acheter cet événement, une nouvelle quittance est générée qui ouvre la voie à une utilisation sans réserve de cet événement si les conditions sont définies comme telles. Cette quittance est alors transmise à l'unité de stockage pour remplacer l'ancienne.

REVENDICATIONS

1. Méthode de stockage d'un événement encrypté par un ou des mots de contrôle (CW) dans une unité de réception et de décryptage (STB) connectée à une unité de sécurité (SC), ces mots de contrôle (CW) et les droits nécessaires à l'accès de cet événement étant contenus dans des messages de contrôle (ECM), caractérisée en ce qu'elle comprend les étapes suivantes:

- à stocker l'événement encrypté ainsi que le ou les messages de contrôle (ECM) sur l'unité de stockage,
- à transmettre à l'unité de sécurité (SC) les messages de contrôle (ECM),
- à vérifier si les droits d'accès à cet événement sont contenus dans l'unité de sécurité (SC),
- à déterminer une quittance (Q) comprenant une signature (SGN) sur tout ou partie du message de contrôle (ECM) grâce à une clé secrète (K) contenue dans l'unité de sécurité (SC) et propre à chaque unité de sécurité,
- à stocker cette quittance (Q) sur l'unité de stockage.

2. Méthode selon la revendication 1, caractérisée en ce que la quittance (Q) n'est calculée que si les droits d'accès sont présents dans l'unité de sécurité.

3. Méthode selon la revendication 1, caractérisée en ce que la quittance (Q) comprend en plus une partie conditionnelle (CD) décrivant des nouvelles conditions indépendantes de la configuration structurelle de la diffusion de l'événement.

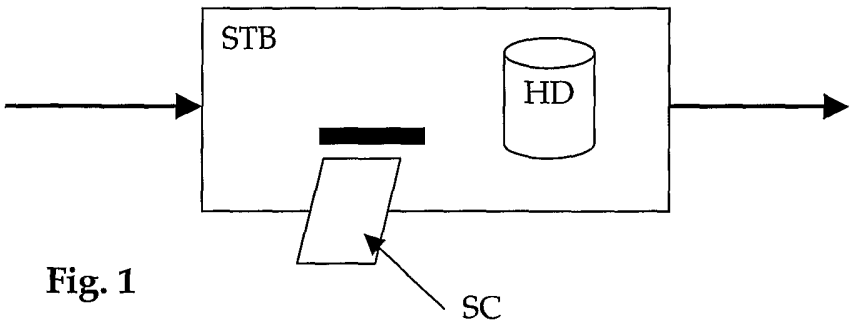


Fig. 1

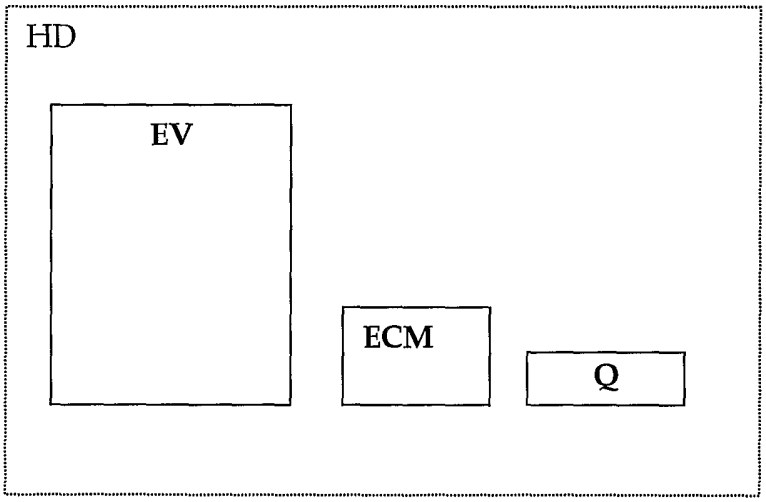


Fig. 2

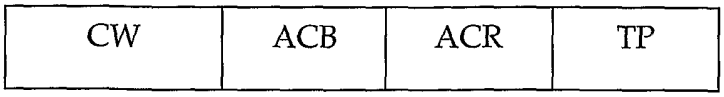


Fig. 3

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/IB 03/01514

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04N5/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 936 774 A (CANAL PLUS SA) 18 August 1999 (1999-08-18)	1
Y	figures 2,3 abstract column 1, line 56 - column 2, line 35 column 3, line 1 - line 15 column 3, line 51 - column 4, line 7 column 6, line 15 - line 35 column 8, line 30 - column 9, line 51 column 10, line 27 - column 11, line 2 column 11, line 20 - line 25 claims 1-9,13,16,17	2,3

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"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)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"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

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"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.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 July 2003	08/07/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dobbelaere, D.

