(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 825 877**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 07658**

(51) Int Cl[7] : **H 04 N 7/16**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 12.06.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 13.12.02 Bulletin 02/50.

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

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *CANAL + TECHNOLOGIES Société anonyme* — FR.

(72) **Inventeur(s) :** DEROUET ODILE.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** BREVALEX.

(54) PROCEDE DE CONTROLE D'ACCES A UN PROGRAMME CRYPTE.

(57) L'invention concerne un procédé de contrôle d'accès à un programme crypté diffusé par un opérateur à une pluralité de groupes d'abonnés, chaque groupe d'abonné étant muni d'une clé de groupe KG, et chaque abonné étant susceptible de recevoir de l'opérateur une clé d'exploitation KT chiffrée par la clé de groupe KG pour décrypter le programme diffusé.

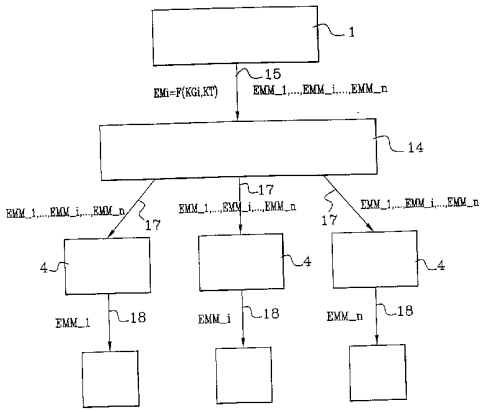
Le procédé selon l'invention comporte en outre les étapes suivantes:

avant la diffusion du programme crypté,

a- associer la clé d'exploitation KT chiffrée à une valeur aléatoire R pour générer un code secret;

b- transmettre le code secret aux abonnés,

b- transmettre la valeur aléatoire R aux abonnés pour calculer la clé d'exploitation KT lorsque le programme crypté est diffusé.



FR 2 825 877 - A1

PROCÉDE DE CONTROLE D'ACCES A UN PROGRAMME CRYPTE

DESCRIPTION

DOMAINE TECHNIQUE

L'invention concerne un procédé de contrôle d'accès à un programme crypté diffusé par un opérateur à une pluralité de groupes d'abonnés, chaque groupe d'abonné étant muni d'une clé de groupe KG, et chaque abonné recevant de l'opérateur, lors de la diffusion du programme crypté, une clé d'exploitation KT chiffrée avec la clé de groupe KG et destinée à décrypter le programme diffusé.

ETAT DE LA TECHNIQUE ANTERIEURE

Dans la norme DVB, les programmes transmis sont cryptés par un mot de contrôle CW qui changent après une période correspondant à sa période de diffusion. Un nouveau mot de contrôle correspondant au même programme ou à un nouveau programme est transmis aux abonnés avec des messages de contrôle d'accès ECM et EMM (respectivement "Entitlement Control Message", et "Entitlement Management Message", en anglais).

Les ECM comportent trois champs, un premier champ contenant les paramètres d'accès qui définissent les conditions d'accès au programme crypté, tels que par exemple le contrôle parental ou la limitation géographique de réception du programme diffusé, un deuxième champ comprenant le mot de contrôle CW chiffré par la clé d'exploitation KT et un troisième champ

contenant les paramètres de contrôle d'intégrité des informations transmises.

Les EMM comportent généralement quatre champs, un premier champ d'adresse pour sélectionner un décodeur individuel, un deuxième champ contenant l'autorisation d'accès de l'utilisateur, un troisième champ contenant la clé d'exploitation KT chiffrée par la clé de groupe KG, et un quatrième champ contenant les paramètres de contrôle de l'intégrité des informations transmises.

Les ECM sont transmis avec le programme crypté tandis que les EMM sont généralement transmis avant la date de diffusion de ces programmes.

Pour un groupe g d'abonnés, le résultat du chiffrement de la clé d'exploitation KT par la clé de groupe KG est fourni avec une EMM chiffrée $EMM_g = F(KT, KG)$ où F désigne un algorithme de chiffrement. Lorsqu'un décodeur reçoit cette EMM, il vérifie si la clé d'exploitation KT est déjà mémorisée, dans une carte à puce par exemple. Sinon, la clé est déchiffrée par la fonction inverse F^{-1} puis stockée dans la carte à puce. Lorsque le programme crypté est diffusé, la clé KT est utilisée par l'algorithme de chiffrement pour déchiffrer le mot de contrôle CW ayant servi à crypter les données du programme diffusé.

