

①②

DEMANDE DE BREVET D'INVENTION

A1

②② Date de dépôt : 07.07.04.

③⑦ Priorité :

⑦① Demandeur(s) : THOMSON LICENSING S.A. Société
anonyme — FR.

④③ Date de mise à la disposition du public de la
demande : 13.01.06 Bulletin 06/02.

⑤⑥ Liste des documents cités dans le rapport de
recherche préliminaire : *Se reporter à la fin du
présent fascicule*

⑦② Inventeur(s) : AMOURIAUX JEAN MICHEL et
STEYER JEAN MARIE.

⑥⑦ Références à d'autres documents nationaux
apparentés :

⑦③ Titulaire(s) :

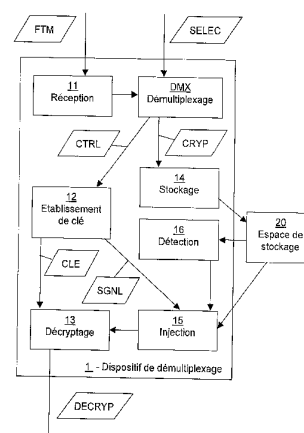
⑦④ Mandataire(s) : THOMSON.

⑤④ DISPOSITIF ET PROCEDE DE DEMULTIPLEXAGE SECURISE ET PRODUITS ASSOCIES.

⑤⑦ La présente invention concerne un dispositif (1) et un procédé de démultiplexage sécurisé d'au moins un flux multiplexé (FTM) de programmes, comprenant chacun des données de représentation cryptées (CRYP) et des données de contrôle d'accès (CTRL).

Le dispositif comprend des moyens de réception (11) du flux, des moyens de démultiplexage (DMX) en fonction d'une sélection d'un ou plusieurs programmes par un utilisateur, extrayant les données de contrôle et de représentation du programme sélectionné, des moyens d'établissement (12) d'une clé de décryptage (CLE) à partir des données de contrôle d'accès, et des moyens de décryptage (13) des données de représentation, au moyen de cette clé.

Il comprend aussi des moyens de stockage (14) d'au moins les données de représentation cryptées du programme sélectionné, dans un espace de stockage transitoire (20), parallèlement à l'établissement de la clé de décryptage, et des moyens d'injection (15) de ces données de représentation, de l'espace de stockage vers les moyens de décryptage lorsque la clé de décryptage est établie.



La présente invention se rapporte à un dispositif et un procédé de démultiplexage sécurisé, ainsi qu'à des produits correspondants.

Un récepteur-décodeur de signaux numériques comprend
5 classiquement un module ayant des fonctions de syntoniseur ou « tuner » et de démodulateur, un démultiplexeur, un module de décryptage, des décodeurs vidéo et audio, des modules de contrôle d'accès et d'interface de carte d'accès sécurisée, permettant de rendre opérationnel le module de décryptage, et une unité centrale ou « CPU » (pour « Central Processing
10 Unit »). Des données destinées aux décodeurs audio et vidéo sont typiquement transmises dans un flux de transport encodé selon la norme MPEG2 (pour « Moving Picture Experts Group »), sous forme multiplexée paquet par paquet. Chacun de ces paquets transporte des informations vidéo, audio, ou destinées au bon fonctionnement et à l'utilisation du
15 récepteur numérique. Le démultiplexeur permet d'aiguiller les paquets vers un traitement ou un autre, à partir d'un identifiant de paquet en en-tête de ce paquet.

Il est habituel de crypter les paquets à l'émission au moyen d'une clé de cryptage, afin de pouvoir contrôler l'accès à un programme
20 numérique. Cette clé est transmise (au moins partiellement) dans un format confidentiel au module de contrôle d'accès. Parmi les données circulant dans le récepteur, certaines sont cryptées et d'autres non, seules les données cryptées transitant par le module de décryptage. On reconstruit généralement la clé de décryptage dans le récepteur numérique, en utilisant
25 une carte d'accès sécurisée qui, à partir de données spécifiques de contrôle d'accès transmises dans le train numérique, permet de reconstituer complètement cette clé. La clé est ensuite positionnée dans le module de décryptage associé au démultiplexeur et a un train paquet identifié.

En pratique, chaque paquet du train numérique est identifié par
30 un descripteur de paquet et par des informations de support au décryptage, qui permettent de réaliser un éventuel décryptage suivant des autorisations

disponibles dans la carte d'accès sécurisée. On peut associer une clé de décryptage à un ou plusieurs identificateurs de paquets. Le nombre de clés à utiliser pour décrypter un flux complet est variable et dépend du type de contrôle d'accès et de son implémentation au niveau de la diffusion.

5

Selon les normes de compression d'images habituellement utilisées dans les décodeurs vidéo, on code des variations d'une image à une autre, afin de réduire sensiblement le nombre de données à transmettre. Il est ainsi d'usage d'envoyer des groupes d'images, notés GOPs (pour « Group Of Pictures »), dont chacun contient au moins une image se suffisant à elle-même pour son décodage, les autres images du groupe dépendant l'une de l'autre.

Notamment, la norme MPEG2 prévoit des séquences d'images dans lesquelles seule la détection d'une image de type intra (« image I »), unique dans chaque GOP, permet de commencer la décompression d'une séquence. Dans la norme JVT (pour « Joint Video Team »), seule la détection d'une image de type IDR (pour « Instantaneous Decoder Refresh ») permet de commencer la décompression d'une séquence vidéo, qui contient plusieurs images de type I – le GOP est dimensionné par l'image de type IDR. La détection de ce type d'images est usuellement réalisée soit par le démultiplexeur, soit par l'un des décodeurs audio et vidéo, soit par la CPU, par une opération de recherche en mémoire.

La taille des séquences vidéo résulte d'un compromis entre un souci de compression vidéo efficace (taille aussi grande que possible) et des opérations de traitement raisonnables pour le type d'image à coder (limite tolérable pour la taille). Habituellement, le nombre d'images par séquence est ainsi compris entre 24 et 60, ce qui se traduit par une durée de diffusion typiquement de l'ordre de 500 ms à plus de 1 s pour un groupe d'image. Des codages de séquences plus grandes sont néanmoins envisagées, avec une durée comprise entre 2 et 5 s.

Cette taille de séquence a un impact direct sur la durée d'un changement de programme (zapping), car le décodage ne peut démarrer qu'à la réception d'une image de type I pour MPEG2 ou IDR pour JVT. Le temps moyen nécessaire à l'établissement du décodage vidéo une fois que
5 les données sont prêtes à l'utilisation vaut en fait la moitié de la durée d'une séquence, et est donc compris habituellement entre 240 et 500 ms.

Un autre facteur augmentant la durée de démarrage du décodage vidéo pour un nouveau programme est la nécessité d'obtenir suffisamment de données pour pouvoir démarrer ce décodage. En effet, outre la durée de
10 transmission nécessaire pour obtenir la totalité de l'image de démarrage (de type I ou IDR), il s'y ajoute un délai requis pour pouvoir afficher la première image décompressée en temps voulu. Si cette image est prête trop tôt, l'image suivante risque de ne pas encore être complètement disponible, soit parce que les données de cette image suivante ne sont pas encore
15 transmises, soit parce que la durée de décodage n'est pas écoulée, soit encore parce que l'image de démarrage décodée est en avance par rapport à son instant de présentation prévu. Une fois que l'image de démarrage est prête à être affichée, on doit donc attendre de disposer de suffisamment d'images suivantes pour que l'affichage puisse se dérouler de manière
20 fluide.

Il faut également tenir compte de la durée nécessaire à l'obtention de la clé de décryptage à partir des données de contrôle d'accès transmises avec le flux. Chaque programme peut en effet être associé à des clés distinctes. Pour une transmission d'un train transport de type MPEG2,
25 chacune de ces clés est ainsi constituée par un mot de contrôle, noté CW (pour « Control Word »), obtenu à partir de messages de contrôle d'habilitation, notés ECM (pour « Entitlement Control Messages »). L'extraction des mots de contrôle est effectuée par la carte d'accès sécurisée, lors d'un traitement pouvant requérir une durée d'une demi-
30 séquence, c'est-à-dire couramment entre 300 et 400 ms.

Pendant la durée de zapping, aucun programme n'est généralement affiché, puisque l'ancien n'est plus sélectionné pour être démultiplexé, décrypté et décodé, et que le nouveau n'est pas encore disponible. Habituellement, l'utilisateur doit donc subir un temps mort, pendant lequel il se contente de voir à l'écran la dernière image du programme précédent ou un écran noir, jusqu'au démarrage du programme suivant. Cette durée d'attente risque d'être encore plus élevée dans l'avenir en raison de l'augmentation de la taille des groupes d'images et de la complexité de décryptage (en dépit d'une amélioration des capacités de traitement).

Pour réduire cette durée, on peut concevoir de poursuivre la diffusion locale du programme en cours jusqu'à ce que le programme suivant devienne disponible, tout en affichant par exemple superposé à l'écran un message de changement de chaîne. Cependant, une telle réalisation requiert un accroissement de complexité du récepteur numérique, et notamment un dédoublement de plusieurs des fonctionnalités – en particulier deux syntoniseurs. De plus, cette solution ne résout pas le problème de l'attente du programme suivant, et risque même d'être déplaisante si l'utilisateur tient à cesser immédiatement la diffusion d'un programme avant de pouvoir passer au suivant.

Le brevet US-5349641 décrit une méthode de transmission et de réception de programmes d'accès conditionnel avec un temps de commutation de programme réduit. Selon cette technique, les messages de contrôle d'habilitation ECM ayant des mots de vérification changés après chaque période de temps, appelée « phase », on transmet d'une part à une première fréquence, des messages de vérification principaux ECMp pour un programme d'accès principal, et d'autre part à une seconde fréquence inférieure, des messages de vérification secondaires ECMs pour des programmes secondaires (en fait, les programmes vers lesquels l'utilisateur

est susceptible de zapper). Les messages de vérification secondaire sont transmis en une phase unique, entre deux transmissions successives des messages de vérification principaux.

De cette manière, on évite de devoir attendre le message ECM du
5 programme vers lequel on commute, puisque ce message est déjà disponible, et on peut même calculer le mot de contrôle en parallèle avec l'acquisition de signal.

Bien que la durée de zapping soit ainsi réduite, cette méthode requiert cependant un traitement spécifique au niveau de l'émission. De
10 plus, elle nécessite un mécanisme d'identification et de stockage continu des messages ECM reçus tout au long de la réception de programmes.

La présente invention concerne un dispositif de démultiplexage sécurisé de flux multiplexés de plusieurs programmes, rendant possible une
15 réduction de la durée de zapping. De plus, ce dispositif peut autoriser l'exploitation de flux sans adaptation particulière au niveau de l'émission, et peut permettre de n'avoir à complexifier les traitements, qu'aux moments des commutations entre programmes.

20 L'invention concerne également un récepteur-décodeur numérique, un procédé de démultiplexage et un programme d'ordinateur ayant les avantages du dispositif de l'invention.

A cet effet, l'invention a pour objet un dispositif de démultiplexage
25 sécurisé comprenant :

- des moyens de réception d'au moins un flux multiplexé d'au moins deux programmes destinés à être représentés à un utilisateur, chacun de ces programmes comprenant au moins des données de représentation cryptées et des données de contrôle d'accès permettant de décrypter les
30 données de représentation de ce programme,

- des moyens de démultiplexage du flux multiplexé en fonction d'une sélection d'au moins un des programmes par l'utilisateur, les moyens de démultiplexage étant prévus pour extraire au moins les données de contrôle d'accès et les données de représentation cryptées du programme sélectionné,
- des moyens d'établissement d'une clé de décryptage des données de représentation cryptées à partir des données de contrôle d'accès,
- et des moyens de décryptage des données de représentation cryptées, au moyen de cette clé de décryptage.