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/IB 03/01514

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A Y	EP 0 975 165 A (SONY CORP) 26 January 2000 (2000-01-26) figures 2,6,7 column 3, line 10 - line 33 column 3, line 43 - line 49 column 4, line 37 - column 5, line 17 column 5, line 52 - column 6, line 30 column 6, line 45 - line 58 column 7, line 31 - column 9, line 40 column 10, line 9 - line 19 column 16, line 36 - column 18, line 26 claims 1-3,6,11,14	1 2,3
A	EP 0 866 615 A (SONY CORP) 23 September 1998 (1998-09-23) figures 1,2 abstract column 2, line 42 - column 3, line 40 column 6, line 6 - line 30 column 7, line 3 - line 19 column 7, line 28 - line 52 claims 4-15	1-3
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 266, 21 December 1995 (1995-12-21), pages 64-77, XP000559450 ISSN: 0251-0936 pp 76-77, paragraphe 7.3 'Home video recorders'	1-3

2

INTERNATIONAL SEARCH REPORT

Intel onal Application No
PCT/IB 03/01514

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0936774 A	18-08-1999	EP 0936774 A1	18-08-1999
		AT 225999 T	15-10-2002
		AU 754015 B2	31-10-2002
		AU 2295199 A	30-08-1999
		AU 749013 B2	13-06-2002
		AU 2296499 A	30-08-1999
		BR 9907877 A	31-10-2000
		BR 9907878 A	31-10-2000
		CA 2318879 A1	19-08-1999
		CA 2318992 A1	19-08-1999
		CN 1305674 T	25-07-2001
		CN 1296695 T	23-05-2001
		DE 69903408 D1	14-11-2002
		DE 69903408 T2	18-06-2003
		EP 0936812 A1	18-08-1999
		EP 1057332 A1	06-12-2000
		EP 1055305 A1	29-11-2000
		ES 2185311 T3	16-04-2003
		HR 20000486 A1	28-02-2001
		HR 20000487 A1	28-02-2001
		HU 0100651 A2	28-06-2001
		HU 0101456 A2	28-09-2001
		WO 9941907 A1	19-08-1999
		WO 9941874 A1	19-08-1999
		JP 2002503919 T	05-02-2002
		JP 2002514834 T	21-05-2002
		NO 20004062 A	13-10-2000
		NO 20004063 A	13-10-2000
		PL 342260 A1	04-06-2001
		PL 342261 A1	04-06-2001
		TR 200002348 T2	21-12-2000
		TR 200002350 T2	22-01-2001
		ZA 9901122 A	30-09-1999
		ZA 9901123 A	12-08-1999
EP 0975165 A	26-01-2000	EP 1126705 A2	22-08-2001
		EP 1244306 A2	25-09-2002
		EP 0975165 A2	26-01-2000
		CN 1390044 A	08-01-2003
		CN 1390043 A	08-01-2003
		CN 1390055 A	08-01-2003
		CN 1390056 A	08-01-2003
		CN 1390057 A	08-01-2003
		CN 1390053 A	08-01-2003
		CN 1389994 A	08-01-2003
		CN 1390054 A	08-01-2003
		CN 1115150 A ,B	17-01-1996
		DE 69523220 D1	22-11-2001
		DE 69523220 T2	13-06-2002
		DE 69530622 D1	05-06-2003
		EP 0691787 A1	10-01-1996
		JP 8077706 A	22-03-1996
		JP 2003134104 A	09-05-2003
		JP 2003143547 A	16-05-2003
		JP 2003101942 A	04-04-2003
		JP 2003116120 A	18-04-2003
		JP 2003116101 A	18-04-2003
		JP 2003143548 A	16-05-2003

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/IB 03/01514

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0975165 A		US 5796828 A	18-08-1998
		US RE38007 E1	25-02-2003
EP 0866615 A	23-09-1998	JP 10262013 A	29-09-1998
		CN 1198637 A	11-11-1998
		EP 0866615 A2	23-09-1998
		SG 70068 A1	25-01-2000
		TW 385618 B	21-03-2000
		US 6219422 B1	17-04-2001

RAPPORT DE RECHERCHE INTERNATIONALE

Dem Internationale No
PCT/IB 03/01514

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/167 H04N5/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 0 936 774 A (CANAL PLUS SA) 18 août 1999 (1999-08-18)	1
Y	figures 2,3 abrégé colonne 1, ligne 56 - colonne 2, ligne 35 colonne 3, ligne 1 - ligne 15 colonne 3, ligne 51 - colonne 4, ligne 7 colonne 6, ligne 15 - ligne 35 colonne 8, ligne 30 - colonne 9, ligne 51 colonne 10, ligne 27 - colonne 11, ligne 2 colonne 11, ligne 20 - ligne 25 revendications 1-9,13,16,17	2,3

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
2 juillet 2003	08/07/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dobbelaere, D.

2

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Dem Internationale No
PCT/IB 03/01514

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A Y	EP 0 975 165 A (SONY CORP) 26 janvier 2000 (2000-01-26) figures 2,6,7 colonne 3, ligne 10 - ligne 33 colonne 3, ligne 43 - ligne 49 colonne 4, ligne 37 - colonne 5, ligne 17 colonne 5, ligne 52 - colonne 6, ligne 30 colonne 6, ligne 45 - ligne 58 colonne 7, ligne 31 - colonne 9, ligne 40 colonne 10, ligne 9 - ligne 19 colonne 16, ligne 36 - colonne 18, ligne 26 revendications 1-3,6,11,14	1 2,3
A	EP 0 866 615 A (SONY CORP) 23 septembre 1998 (1998-09-23) figures 1,2 abrégé colonne 2, ligne 42 - colonne 3, ligne 40 colonne 6, ligne 6 - ligne 30 colonne 7, ligne 3 - ligne 19 colonne 7, ligne 28 - ligne 52 revendications 4-15	1-3
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 266, 21 décembre 1995 (1995-12-21), pages 64-77, XP000559450 ISSN: 0251-0936 pp 76-77, paragraphe 7.3 'Home video recorders'	1-3

2

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/IB 03/01514

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
		CN 1198637 A	11-11-1998
		EP 0866615 A2	23-09-1998
		SG 70068 A1	25-01-2000
		TW 385618 B	21-03-2000
		US 6219422 B1	17-04-2001