La figure 1 représente schématiquement un exemple de dispositif de réception de programmes cryptés diffusés par un opérateur 1. Pour recevoir ces programmes, un abonné dispose d'un récepteur 2, d'un décodeur 4 et d'une carte à puce 6 qui doit être inséré dans le décodeur 4 et dans laquelle est stockée la clé

de groupe KG commune à un groupe de N cartes, N étant égal à 256 par exemple. Un modem 8 connecté à la ligne téléphonique de l'abonné permet d'assurer une voie de retour entre cet abonné et l'opérateur 1. Une antenne 12 reçoit les signaux transmis par l'opérateur 1 et les transmet au décodeur 4.

La figure 2 illustre schématiquement le fonctionnement du dispositif de la figure 1.

L'opérateur 1 envoie à un système de diffusion 14 (flèche 15), une clé d'exploitation KT chiffrée à l'aide de la clé de groupe KG de chaque groupe. Le système de diffusion 14 envoie à chaque décodeur 4 (flèches 17) l'ensemble des $EMM_i = F(KG_i, KT)$. Chaque décodeur 4 transfère à la carte à puce 6 (flèches 18) d'un abonné du groupe g considéré l'EMM_g correspondant à ce groupe. A la réception de l'EMM_g, la carte à puce 6 déchiffre la clé KT au moyen de la clé du groupe KG et mémorise la clé déchiffrée. A la date prévue pour diffuser un programme crypté, l'opérateur diffuse de façon cyclique les ECM_i avec ce programme crypté vers les décodeurs 4. A la réception de ces ECM_i, le décodeur 4 trie les ECM_i correspondant à la clé KT transmise et les envoie à la carte à puce.

Une faiblesse de ce procédé provient du fait que la clé d'exploitation KT est commune à tous les utilisateurs. Par conséquent, il est possible pour un utilisateur qui réussit à retrouver sa clé de groupe KG, de calculer frauduleusement la clé d'exploitation KT et de la diffuser.

Le but de l'invention est de retrouver l'origine d'une diffusion frauduleuse d'une clé d'exploitation KT.

Un autre but de l'invention est de rendre imprévisible pour un fraudeur potentiel, la date à laquelle la clé d'exploitation KT sera utilisée.

Selon un premier mode de réalisation de l'invention, le procédé comporte les étapes suivantes :
avant la diffusion du programme crypté,
a- associer à la clé d'exploitation KT chiffrée une valeur aléatoire R pour générer un code secret ;
b- transmettre ce code secret aux abonnés, et
c- transmettre la valeur aléatoire R aux abonnés pour calculer la clé d'exploitation KT seulement lorsque le programme crypté est diffusé..

Selon l'invention, le code secret est calculé par une fonction arithmétique réversible.

Selon l'invention, la fonction arithmétique réversible est l'opération logique XOR.

Selon l'invention, le code secret calculé est mémorisé dans une carte à puce.

Dans un deuxième mode de réalisation de l'invention dans lequel chaque abonné est susceptible de recevoir de l'opérateur un nombre entier m de clés d'exploitation KT_i pour décrypter un programme diffusé, le procédé comporte les étapes suivantes :
avant la diffusion du programme crypté,
a- associer à chaque clé d'exploitation KT_i chiffrée une valeur aléatoire R_i pour générer un nombre entier r de codes secrets distincts;

b- transmettre ces codes secrets générés à chaque abonné; et

c- transmettre aux abonnés une valeur aléatoire R_i pour calculer une clé d'exploitation KT_i parmi les m clés KT_i seulement lorsque le programme crypté est diffusé, et au bout d'une durée choisie par l'opérateur,

d- transmettre aux abonnés une nouvelle valeur aléatoire R_i pour changer la clé d'exploitation KT_i.

Selon une caractéristique de ce mode de réalisation, les valeurs aléatoires Ri sont transmises successivement aux abonnés à des dates imprévisibles.

Selon l'invention, chaque code secret est calculé par une fonction arithmétique réversible.

Selon l'invention, les codes secrets calculés sont mémorisés dans une carte à puce.

Grâce à l'invention, si un fraudeur veut diffuser publiquement la clé KT avant la diffusion du programme à décrypter, il devra diffuser la valeur de l'EMMg ce qui permettra à l'opérateur de retrouver le groupe auquel appartient le fraudeur.