Selon l'invention, le dispositif de démultiplexage comprend :

- des moyens de stockage d'au moins les données de représentation cryptées du programme sélectionné, dans au moins un espace de stockage transitoire, parallèlement à l'établissement de la clé de décryptage des données de représentation par les moyens d'établissement,
- et des moyens d'injection des données de représentation cryptées du programme sélectionné, de l'espace de stockage transitoire vers les moyens de décryptage lorsque la clé de décryptage est établie.

Par « représentation », on entend une diffusion locale destinée à des utilisateurs, notamment un affichage d'image pour de la vidéo et une émission sonore pour de l'audio.

Les « moyens » définis dans le dispositif de démultiplexage doivent s'entendre comme des entités purement fonctionnelles, qui peuvent ou non coïncider avec des entités matérielles. Plusieurs de ces moyens peuvent ainsi être regroupés dans un composant électronique ou un logiciel, et *a contrario*, certains des moyens peuvent être répartis dans plusieurs entités physiques. Ceci est vrai également pour les modes de réalisation préférés définis plus bas.

Les moyens de stockage, prévus pour stocker pour une durée transitoire au moins les données de représentation cryptées du programme sélectionné, peuvent être destinés à stocker sélectivement ces données, ou au contraire à stocker plus largement un ensemble de données incluant ces

5 données de représentation, tel que notamment l'ensemble du flux entrant.

Ils sont prévus pour opérer « parallèlement » aux moyens d'établissement, en ce sens qu'au moins une partie de l'enregistrement des données de représentation dans l'espace de stockage s'effectue pendant que la clé de décryptage est en cours d'établissement. Par ailleurs, les

10 moyens de stockage peuvent aussi fonctionner à d'autres moments sans que les moyens d'établissement soient en train de déterminer la clé de décryptage.

Les moyens de démultiplexage peuvent être situés en amont ou en aval des moyens de stockage, ou éventuellement les deux.

15 Les moyens d'injection sont destinés à transférer les données de représentation de l'espace de stockage transitoire vers les moyens de décryptage, avec optionnellement l'intermédiaire d'un démultiplexeur. L'injection est effective lorsque la clé de décryptage est établie, ce qui n'exclut pas qu'elle ait débuté avant ce moment d'établissement de la clé.

20

De manière surprenante, ce sont les données de représentation qu'on stocke en espace de stockage transitoire, tel qu'une mémoire tampon, tout en établissant en parallèle la clé de décryptage, puis c'est à une extraction des données utiles qu'on a recours à partir de cet espace de

25 stockage. On tranche ainsi avec le traditionnel mode du « pousser », ou mode « push », en introduisant partiellement le mode du « tirer », ou mode « pull ».

Cette extraction des données de représentation à partir de l'espace de stockage transitoire rend possible une récupération accélérée

30 des données utiles, telles que notamment les données de démarrage du

type images intra. On peut ainsi réduire sensiblement en moyenne le temps d'accrochage à un nouveau programme lors d'un zapping.

Selon un mode de réalisation particulier, le dispositif de
5 démultiplexage est utilisé pour tamponner (c'est-à-dire mettre en mémoire tampon) les données à décrypter (audio, vidéo et autres) pendant la durée de traitement par une carte d'accès sécurisée d'un message ECM de décryptage correspondant. Une fois le mot de contrôle CW destiné au décryptage disponible, le dispositif est prévu pour injecter les données
10 tamponnées dans un sous-ensemble de démultiplexage / décryptage avec ce mot de contrôle, qui offre la bonne clé de décryptage.

Dans une forme de réalisation préférée du dispositif de l'invention, les moyens de démultiplexage comprennent :

- 15 - des premiers moyens de démultiplexage prévus pour démultiplexer le flux reçu par les moyens de réception, extraire les données de représentation cryptées et les données de contrôle d'accès du programme sélectionné, et envoyer au moins les données de représentation cryptées vers les moyens de stockage et les données de contrôle d'accès
20 vers les moyens d'établissement,
- et des deuxièmes moyens de démultiplexage prévus pour recevoir au moins les données de représentation cryptées du programme sélectionné en provenance de l'espace de stockage transitoire par les moyens d'injection et pour transmettre les données de représentation
25 cryptées vers les moyens de décryptage.

Ce mode de réalisation repose donc sur un double démultiplexage, qui inclut un premier et un deuxième démultiplexage respectivement en amont et en aval des moyens de stockage. Le premier
30 démultiplexage rend possible une extraction des données de contrôle d'accès appropriées et un stockage sélectif en espace de stockage

transitoire des données du programme visé, incluant notamment les données de représentation. Cette partie est plutôt associée à un mode de pousser (réception des flux de données). Le deuxième démultiplexage permet de traiter distinctement les diverses données du programme visé, récupérées à partir de l'espace de stockage grâce aux moyens d'injection. Cette partie est plutôt associée à un mode de tirer (récupération des données stockées).

L'ensemble permet d'offrir une réduction efficace de la durée de zapping, grâce à un accrochage accéléré au nouveau programme (pendant que la clé est calculée, les données de représentation deviennent peu à peu disponibles pour y extraire les données de démarrage et les données suivantes). De plus, le stockage supplémentaire requis peut être assez restreint (une petite portion de programme pendant une courte durée) et rend possible une utilisation de composants standards.

Dans une variante de réalisation, on prévoit un basculement des premiers vers les seconds moyens de démultiplexage, lorsque la clé de décryptage est établie et l'espace de stockage transitoire est vidé de ses données de représentation. Cette variante repose sur une vitesse d'injection du module d'injection plus élevée que la vitesse d'arrivée des données du flux. Elle rend possible l'utilisation d'un unique multiplexeur en régime établi, les moyens de démultiplexage non utilisés étant alors libérés pour d'autres applications. Cependant, son implémentation est relativement complexe.

Dans une autre forme de réalisation préférée du dispositif de l'invention :

- les moyens de stockage sont prévus pour stocker le flux multiplexé dans l'espace de stockage transitoire,
- les moyens de démultiplexage ont un premier mode de fonctionnement dans lequel les moyens de démultiplexage reçoivent le flux multiplexé en provenance des moyens de réception, extraient les données

de contrôle d'accès du programme sélectionné et transmettent ces données de contrôle d'accès aux moyens d'établissement, et un deuxième mode de fonctionnement dans lequel les moyens de démultiplexage reçoivent le flux multiplexé en provenance de l'espace de stockage transitoire par les
5 moyens d'injection, extraient les données de représentation cryptées du programme sélectionné et transmettent les données de représentation aux moyens de décryptage,

- et le dispositif de démultiplexage comprend des moyens de commutation automatique des moyens de démultiplexage du premier mode
10 de fonctionnement au deuxième mode de fonctionnement lorsque la clé de décryptage est établie.

Une particularité intéressante de cette autre forme de réalisation est de pouvoir exploiter les mêmes moyens de démultiplexage pour agir en
15 amont et en aval des moyens de stockage. En amont, les moyens de démultiplexage permettent d'extraire les données de contrôle d'accès du programme sélectionné, et en aval, ils permettent d'extraire de l'espace de stockage transitoire les données appropriées pour ce programme, tels que notamment la vidéo et l'audio. Les mêmes moyens de démultiplexage
20 peuvent ainsi intervenir en mode de pousser (amont) et en mode de tirer (aval), le passage d'un mode à l'autre étant contrôlé par des moyens de commutation.

Cette réalisation, par rapport à celle de la forme précédente, requiert plus de place de stockage, puisque le tri dans le flux de données
25 reçu pour se focaliser sur le programme sélectionné n'est pratiqué qu'en aval du stockage. De plus, par rapport à des composants standards, elle peut nécessiter une cellule matérielle (« hardware ») supplémentaire, permettant l'écriture du flux reçu directement en espace de stockage sans
30 passer par une cellule de démultiplexage.

Selon une forme supplémentaire de réalisation préférée du dispositif de l'invention, les moyens de décryptage comprennent des premiers et des deuxièmes moyens de décryptage. De plus, les moyens de démultiplexage comprennent :

- 5 - des premiers moyens de démultiplexage prévus pour démultiplexer le flux reçu par les moyens de réception, extraire les données de représentation cryptées et les données de contrôle d'accès du programme sélectionné, et envoyer au moins les données de représentation cryptées vers les moyens de stockage et les données de contrôle d'accès
10 vers les moyens d'établissement,
- des deuxièmes moyens de démultiplexage prévus pour recevoir au moins les données de représentation cryptées du programme sélectionné en provenance de l'espace de stockage transitoire par les
15 moyens d'injection et pour transmettre les données de représentation cryptées vers les premiers moyens de décryptage,
- et des troisièmes moyens de démultiplexage prévus pour démultiplexer le flux reçu par les moyens de réception, extraire les données de représentation cryptées et les données de contrôle d'accès du
20 programme sélectionné, et envoyer au moins les données de représentation cryptées vers les deuxièmes moyens de décryptage et les données de contrôle d'accès vers les moyens d'établissement.

Le dispositif de démultiplexage comprend aussi des moyens de basculement des premiers moyens de décryptage vers les deuxièmes
25 moyens de décryptage pour exploiter les données de représentation après décryptage, ces moyens de basculement étant prévus pour opérer lorsque l'espace de stockage transitoire est totalement vidé par les moyens d'injection, des données de représentation cryptées stockées dans cet espace de stockage.

30 Cette réalisation rend possible l'utilisation d'un unique démultiplexeur en régime établi, les moyens de démultiplexage non utilisés

étant alors libérés pour d'autres applications. Elle est cependant relativement délicate à implémenter, car elle nécessite de mettre en place de manière adéquate une phase de transition en entrées des démultiplexeurs.

5 Préférentiellement, le dispositif de démultiplexage comprend des moyens de détection pour chacun des programmes, de données de démarrage parmi les données de représentation du programme, ces données de démarrage permettant d'initier une représentation du programme.

10

Ces moyens de détection peuvent en particulier être matériellement intégrés dans les moyens de démultiplexage, dans un ou plusieurs décodeurs (par exemple audio ou vidéo) en aval des moyens de décryptage, ou dans une unité centrale. Ils peuvent aussi être présents à la
15 fois dans plusieurs de ces entités.

Une identification des types de données du flux reçu est généralement présente au niveau des décodeurs ou de l'unité centrale pour s'appliquer à des flux décryptés. Cependant, il est intéressant d'exploiter des
20 moyens supplémentaires de détection en amont s'appliquant à des flux cryptés, ce qui permet de limiter les données à stocker et/ou à transférer.

Avantageusement, les données de représentation incluant des données vidéo, ces moyens de détection sont capables de détecter des images de type intra.

25

Les données de représentation étant prévues pour être reçues par les moyens de réception selon un débit de réception, les moyens d'injection sont de préférence capables d'injecter ces données de représentation vers les moyens de décryptage à un débit d'injection
30 supérieur au débit de réception.

De cette manière, on peut transmettre pour traitement les données mises dans l'espace de stockage transitoire plus rapidement que les données n'arrivent dans le flux. On rend ainsi possible une recherche plus rapide des données de démarrage et/ou un décryptage et un décodage plus rapide permettant de rattraper un retard à la représentation et de représenter aux bons instants de représentation les données de représentation décryptées.

Avantageusement, le dispositif de démultiplexage comprend alors des moyens de décodage des données de représentation décryptées, disposés en aval des moyens de décryptage et chacun des programmes étant prévu pour être représenté en temps réel à un débit de représentation des données de représentation de ce programme, les moyens de décodage sont aptes à décoder les données de représentation à un débit de décodage supérieur au débit de représentation.

Un tel décodage de rythme supérieur à l'unité permet de raccourcir les délais de traitement des données de représentation, lorsque ces données deviennent aptes à être décryptées après un zapping. En pratique, préférentiellement, c'est un décodeur vidéo qui dispose de capacités de décodage à une vitesse supérieure à l'unité.

Avec une injection rapide, il est également avantageux de disposer d'un mécanisme de détection rapide de données de démarrage (telle que la recherche d'images de type I ou IDR). De préférence, les moyens de détection associés sont capables de fonctionner un rythme au moins égal à celui d'injection.

Le dispositif de démultiplexage est préférentiellement prévu pour que les données de représentation comprennent des données

audiovisuelles. On entend par « données audiovisuelles » des données audio et/ou vidéo.

L'invention concerne également un récepteur – décodeur
5 numérique caractérisé en ce qu'il comprend un dispositif de démultiplexage conforme à l'une quelconque des formes de l'invention.

Un autre objet de l'invention est un procédé de démultiplexage sécurisé comprenant :

- 10 - une étape de réception d'au moins un flux multiplexé d'au moins deux programmes destinés à être représentés à un utilisateur, chacun de ces programmes comprenant au moins des données de représentation cryptées et des données de contrôle d'accès permettant de décrypter les données de représentation de ce programme,
- 15 - une étape de démultiplexage du flux multiplexé en fonction d'une sélection d'au moins un des programmes par l'utilisateur, dans laquelle on extrait au moins les données de contrôle d'accès et les données de représentation cryptées du programme sélectionné,
- une étape d'établissement d'une clé de décryptage des
20 données de représentation cryptées à partir des données de contrôle d'accès,
- et une étape de décryptage des données de représentation cryptées, au moyen de la clé de décryptage.

25 Selon l'invention, le procédé comprend une étape de stockage transitoire d'au moins les données de représentation cryptées du programme sélectionné, parallèlement à l'établissement de la clé de décryptage des données de représentation, l'étape de décryptage étant appliquée aux données de représentation cryptées du programme
30 sélectionné précédemment stockées, lorsque la clé de décryptage est établie.

Ce procédé de démultiplexage est préférentiellement mis en œuvre au moyen d'un dispositif de formes de l'invention.

5 L'invention s'applique également à un produit programme d'ordinateur comprenant des instructions de code de programme pour l'exécution d'au moins l'étape de stockage du procédé de démultiplexage selon l'invention, lorsque ce programme est exécuté sur un ordinateur. Par « produit programme d'ordinateur », on entend un support de programme
10 d'ordinateur, qui peut consister non seulement en un espace de stockage contenant le programme, tel qu'une disquette ou une cassette, mais aussi en un signal, tel qu'un signal électrique ou optique.

L'invention sera mieux comprise et illustrée au moyen des
15 exemples suivants de réalisation et de mise en œuvre, nullement limitatifs, en référence aux figures annexées sur lesquelles :

- la Figure 1 est un schéma de principe d'un dispositif de démultiplexage sécurisé conforme à l'invention ;
- 20 - la Figure 2 représente un premier mode de réalisation d'un dispositif de démultiplexage conforme à la Figure 1 ;
- la Figure 3 représente un deuxième mode de réalisation d'un dispositif de démultiplexage conforme à la Figure 1 ;
- la Figure 4 représente un troisième mode de réalisation d'un
25 dispositif de démultiplexage conforme à la Figure 1 ;
- la Figure 5 montre une implémentation particulière du dispositif de démultiplexage de la Figure 2, dans un récepteur-décodeur numérique ;
- la Figure 6 donne les évolutions en fonction du temps de la réception d'images, de la synchronisation requise pour les instants
30 d'affichage d'images, du décodage d'images et de l'affichage effectif d'images, obtenues avec le dispositif de démultiplexage de la Figure 4 ;

- et la Figure 7 montre une implémentation particulière du dispositif de démultiplexage de la Figure 3, dans un récepteur-décodeur numérique .

- 5 Sur les Figures 1 à 5 et 7, les modules représentés sont des unités fonctionnelles, qui peuvent ou non correspondre à des unités physiquement distinguables. Par exemple, ces modules ou certains d'entre eux peuvent être regroupés dans un unique composant, ou constituer des fonctionnalités d'un même logiciel. *A contrario*, certains modules peuvent
10 éventuellement être composés d'entités physiques séparées.

Des éléments identiques ou similaires sont désignés par les mêmes références, des suffixes A, B, C et D pouvant être utilisés pour respectivement quatre exemples de réalisation décrits ci-après.

- 15 Un dispositif de démultiplexage 1 sécurisé (figure 1) comprend un module de réception 11 d'un flux transport multiplexé FTM de plusieurs programmes, par exemple de programmes de télévision. Chacun de ces programmes comprend notamment des données de représentation cryptées CRYP et des données de contrôle d'accès CTRL permettant de décrypter
20 les données de représentation. Le dispositif de démultiplexage 1 est typiquement incorporé dans un récepteur-décodeur numérique.

- Ce dispositif 1 comprend également un ensemble de démultiplexage DMX du flux FTM, en fonction d'instructions de sélection SELEC d'un des programmes par un utilisateur, chargé d'extraire au moins
25 les données de contrôle d'accès CTRL et les données de représentation cryptées CRYP pour le programme sélectionné. Un module d'établissement 12 a pour fonction de construire une clé CLE (ou plusieurs) de décryptage de ces données de représentation cryptées CRYP, à partir de ces données de contrôle d'accès CTRL.

Un ensemble de décryptage 13 en aval de l'ensemble DMX de démultiplexage est prévu pour décrypter les données de représentation cryptées CRYP du programme sélectionné, au moyen de la clé CLE obtenue par le module d'établissement 12, et pour produire des données de représentation décryptées DECRYP.

Le dispositif de démultiplexage 1 comprend aussi un module de stockage 14 d'au moins les données de représentation cryptées CRYP du programme sélectionné, dans un espace de stockage transitoire 20, tel que notamment une mémoire tampon. Ce module de stockage 14 est prévu pour effectuer ce stockage (au moins en partie) parallèlement à l'établissement de la clé de décryptage CLE par le module d'établissement 12.

Un module d'injection 15 est prévu pour injecter les données de représentation cryptées CRYP du programme sélectionné, de l'espace de stockage 20 vers l'ensemble de décryptage 13 lorsque la clé de décryptage CLE est établie – un signal SGNL étant par exemple transmis à cet effet (directement ou non) par le module d'établissement 12 au module d'injection 15 pour déclencher l'injection.

Dans la réalisation préférée représentée, le dispositif de démultiplexage 1 comprend aussi un module de détection 16 de données de démarrage pour chaque programme, parmi les données de représentation de ce programme. Ces données de démarrage permettent d'initier une représentation du programme (telle qu'un affichage écran).

Dans la réalisation d'illustration (figure 1), le module de détection 16 effectue la détection à partir de l'espace de stockage 20, et influe sur le module d'injection 15. Cette réalisation repose sur des données de type transport non cryptées présentes dans le flux FTM reçu. Dans d'autres réalisations, le module de détection 16 est disposé en aval de l'ensemble de décryptage 13. De telles solutions sont utilisées en particulier quand le flux FTM ne contient pas de données de type transport décryptées, pertinentes

pour l'identification des données de démarrage. Plus précisément, selon une implémentation préférée, le module de détection 16 est disposé au niveau du décodage vidéo.

- 5 Le dispositif de démultiplexage 1, exposé sous forme générique, va maintenant être développé selon quatre exemples de réalisation particulièrement intéressants.

10 Dans le premier exemple de réalisation (figure 2), le dispositif 1 noté 1A comprend deux modules de démultiplexage DMX1A et DMX2A composant l'ensemble de démultiplexage DMX. Le premier module de démultiplexage DMX1A est chargé de démultiplexer le flux FTM reçu par le module de réception 11, d'extraire les données de représentation cryptées CRYP et les données de contrôle d'accès CTRL du programme sélectionné,
15 et d'envoyer au moins ces données de représentation cryptées CRYP vers le module de stockage 14 et les données de contrôle d'accès CTRL vers le module d'établissement 12. Le second module de démultiplexage DMX2A est quant à lui chargé de recevoir au moins les données de représentation cryptées CRYP du programme sélectionné en provenance de l'espace de
20 stockage transitoire 20, par le module d'injection 15, et de transmettre les données de représentation cryptées CRYP vers l'ensemble de décryptage 13, formé d'un module de décryptage 13A.

25 Dans le deuxième exemple de réalisation (figure 3), le dispositif 1 noté 1B comprend trois modules de démultiplexage DMX1B, DMX2B et DMX3B composant l'ensemble de démultiplexage DMX, et deux modules de décryptage 13B et 13B' composant l'ensemble de décryptage 13. Le module de décryptage 13B est disposé en aval des modules de démultiplexage DMX1B et DMX2B en série, et le module de décryptage 13B' est disposé en
30 aval du module de démultiplexage DMX3B. De plus, le dispositif de démultiplexage 1B comprend deux modules additionnels de stockage 19B et

19B' respectivement dans des espaces de stockage provisoire 30B et 30B' en aval des modules de décryptage 13B et 13B'. Ces espaces 30B et 30B' sont de préférence destinés à alimenter des décodeurs.

5 En pratique, des modules de stockage tels que 19B et 19B' et des espaces de stockages 30B et 30B' associés sont de préférence prévus pour chaque type de composante du flux FTM. On peut ainsi disposer par exemple de deux couples distincts de mémoires tampons respectivement pour l'audio et la vidéo (chaque couple comprenant les espaces de stockage
10 30B et 30B' pour une des composantes), ces mémoires tampons se remplissant et se vidant séparément au rythme respectivement de l'audio ou de la vidéo. Ainsi, le passage du stockage en aval du module de démultiplexage DMX2B, au stockage en aval du module de démultiplexage DMX3B est effectué pour l'audio indépendamment de la vidéo.

15

 Le premier module de démultiplexage DMX1B est, dans un premier temps, chargé de démultiplexer le flux FTM reçu par le module de réception 11, d'extraire les données de représentation cryptées CRYP et les données de contrôle d'accès CTRL du programme sélectionné, et d'envoyer
20 au moins ces données de représentations cryptées CRYP vers le module de stockage 14 et les données de contrôle d'accès CTRL vers le module d'établissement 12.

 Le deuxième module de démultiplexage DMX2B est chargé, dans
25 un deuxième temps, de démultiplexer les données de représentation cryptées CRYP du programme sélectionné en provenance de l'espace de stockage transitoire 20, fournies par le module d'injection 15. Cette étape se déclenche une fois la clé de décryptage CLE établie (signal SGNL2 du module d'établissement 12) et transmise au module de décryptage 13B, et le
30 deuxième module de démultiplexage DMX2B configuré. En fonctionnement, ce dernier fournit ainsi les données de représentation cryptées CRYP au

module de décryptage 13B, qui décrypte les données reçues et transmet les données décryptées DECRYPT au module de stockage 19B, qui les place provisoirement dans l'espace de stockage 30B avant exploitation. Cet espace 30B est celui utilisé en aval jusqu'à instruction contraire.

5

Le troisième module de démultiplexage DMX3B est chargé de démultiplexer le flux FTM reçu par le module de réception 11, une fois la clé de décryptage établie (signal SGNL3 du module d'établissement 12) et transmise au module de décryptage 13B'. Il est prévu pour extraire les données de représentation cryptées CRYPT et les données de contrôle d'accès CTRL du programme sélectionné, et pour envoyer les données de contrôle d'accès CTRL vers le module d'établissement 12 et les données de représentation cryptées CRYPT vers le module de décryptage 13B'. En fonctionnement, ce dernier décrypte les données reçues et transmet les données décryptées DECRYPT au module de stockage 19B', qui les place provisoirement dans l'espace de stockage 30B' avant exploitation. Cet espace 30B' n'est utilisé en aval qu'après instruction explicite (auparavant, seul l'espace 30B fournit les données à exploiter).

Une implémentation de synchronisation de fonctions permet de régler au cours du temps l'exploitation des démultiplexeurs DMX1B, DMX2B et DMX3B. Pour ce faire, le module d'établissement 12 est chargé de provoquer lorsque la clé de décryptage CLE est disponible, outre l'activation des modules de démultiplexage DMX2B et DMX3B, la libération du module de démultiplexage DMX1B. Dans la réalisation décrite, le module d'établissement est par ailleurs prévu pour communiquer la clé CLE en même temps aux deux modules de démultiplexage DMX2B et DMX3B, dès que celle-ci est déterminée.

De plus, le dispositif de démultiplexage 1B comprend un ensemble de commutation 18, destiné à agir lors d'une première transition

lorsque les données de représentation cryptées CRYP enregistrées dans l'espace de stockage transitoire 20 sont totalement consommées, et lors d'une seconde transition lorsque l'espace de stockage 30B est vidé. Pendant la phase de transition entre l'établissement de la clé de décryptage

5 CLE par le module d'établissement 12 et la le vidage complet de l'espace de stockage 30B, la même clé CLE est utilisée dans les deux modules de décryptage 13B et 13B'.

Lors de la première transition, l'ensemble de commutation 18 est

10 prévu pour libérer le deuxième module de démultiplexage DMX2B ainsi que l'espace de stockage 20 . Ainsi, une fois récupérées toutes les données de représentation cryptées CRYP stockées dans l'espace de stockage 20, seul le troisième démultiplexeur DMX3B poursuit le démultiplexage. En pratique, on peut donc se contenter d'utiliser simultanément parmi les

15 démultiplexeurs, d'abord DMX1B seulement, puis uniquement DMX2B et DMX3B, puis seulement DMX3B.

Lors de la seconde transition (espace de stockage 30B vide), l'ensemble de commutation 18 est prévu pour activer la sortie de l'espace de

20 stockage 30B' et désactiver la sortie de l'espace de stockage 30B, et pour provoquer à la fois une désactivation du module de décryptage 13B et une activation du module de décryptage 13B' (flèche d'action non représentée sur la figure 3).

25 La durée d'établissement de la clé CLE est distincte d'une durée de crypto période déterminée par un diffuseur de programme et un fournisseur de contrôle d'accès. En général, cette dernière vaut plusieurs fois la durée d'établissement de la clé CLE.

On considère plus précisément pour la fiabilité du système, que la

30 durée de validité des clés de décryptage est suffisante pour couvrir l'ensemble des opérations de démultiplexage ayant lieu dans les

démultiplexeurs DMX2B et DMX3B lors de la phase de transition, de manière à ce que la même clé de décryptage CLE puisse être utilisée dans tout le processus associé à cette phase.

De plus, on réalise aisément la transition dès lors que les
5 fonctions de démultiplexage sont en mesure de changer leur entrée de flux avec la précision d'un paquet. On n'a alors besoin que d'un seul démultiplexeur en régime établi.

Dans le troisième exemple de réalisation, pouvant être dérivé du
10 premier exemple (figure 2), le premier module de démultiplexage DMX1A n'est utilisé que durant les phases de remplissage de l'espace de stockage 20 (parallèle à l'établissement de la clé de décryptage CLE) et de vidage du contenu de cet espace 20 par le module d'injection 15. On choisit une vitesse d'injection par le module d'injection 15 plus élevée que la vitesse
15 d'arrivée des données du flux FTM. Il arrive alors un instant où l'espace de stockage 20 ne contient plus de données de représentation cryptées CRYP.

A ce moment, le module de démultiplexage DMX1A est supprimé et le flux FTM est connecté directement au second module de démultiplexage DMX2A. Les données de contrôle CTRL sont alors
20 récupérées par ce dernier.

Cette réalisation peut être aisément obtenue dès lors que les fonctions de démultiplexage sont en mesure de changer leur entrée de flux avec la précision d'un paquet. On n'a alors besoin, comme pour le deuxième
25 exemple, que d'un seul démultiplexeur en régime établi.

Dans le quatrième exemple de réalisation (figure 4), l'ensemble de démultiplexage DMX du dispositif de démultiplexage 1, noté 1D, se réduit à un unique module de démultiplexage DMX-D, et le module de stockage 14
30 est prévu pour stocker le flux FTM reçu dans l'espace de stockage

transitoire 20. Le module de démultiplexage DMX-D dispose de deux modes de fonctionnement :

- un premier mode dans lequel le module de démultiplexage DMX-D reçoit le flux FTM en provenance du module d'entrée 11, extrait les données de contrôle d'accès CTRL et transmet ces dernières au module d'établissement 12,
- et un second mode dans lequel le module de démultiplexage DMX-D reçoit le flux FTM en provenance de l'espace de stockage 20 par le module d'injection 15, extrait les données de représentation cryptées CRYP du programme sélectionné et transmet ces dernières à un module de décryptage 13D formant l'ensemble de décryptage 13.

De plus, le dispositif de démultiplexage 1D comprend un module de commutation 17 du module de démultiplexage DMX-D, du premier au second mode de fonctionnement lorsque la clé de décryptage CLE est établie (le module de commutation 17 recevant alors par exemple un signal SGNL' du module d'établissement 12).

Le premier exemple de réalisation (figure 2) est détaillé ci-après en référence à une implémentation particulière (figure 4). Dans cette implémentation, le dispositif de démultiplexage 1A est intégré à un récepteur-décodeur numérique 10, noté 10A, de flux audiovisuels. Celui-ci comprend :

- un syntoniseur / démodulateur 21 recevant le flux FTM,
- le premier module de démultiplexage DMX1A en sortie du syntoniseur / démodulateur 21, sous forme d'un démultiplexeur programmé pour extraire des informations d'identification d'un service ; ceci se traduit par exemple pour un flux MPEG2 par la recherche d'une table d'allocation de programme ou PAT (pour « Program Allocation Table ») décrivant une liste de services ou programmes disponibles dans un flux transport, puis d'une table de répartition de programme ou PMT (pour « Program Map

- Table ») décrivant une liste de composantes audio, vidéo, de données de décryptage ou d'autres données propres aux programmes considérés ; ce démultiplexeur est programmé pour extraire des données de fonctionnement FONC non cryptées et les données de décryptage constituant les données
- 5 de contrôle d'accès CTRL sous forme de messages ECM ;
- l'espace de stockage provisoire 20 en sortie du premier module de démultiplexage DMX1A, sous forme de mémoire tampon, prévu pour recevoir un flux transport partiel ne contenant que les composantes des flux audio, vidéo et autres données à décrypter, acquises par le module de
- 10 démultiplexage DMX1A (le module de stockage 14 est ici fonctionnellement inclus dans le module de démultiplexage DMX1A) ;
- le module d'injection 15, ayant une entrée reliée à l'espace de stockage 20 et une sortie reliée au second module de démultiplexage DMX2A ;
- 15 - le second module de démultiplexage DMX2A, programmé avec des identificateurs des composantes utilisées pour construire le flux partiel dans le premier module de démultiplexage DMX1A ; deux chemins de données partent en aval de ce module de démultiplexage DMX2A : un premier chemin CH1 sans décryptage pour données non cryptées, et un
- 20 second chemin CH2 pour données cryptées , conduisant au module de décryptage 13A ;
- le module d'établissement 12 sous forme d'un module récepteur 12A d'une carte d'accès sécurisée prévu pour recevoir les données de contrôle d'accès CTRL ; dès que les composantes véhiculant ces données sont disponibles, elles sont fournies à la carte d'accès qui
- 25 amorce l'extraction du ou des mot(s) de contrôle CW, aptes à servir de clé de décryptage CLE pour chacune des composantes audio, vidéo, ou d'autre type, à décrypter ;
- le module de décryptage 13A en aval du module de
- 30 démultiplexage DMX2A, prévu pour recevoir du module d'établissement 12 les clés CLE rendues disponibles ; une fois cette opération accomplie et le

second module de démultiplexage DMX2A programmé, le mécanisme d'injection des données peut démarrer et fournir des données à ce module de démultiplexage DMX2A ; le second module de démultiplexage DMX2A et le module de décryptage 13A forment une cellule de démultiplexage et

5 décryptage 22 qui produit des données non cryptées vidéo, audio et de fonctionnement FONC2 ;

- un décodeur vidéo 26 recevant les données vidéo décryptées de la cellule 22 ;
- un décodeur audio 27 recevant les données audio décryptées
- 10 de la cellule 22 ;
- et une unité centrale 25.

Un mécanisme de détection d'images de type I (ou IDR pour la norme JVT) est implémenté dans le second module de démultiplexage

15 DMX2A, l'un des décodeurs 26 ou 27, ou l'unité centrale 25.

Dans l'exemple préféré représenté, on dispose de débits de traitement appropriés de la manière suivante :

- le module d'injection 15 est en mesure d'injecter des données à
- 20 un débit plus important que le débit original des composantes du flux FTM reçu ;
- le mécanisme de recherche d'image de types I ou IDR fonctionne à un rythme au moins égal à la vitesse d'injection par le module d'injection 15 ;
- 25 - et le décodeur vidéo 26 permet de décoder des images plus rapidement que l'unité.

Cette implémentation permet d'assurer de façon anticipée la synchronisation requise pour les instants de présentation des images

30 décodées. En effet, on consomme ainsi les données mises dans l'espace de stockage 20 plus rapidement que les données n'arrivent avec le flux FTM.

Les processus de déroulement au cours du temps des traitements relatifs aux images à afficher au moyen du récepteur-décodeur numérique 10A vont maintenant être exposés plus en détail (Figure 6).

5

Le flux FTM entrant est par exemple formé d'un multiplex MPEG2, qui comprend une succession de groupes d'images I1, I2, I3... arrivant au cours du temps t (axe 30), chaque groupe d'images étant initié par une image intra I0. Cette succession forme ainsi une chaîne d'images CI1
10 formée de séquences successives SEQ1, SEQ2... En pratique, le récepteur-décodeur 10A reçoit une instruction de changement de programme et commence à identifier les composantes de décryptage appropriées (messages ECM) à un instant t0.

15

Les messages ECM associés au programme visé sont reçus avec le flux entrant FTM et sont exploités par la carte d'accès sécurisée pour déterminer la clé de décryptage CLE. Celle-ci est obtenue après une durée DT de traitement, à un instant t1. De plus, des instants d'affichage successifs des images reçues sont transportés sous forme de données de
20 synchronisation dans le flux FTM. Ils définissent une chaîne d'images CI3 synchronisées, qui est celle requise pour l'affichage des séquences SEQ1, SEQ2...

Selon la méthode classique, après avoir obtenu la clé CLE, le
25 récepteur numérique se mettrait en attente du prochain début de séquence. Ce dernier interviendrait ici avec l'arrivée de l'image intra I0 de la séquence SEQ2 au bout d'une durée d'attente DA, à un instant t3. La chaîne d'images reçues CI2 à partir de cet instant t3 permettrait alors de décoder les images et de les afficher aux instants d'affichage prévus, la première image décodée
30 (image intra I0) devant être prête à un instant t4.

Avec le récepteur-décodeur 10A, les données vidéo cryptées reçues sont stockées dans l'espace de stockage 20 (elles sont tamponnées) au fur et à mesure de leur réception (chaîne d'images CI4).

5 La disponibilité de la clé CLE initie l'étape de détection d'image de démarrage et les étapes de décryptage et de décodage. On obtient ainsi après une phase de recherche de début de séquence RD, une chaîne d'image CI5 correspondant au décodage des séquences d'images au cours du temps. Dans l'exemple représenté, l'image intra I0 de la séquence
10 courante SEQ1 a été reçue et tamponnée pendant l'établissement de la clé CLE.

L'affichage effectif des images décodées (chaîne d'images CI6, identique à la chaîne d'images CI3) n'est effectué qu'à partir du moment où les images deviennent disponibles en temps voulu par rapport aux instants
15 d'affichage prévus. Ainsi, les premières images décodées I-Tard, prêtes trop tardivement, ne sont pas affichées (ici, I0, I1 et I2 de la séquence SEQ1). Après une durée DR de recalage par rapport aux instants requis, la première image décodée à temps est affichée (ici l'image I4 de la séquence SEQ1 à un instant t2).

20

Plus tard, la séquence suivante est reçue puis affichée (ici, la séquence SEQ2 commence à être reçue à un instant t3 et doit commencer à être affichée à un instant t4).

25 En fin de compte, la durée d'affichage gagnée lors du zapping, par rapport à un accrochage qui serait fait classiquement sur l'image intra reçue pour la séquence suivante (ici, l'image I0 de la séquence SEQ2), est une durée GAIN donnée par la différence entre les temps t4 et t2.

30 Le deuxième exemple de réalisation (figure 3) est détaillé ci-dessous en référence à une implémentation particulière (figure 7). Dans

cette implémentation, le dispositif de démultiplexage 1B est intégré à un récepteur-décodeur numérique 10, noté 10B, de flux audiovisuels. Celui-ci comprend (les éléments identiques ou similaires à ceux du premier exemple ne sont pas détaillés) :

- 5 - le syntoniseur / démodulateur 21 recevant le flux FTM ;
- le premier module de démultiplexage DMX1B en sortie du syntoniseur / démodulateur 21 ; les données cryptées extraites par ce module vont vers le module de décryptage 13B ;
- l'espace de stockage provisoire 20 en sortie du premier module
- 10 de démultiplexage DMX1B ;
- le module d'injection 15 ayant une entrée reliée à l'espace de stockage 20 et une sortie reliée au deuxième module de démultiplexage DMX2B ;
- le deuxième module de démultiplexage DMX2B, en aval du
- 15 module d'injection 15 ;
- le troisième module de démultiplexage DMX3B, ayant une entrée reliée à une sortie du syntoniseur / démodulateur 21 (flux FTM) ;
- le module d'établissement 12 sous forme d'un module récepteur 12B d'une carte d'accès sécurisée, pour recevoir les données de
- 20 contrôle d'accès CTRL et extraire les mots de contrôle CW ;
- les modules de décryptage 13B et 13B' en aval des modules de démultiplexage DMX2B et DMX3B, prévus pour recevoir du module d'établissement 12 les clés CLE rendues disponibles ; une fois cette
- 25 opération accomplie et le troisième module de démultiplexage DMX3B programmé pour démultiplexer le flux FTM venant du syntoniseur /
- démodulateur 21, le mécanisme d'injection des données démarre et fournit des données au deuxième module de démultiplexage DMX2B et au module de décryptage 13B correspondant ; ces derniers produisent alors des
- 30 données non cryptées vidéo, audio et de fonctionnement FONC1 qui sont transférées dans l'espace de stockage 30B constitué de plusieurs mémoires tampons, notamment audio et vidéo (le module de stockage 19B est ici

- intégré au module de décryptage 13B) ; le troisième module de démultiplexage DMX3B et le module de décryptage 13B' correspondant produisent des données non cryptées audio, vidéo et de fonctionnement FONC2 et les fournissent à l'espace de stockage 30B',
- 5 constitué de plusieurs mémoires tampons ;
- le décodeur vidéo 26 recevant les données vidéo décryptées de la partie des espaces de stockage 30B correspondant aux mémoires tampons vidéo ;
 - le décodeur audio 27 recevant les données audio décryptées
- 10 de la partie des espaces de stockage 30B correspondant aux mémoires tampons audio ;
- un interrupteur 28 de choix de source pour les données de contrôle d'accès CTRL (cette source pouvant être le module de démultiplexage DMX1B ou DMX3B) à destination de la carte sécurisée,
- 15 formant une partie du module de commutation 18 ;
- et l'unité centrale 25.

Un mécanisme de détection d'image de type I ou IDR est implémenté dans le deuxième et le troisième modules de démultiplexage

20 DMX2B et DMX3B, l'un des décodeurs 26 ou 27, ou l'unité centrale 25.

De préférence, on dispose de débits de traitement appropriés comme dans l'implémentation particulière du premier exemple de réalisation (figure 5).

- 25 Une implémentation particulière du quatrième exemple de réalisation (figure 4) conduit au processus par étapes suivant :
- transfert du flux transport FTM complet à la fois dans une cellule de démultiplexage et décryptage (modules de démultiplexage DMX-B et de décryptage 13) et dans l'espace de stockage 20 ;
- 30 - extraction des données de contrôle d'accès CTRL et transmission à une carte d'accès sécurisée (module d'établissement 12) ;

- une fois les mots de contrôle CW rendus disponibles par la carte d'accès sécurisée, configuration du module de décryptage 13 de la cellule de démultiplexage et décryptage et aiguillage de la sortie de l'espace de stockage 20 vers cette cellule ; à ce moment, le flux FTM est
- 5 uniquement transféré dans l'espace de stockage 20 et non plus directement vers la cellule de démultiplexage et décryptage ;
- extraction des flux embrouillés tels que vidéo et audio par la cellule de démultiplexage et décryptage.

REVENDICATIONS

1. Dispositif de démultiplexage sécurisé (1) comprenant :
- 5 - des moyens de réception (11) d'au moins un flux multiplexé (FTM) d'au moins deux programmes destinés à être représentés à un utilisateur, chacun desdits programmes comprenant au moins des données de représentation cryptées (CRYP) et des données de contrôle d'accès (CTRL) permettant de décrypter lesdites données de représentation dudit
- 10 programme,
- des moyens de démultiplexage (DMX) dudit flux multiplexé (FTM) en fonction d'une sélection d'au moins un desdits programmes par ledit utilisateur, lesdits moyens de démultiplexage (DMX) étant prévus pour extraire au moins les données de contrôle d'accès (CTRL) et les données de
- 15 représentation cryptées (CRYP) dudit programme sélectionné,
- des moyens d'établissement (12) d'une clé de décryptage (CLE) desdites données de représentation cryptées (CRYP) à partir desdites données de contrôle d'accès (CTRL),
- et des moyens de décryptage (13) desdites données de
- 20 représentation cryptées (CRYP), au moyen de ladite clé de décryptage (CLE),
- caractérisé en ce que ledit dispositif (1) comprend :
- des moyens de stockage (14) d'au moins les données de
- 25 représentation cryptées (CRYP) dudit programme sélectionné, dans au moins un espace de stockage transitoire (20), parallèlement à l'établissement de ladite clé de décryptage (CLE) desdites données de représentation (CRYP) par les moyens d'établissement (12),
- et des moyens d'injection (15) desdites données de
- 30 représentation cryptées (CRYP) dudit programme sélectionné, dudit espace

de stockage transitoire (20) vers les moyens de décryptage (13) lorsque ladite clé de décryptage (CLE) est établie.

2. Dispositif de démultiplexage (1A) selon la revendication 1,
5 caractérisé en ce que lesdits moyens de démultiplexage (DMX) comprennent :

- des premiers moyens de démultiplexage (DMX1A) prévus pour démultiplexer ledit flux (FTM) reçu par les moyens de réception (11), extraire les données de représentation cryptées (CRYP) et les données de contrôle
10 d'accès (CTRL) dudit programme sélectionné, et envoyer au moins lesdites données de représentation cryptées (CRYP) vers lesdits moyens de stockage (14) et les données de contrôle d'accès (CTRL) vers lesdits moyens d'établissement (12),

- et des deuxièmes moyens de démultiplexage (DMX2A) prévus
15 pour recevoir au moins lesdites données de représentation cryptées (CRYP) dudit programme sélectionné en provenance dudit espace de stockage transitoire (20) par les moyens d'injection (15) et pour transmettre lesdites données de représentation cryptées (CRYP) vers les moyens de décryptage (13A).

20

3. Dispositif de démultiplexage (1D) selon la revendication 1, caractérisé en ce que :

- lesdits moyens de stockage (14) sont prévus pour stocker ledit flux multiplexé (FTM) dans ledit espace de stockage transitoire (20),
- 25 - les moyens de démultiplexage (DMX) ont un premier mode de fonctionnement dans lequel lesdits moyens de démultiplexage reçoivent ledit flux multiplexé (FTM) en provenance des moyens de réception (11), extraient les données de contrôle d'accès (CTRL) dudit programme sélectionné et transmettent lesdites données de contrôle d'accès (CTRL)
30 aux moyens d'établissement (12), et un deuxième mode de fonctionnement dans lequel lesdits moyens de démultiplexage (DMX) reçoivent ledit flux

multiplexé (FTM) en provenance dudit espace de stockage transitoire (20) par les moyens d'injection (15), extraient les données de représentation cryptées (CRYP) dudit programme sélectionné et transmettent lesdites données de représentation aux moyens de décryptage (13D),

- 5 - et ledit dispositif de démultiplexage (1D) comprend des moyens de commutation (17) automatique des moyens de démultiplexage (DMX) du premier mode de fonctionnement au deuxième mode de fonctionnement lorsque ladite clé de décryptage (CLE) est établie.

- 10 4. Dispositif de démultiplexage (1B) selon la revendication 1, caractérisé en ce que lesdits moyens de décryptage (13) comprennent des premiers (13B) et des deuxièmes (13B') moyens de décryptage, en ce que lesdits moyens de démultiplexage (DMX) comprennent :

- 15 - des premiers moyens de démultiplexage (DMX1B) prévus pour démultiplexer ledit flux (FTM) reçu par les moyens de réception (11), extraire les données de représentation cryptées (CRYP) et les données de contrôle d'accès (CTRL) dudit programme sélectionné, et envoyer au moins lesdites données de représentation cryptées (CRYP) vers lesdits moyens de stockage (14) et les données de contrôle d'accès (CTRL) vers lesdits
20 moyens d'établissement (12),

- des deuxièmes moyens de démultiplexage (DMX2B) prévus pour recevoir au moins lesdites données de représentation cryptées (CRYP) dudit programme sélectionné en provenance dudit espace de stockage transitoire (20) par les moyens d'injection (15) et pour transmettre lesdites
25 données de représentation cryptées (CRYP) vers les premiers moyens de décryptage (13B),

- et des troisièmes moyens de démultiplexage (DMX3B) prévus pour démultiplexer ledit flux (FTM) reçu par les moyens de réception (11), extraire les données de représentation cryptées (CRYP) et les données de
30 contrôle d'accès (CTRL) dudit programme sélectionné, et envoyer au moins lesdites données de représentation cryptées (CRYP) vers les deuxièmes

moyens de décryptage (13B') et les données de contrôle d'accès (CTRL) vers lesdits moyens d'établissement (12),

et en ce que ledit dispositif de démultiplexage (1B) comprend des moyens de basculement (18) des premiers moyens de décryptage (13B) vers les deuxièmes moyens de décryptage (13B') pour exploiter les données de représentation après décryptage (DECryp), lesdits moyens de basculement (18) étant prévus pour opérer lorsque ledit espace de stockage transitoire (20) est totalement vidé par les moyens d'injection (15), desdites données de représentation cryptées (CRYP) stockées dans ledit espace de stockage (20).

5. Dispositif de démultiplexage (1) selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit dispositif de démultiplexage comprend des moyens de détection (16) pour chacun desdits programmes, de données de démarrage (I, Idr) parmi lesdites données de représentation dudit programme, lesdites données de démarrage permettant d'initier une représentation dudit programme.

6. Dispositif de démultiplexage (1) selon la revendication 5, caractérisé en ce que lesdites données de représentation (CRYP) incluant des données vidéo, les moyens de détection (16) sont capables de détecter des images de type intra (I, Idr).

7. Dispositif de démultiplexage (1) selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdites données de représentation (CRYP) étant prévues pour être reçues par les moyens de réception (11) selon un débit de réception, les moyens d'injection (15) sont capables d'injecter lesdites données de représentation vers les moyens de décryptage (13) à un débit d'injection supérieur audit débit de réception.

8. Dispositif de démultiplexage (1) selon la revendication 7, caractérisé en ce qu'il comprend des moyens de décodage (26, 27) desdites données de représentation décryptées (DECryp), disposés en aval des moyens de décryptage (13) et en ce que chacun desdits programmes étant
- 5 prévu pour être représenté en temps réel à un débit de représentation des données de représentation dudit programme, les moyens de décodage (26, 27) sont aptes à décoder lesdites données de représentation à un débit de décodage supérieur au débit de représentation.
- 10 9. Dispositif de démultiplexage (1) selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit dispositif de démultiplexage est prévu pour que les données de représentation comprennent des données audiovisuelles.
- 15 10. Récepteur – décodeur (10) numérique caractérisé en ce qu'il comprend un dispositif de démultiplexage (1) conforme à l'une quelconque des revendications 1 à 9.
- 20 11. Procédé de démultiplexage sécurisé comprenant :
- une étape de réception d'au moins un flux multiplexé (FTM) d'au moins deux programmes destinés à être représentés à un utilisateur, chacun desdits programmes comprenant au moins des données de représentation cryptées (CRYP) et des données de contrôle d'accès (CTRL) permettant de décrypter lesdites données de représentation dudit
- 25 programme,
- une étape de démultiplexage dudit flux multiplexé (FTM) en fonction d'une sélection d'au moins un desdits programmes par ledit utilisateur, dans laquelle on extrait au moins les données de contrôle d'accès (CTRL) et les données de représentation cryptées (CRYP) dudit
- 30 programme sélectionné,

- une étape d'établissement d'une clé de décryptage (CLE) desdites données de représentation cryptées (CRYP) à partir desdites données de contrôle d'accès (CTRL),
- et une étape de décryptage desdites données de représentation cryptées (CRYP), au moyen de ladite clé de décryptage (CLE),

caractérisé en ce que ledit procédé comprend une étape de stockage transitoire d'au moins les données de représentation cryptées (CRYP) dudit programme sélectionné, parallèlement à l'établissement de ladite clé de décryptage (CLE) desdites données de représentation (CRYP), l'étape de décryptage étant appliquée aux dites données de représentation cryptées (CRYP) du programme sélectionné précédemment stockées, lorsque la clé de décryptage (CLE) est établie,

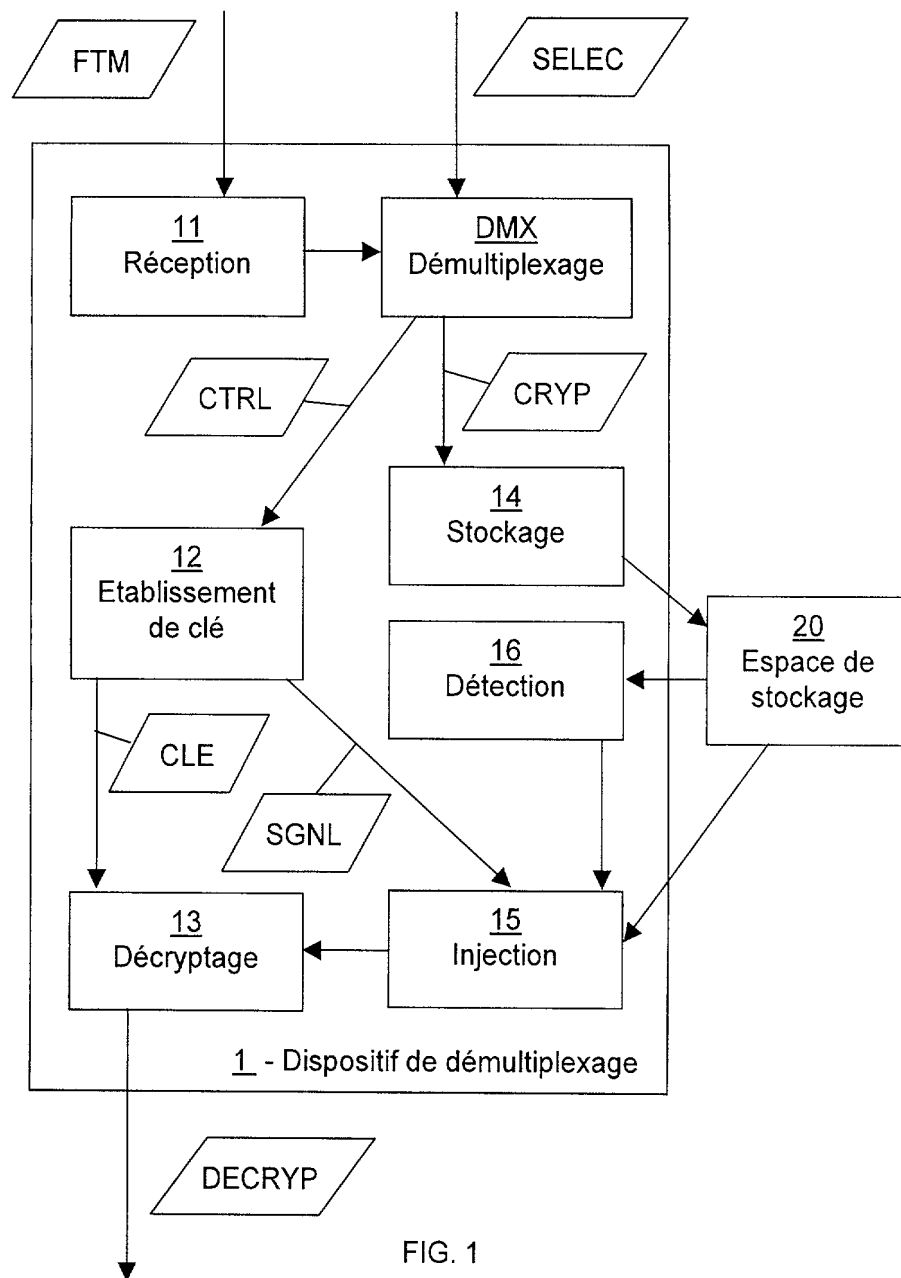
15

ledit procédé de démultiplexage étant préférentiellement mis en œuvre au moyen d'un dispositif de démultiplexage sécurisé (1) conforme à l'une quelconque des revendications 1 à 10.

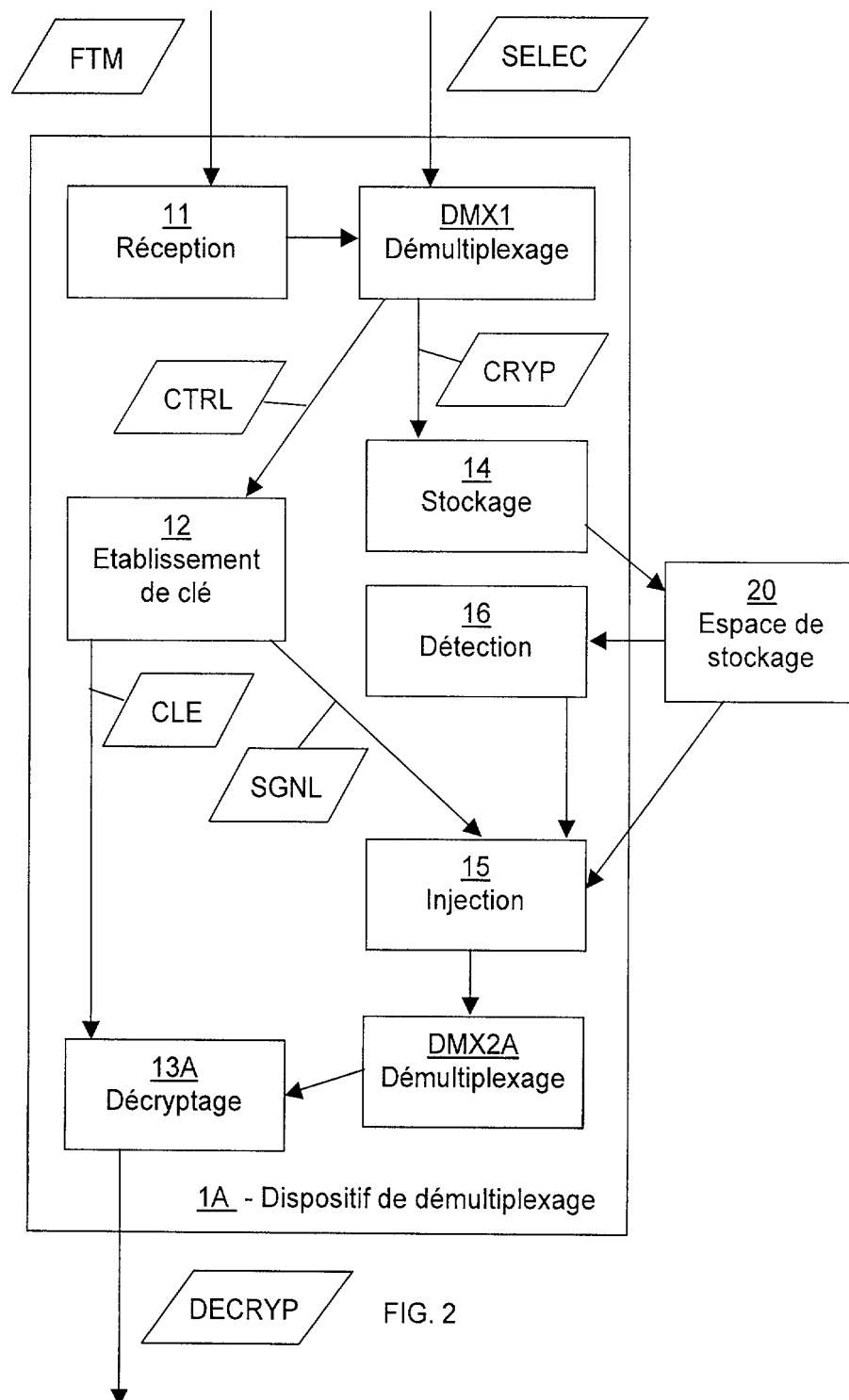
12. Produit programme d'ordinateur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution d'au moins l'étape de stockage du procédé de contrôle d'accès selon la revendication 11 lorsque ledit programme est exécuté sur un ordinateur.

20

1/7



2/7



3/7

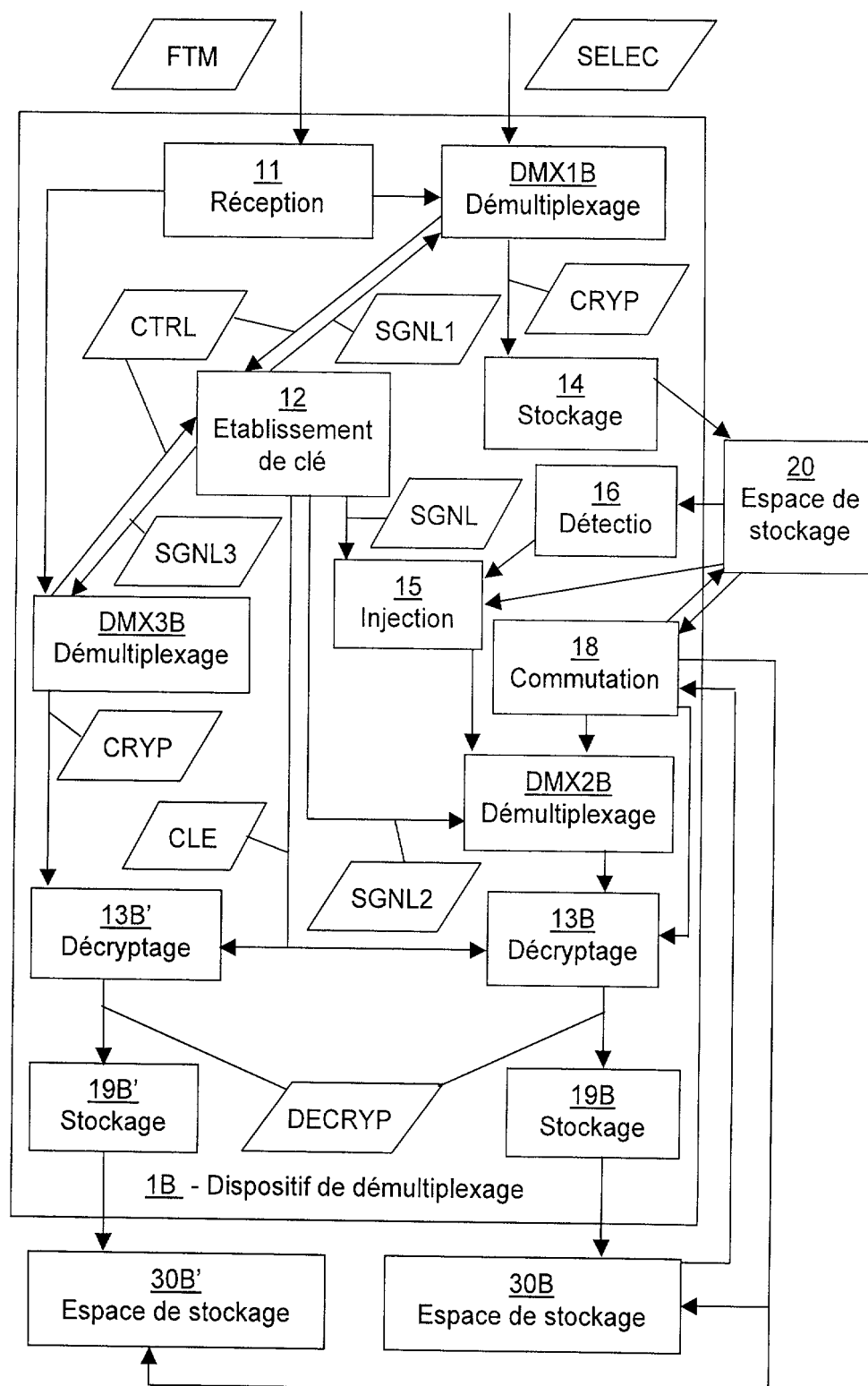
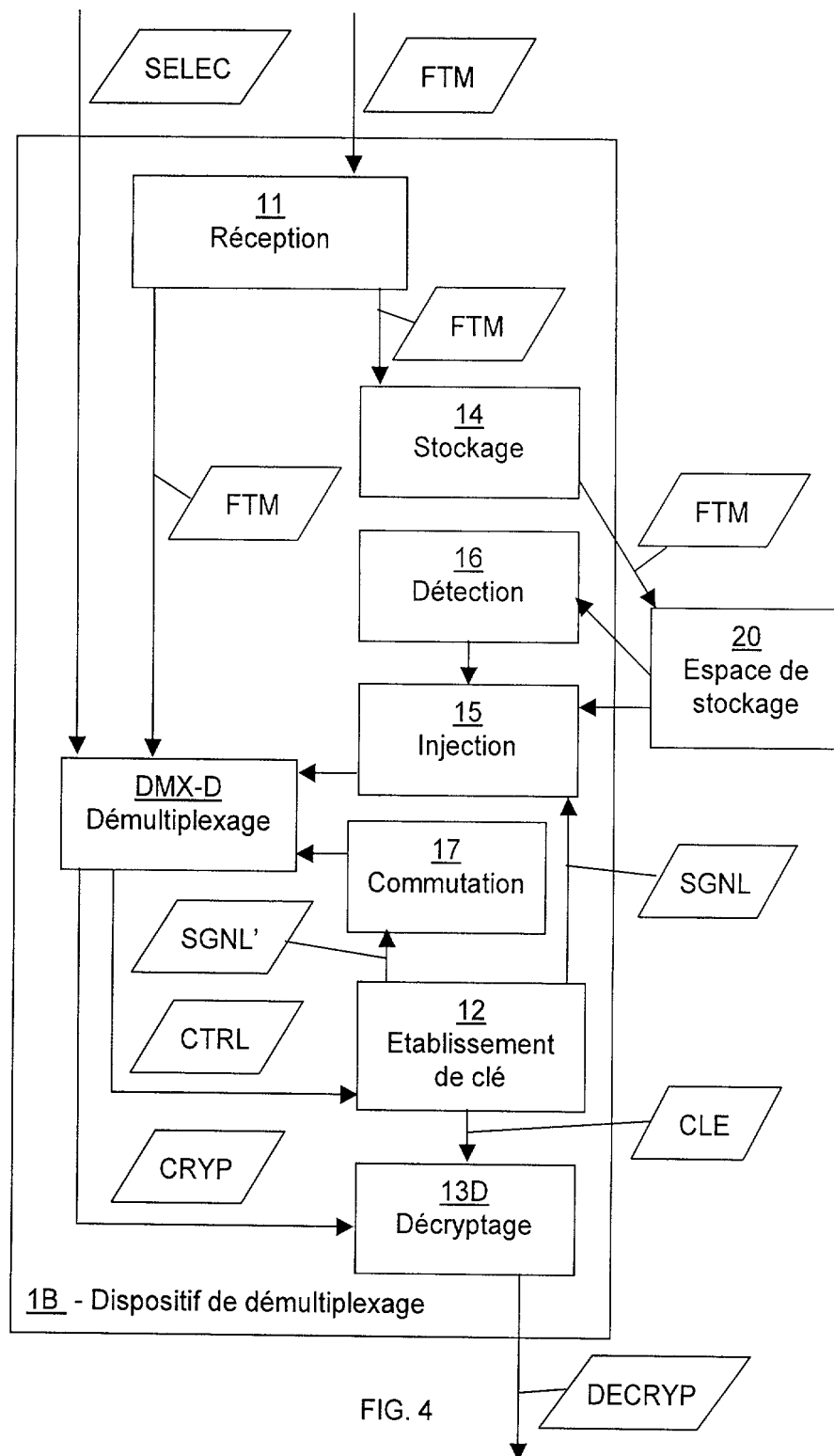


FIG. 3

4/7



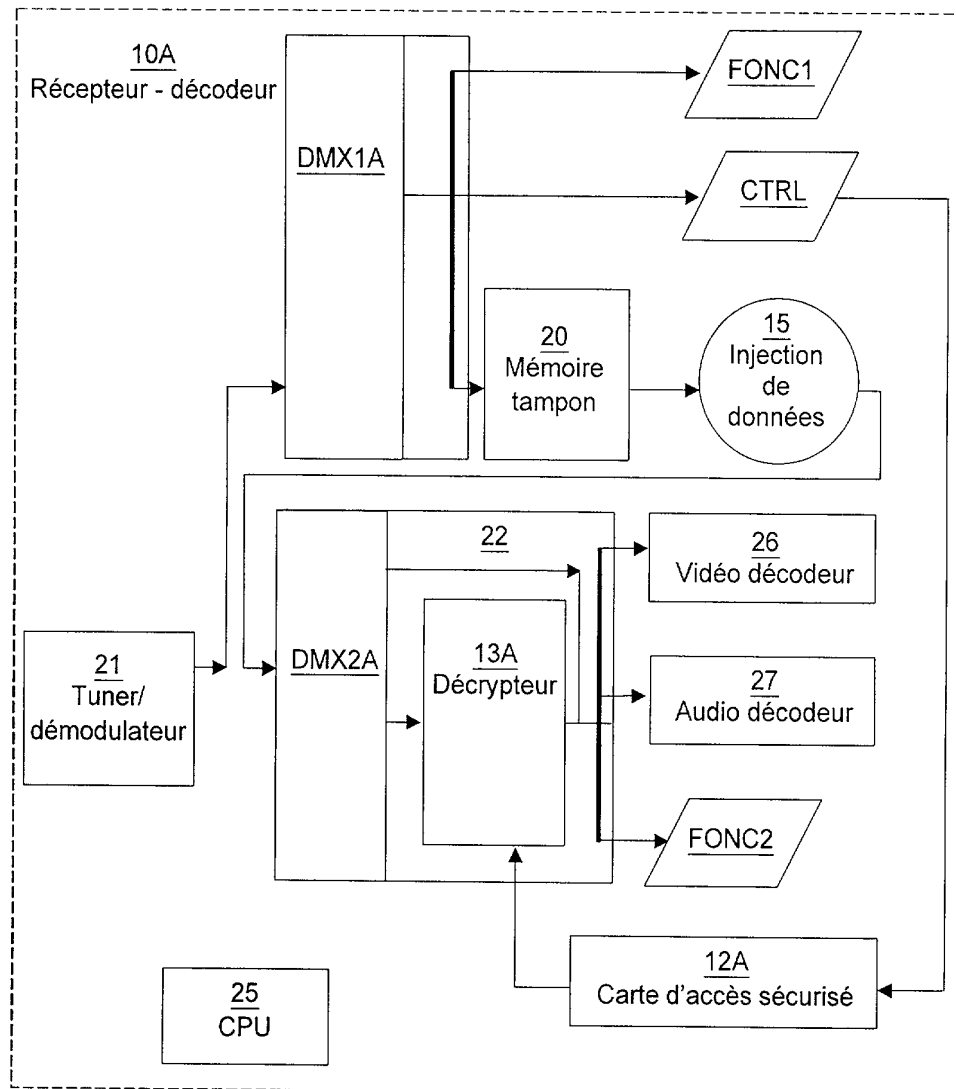


FIG. 5

6/7

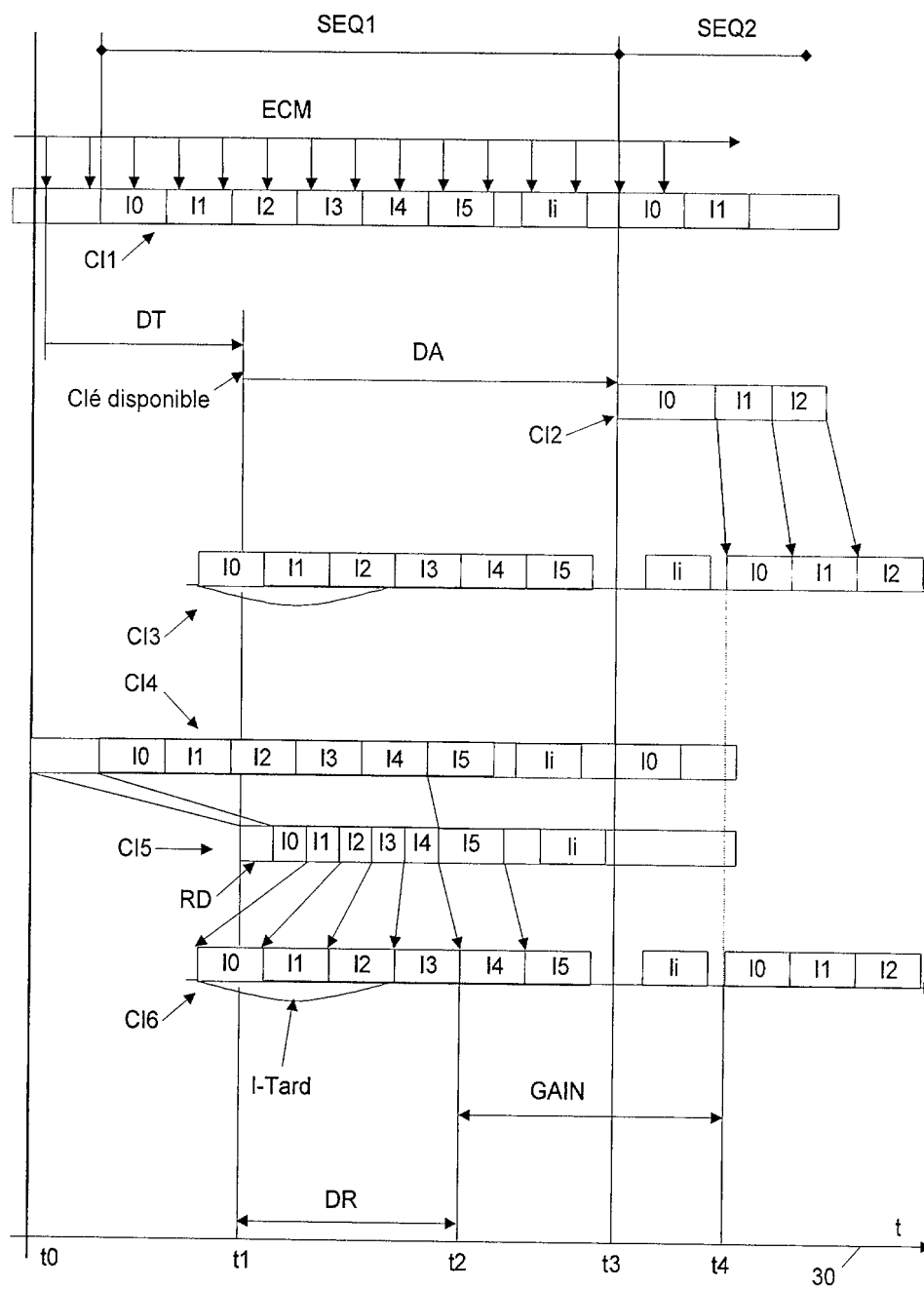


FIG. 6

7/7

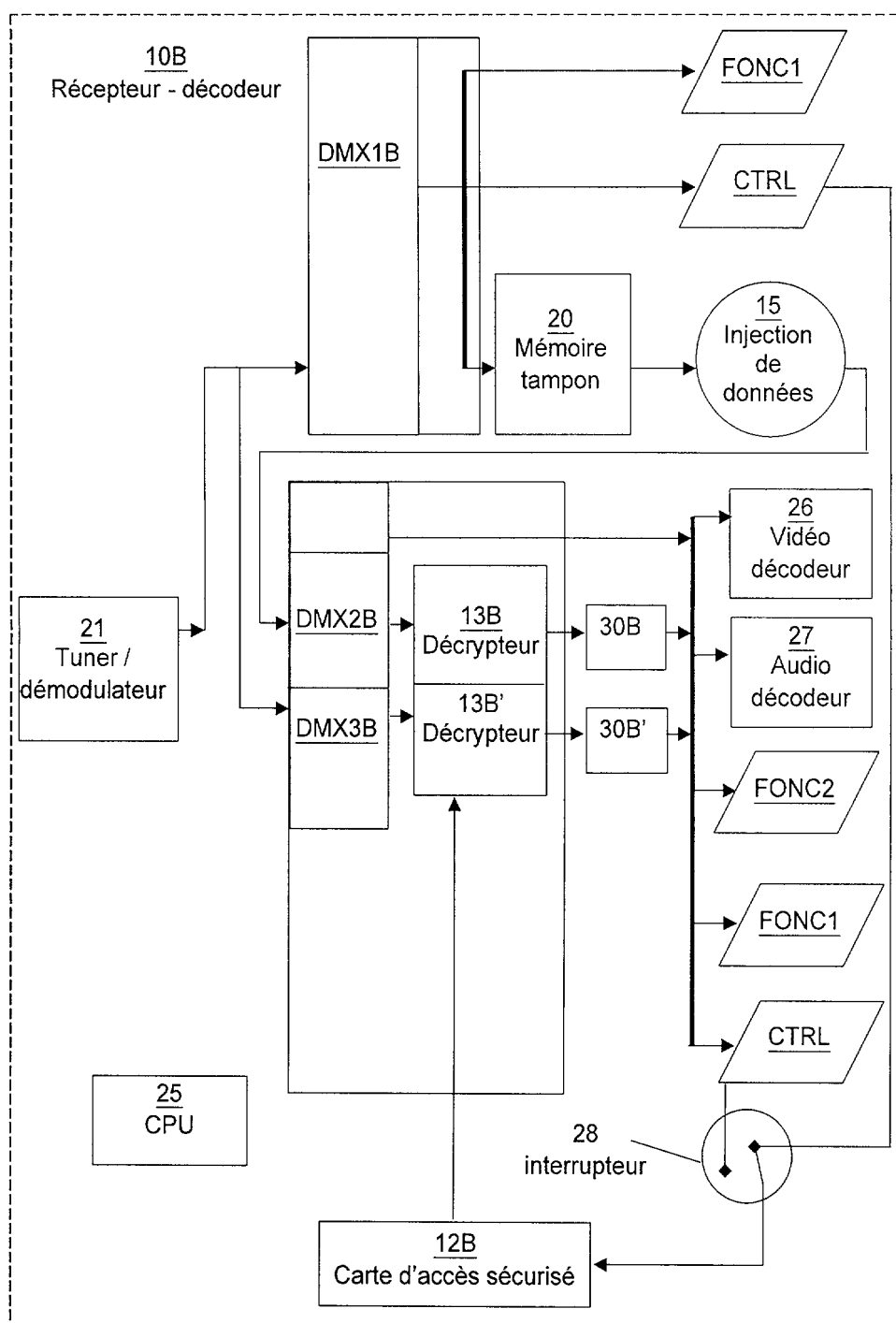


FIG. 7



RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

N° d'enregistrement
national

FA 659022
FR 0451466

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 5 621 794 A (MATSUDA ET AL) 15 avril 1997 (1997-04-15)	1-3,12	H04N7/16
A	* figure 4 *	4-11	

X	EP 1 304 871 A (CANAL+ TECHNOLOGIES SOCIÉTÉ ANONYME) 23 avril 2003 (2003-04-23)	1-3,12	
A	* alinéa [0218] - alinéa [0232] * * figure 16 *	4-11	

X	WO 01/04892 A (SIMOCO INTERNATIONAL LIMITED; MCBIRNIE, STEVEN; RAYNE, MARK, WENTWORTH) 18 janvier 2001 (2001-01-18)	1,12	
A	* abrégé *	2-11	

A,D	US 5 349 641 A (COUTROT ET AL) 20 septembre 1994 (1994-09-20) * le document en entier *	1-12	
-----			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
A	PATENT ABSTRACTS OF JAPAN vol. 2003, no. 12, 5 décembre 2003 (2003-12-05) & JP 2004 128942 A (MITSUBISHI ELECTRIC CORP), 22 avril 2004 (2004-04-22) * abrégé *	1-12	H04N

A	EP 1 107 601 A (THOMSON LICENSING S.A) 13 juin 2001 (2001-06-13) * le document en entier *	1-12	

A	EP 1 389 874 A (MICROSOFT CORPORATION) 18 février 2004 (2004-02-18) * alinéa [0027] - alinéa [0030] * * alinéa [0042] * * alinéa [0058] *	1-12	

-/--			
Date d'achèvement de la recherche		Examineur	
26 mai 2005		Bertrand, F	
CATÉGORIE DES DOCUMENTS CITÉS X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant			



RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

N° d'enregistrement
national

FA 659022
FR 0451466

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	WO 01/72044 A (THOMSON MULTIMEDIA; LEYENDECKER, PHILIPPE; STEYER, JEAM-MARIE) 27 septembre 2001 (2001-09-27) * le document en entier *	1-12	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
A	EP 1 148 720 A (KONINKLIJKE PHILIPS ELECTRONICS N.V) 24 octobre 2001 (2001-10-24) * le document en entier *	1-12	
A	US 6 175 595 B1 (KEESMAN GERRIT J) 16 janvier 2001 (2001-01-16) * le document en entier *	1-12	
A	EP 1 286 349 A (CANAL+ TECHNOLOGIES SOCIETE ANONYME) 26 février 2003 (2003-02-26) * le document en entier *	1-12	
A	WEISS S M: "SWITCHING FACILITIES IN MPEG-2: NECESSARY BUT NOT SUFFICIENT" SMPTE JOURNAL, SMPTE INC. SCARSDALE, N.Y, US, vol. 104, no. 12, décembre 1995 (1995-12), pages 788-802, XP000543847 ISSN: 0036-1682 * le document en entier *	1-12	
A	PATENT ABSTRACTS OF JAPAN vol. 1996, no. 02, 29 février 1996 (1996-02-29) & JP 07 274084 A (TOSHIBA CORP), 20 octobre 1995 (1995-10-20) * le document en entier *	1-12	
-/--			
Date d'achèvement de la recherche		Examineur	
26 mai 2005		Bertrand, F	
CATÉGORIE DES DOCUMENTS CITÉS X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire		T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	

 1
EPO FORM 1503 12.99 (P04C14)



RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

N° d'enregistrement
national

FA 659022
FR 0451466

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	HURST N ET AL: "MPEG SPLICING: A NEW STANDARD FOR TELEVISION - SMPTE 312M" SMPTE JOURNAL, SMPTE INC. SCARSDALE, N.Y, US, vol. 107, no. 11, novembre 1998 (1998-11), pages 978-988, XP000804761 ISSN: 0036-1682 * le document en entier * -----	1,2	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
Date d'achèvement de la recherche		Examineur	
26 mai 2005		Bertrand, F	
CATÉGORIE DES DOCUMENTS CITÉS X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant			

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE**RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0451466 FA 659022**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **26-05-2005**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5621794	A	15-04-1997	JP 2842796 B2	06-01-1999
			JP 8163533 A	21-06-1996
EP 1304871	A	23-04-2003	EP 1286262 A1	26-02-2003
			EP 1304871 A2	23-04-2003
			CN 1572106 A	26-01-2005
			EP 1421781 A2	26-05-2004
			WO 03019931 A2	06-03-2003
			JP 2005501484 T	13-01-2005
			CA 2450417 A1	19-12-2002
			EP 1267572 A2	18-12-2002
			EP 1286537 A2	26-02-2003
			EP 1286349 A1	26-02-2003
			EP 1286549 A2	26-02-2003
			EP 1286351 A2	26-02-2003
			EP 1396151 A2	10-03-2004
			WO 02102082 A2	19-12-2002
			WO 03034742 A1	24-04-2003
			JP 2003235012 A	22-08-2003
			US 2003078930 A1	24-04-2003
WO 0104892	A	18-01-2001	AU 6297000 A	30-01-2001
			WO 0104892 A1	18-01-2001
			GB 2353925 A	07-03-2001
US 5349641	A	20-09-1994	FR 2694860 A1	18-02-1994
			CA 2103935 A1	14-02-1994
			DE 69316478 D1	26-02-1998
			DE 69316478 T2	23-07-1998
			EP 0583202 A1	16-02-1994
JP 2004128942	A	22-04-2004	AUCUN	
EP 1107601	A	13-06-2001	CN 1298259 A	06-06-2001
			EP 1107601 A2	13-06-2001
			JP 2001204035 A	27-07-2001
			MX PA00011721 A	09-07-2002
EP 1389874	A	18-02-2004	US 2004034863 A1	19-02-2004
			CN 1484450 A	24-03-2004
			EP 1389874 A2	18-02-2004
			JP 2004080785 A	11-03-2004
			MX PA03006913 A	19-02-2004
WO 0172044	A	27-09-2001	AU 7389701 A	03-10-2001
			WO 0172044 A1	27-09-2001

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE**RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0451466 FA 659022**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **26-05-2005**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1148720 A	24-10-2001	EP 1148720 A1	24-10-2001
US 6175595 B1	16-01-2001	DE 69608231 D1	15-06-2000
		DE 69608231 T2	30-11-2000
		EP 0783817 A2	16-07-1997
		ES 2148768 T3	16-10-2000
		WO 9704590 A2	06-02-1997
		JP 10505996 T	09-06-1998
		PT 783817 T	31-10-2000
EP 1286349 A	26-02-2003	EP 1286262 A1	26-02-2003
		EP 1286349 A1	26-02-2003
		EP 1286351 A2	26-02-2003
		JP 2003235012 A	22-08-2003
		US 2003078930 A1	24-04-2003
		CA 2450417 A1	19-12-2002
		CN 1572106 A	26-01-2005
		EP 1267572 A2	18-12-2002
		EP 1286537 A2	26-02-2003
		EP 1286549 A2	26-02-2003
		EP 1304871 A2	23-04-2003
		EP 1396151 A2	10-03-2004
		EP 1421781 A2	26-05-2004
		WO 02102082 A2	19-12-2002
		WO 03034742 A1	24-04-2003
		WO 03019931 A2	06-03-2003
		JP 2005501484 T	13-01-2005
JP 07274084 A	20-10-1995	JP 3319648 B2	03-09-2002