BREVE DESCRIPTION DES FIGURES

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va suivre, prise à titre d'exemple non limitatif, en référence aux figures annexées dans lesquelles :

- La figure 1 décrite précédemment représente un exemple de dispositif connu de réception de programmes cryptés;

- la figure 2 décrite précédemment illustre schématiquement le fonctionnement du dispositif de la figure 1;

La figure 3 illustre schématiquement un premier mode de réalisation du procédé de l'invention;

- la figure 4 illustre schématiquement un deuxième mode de réalisation du procédé de l'invention.

DESCRIPTION DETAILLEE DE MODE DE MISE EN ŒUVRE DE L'INVENTION

Dans la suite de la description, des références identiques désigneront les éléments et les étapes communs au procédé de l'art antérieur et au procédé selon l'invention.

En référence à la figure 3, un opérateur 1 associe une valeur aléatoire R à une clé d'exploitation KT et envoie à un système de diffusion 14 (flèche 15) le code secret résultant de cette association. Préférentiellement, la clé d'exploitation KT chiffrée à l'aide de la clé de groupe KG est combinée par l'opération logique XOR à la valeur aléatoire secrète R. Le code généré ne pourra être déchiffré que si la valeur R est dévoilée. Le système de diffusion 14 envoie ensuite à chaque décodeur 4 (flèches 17) d'un groupe i, i représentant le rang d'un groupe d'abonnés parmi n groupes distincts, une EMM calculée par l'expression :

$EMM_i = F(KG_i, KT) + R$.

Chaque décodeur 4 transfère à la carte à puce 6 (flèche 18) l'EMM_i correspondant au groupe i. A la date de diffusion du programme crypté, l'opérateur diffuse

de façon cyclique les ECM avec ce programme vers les décodeurs 4. Ces ECM contiennent le mot de contrôle CW utilisés pour crypter les données du programme transmis. Le décodeur 4 trie les ECM_i correspondant à la clé KT et les envoie à la carte à puce 6 qui mémorise le code secret généré. Tant que l'opérateur n'pas diffusé la valeur R, la carte à puce ne pourra pas déchiffrer ce code secret pour retrouver la clé d'exploitation KT. Ceci permet à l'opérateur de diffuser la valeur R le plus tard possible, c'est à dire, uniquement lorsque la clé d'exploitation KT doit être utilisée pour déchiffrer le mot de contrôle CW.

Dès que la clé KT est utilisée, l'opérateur envoie aux décodeurs 4 la valeur:

$ECM = R \oplus F(EMMg \oplus R, KG)$.

L'algorithme hébergé par la carte à puce pourra alors calculer la valeur de la clé d'exploitation KT en utilisant l'opération :

$KT = F^{-1}(EMM_g \oplus R, KG)$;

Le mot de contrôle peut ensuite être déduit par l'expression :

$CW = F^{-1}(ECM, KT)$.

Si un fraudeur veut diffuser publiquement la clé KT avant le début de la diffusion du programme crypté, il devra diffuser la valeur EMM_g qui dépend de la clé de groupe KG. L'opérateur sera en mesure de retrouver le groupe auquel appartient le fraudeur et retirer les droits d'accès à ce groupe.

Ce mode de réalisation dissuade par conséquent le fraudeur de diffuser les clés d'exploitation KT lors de la réception des EMM.

Cependant, lorsque la valeur R est dévoilée par l'opérateur, la valeur de la clé d'exploitation KT peut être recalculée et diffusée publiquement.

Aussi, pour empêcher cette diffusion, ou du moins la rendre fastidieuse, selon un deuxième mode de réalisation de l'invention illustré par la figure 4, avant la diffusion du programme crypté, l'opérateur 1 envoie au système de diffusion 14 (flèche 15), un nombre entier m de clés d'exploitation KT_1, $KT_2 \ldots KT_i \ldots KT_m$. Chaque clé KT_i est chiffrée à l'aide de la clé de groupe KG du groupe i et est associée par l'opération logique XOR à une valeur aléatoire secrète R_i connue uniquement par l'opérateur de manière à générer un code secret qui ne pourra être déchiffré que si la valeur R_i est dévoilée.

Le système de diffusion 14 envoie à chaque décodeur 4 (flèches 17) l'ensemble des EMM calculés par l'expression :

$EMM_i = F(KG_i, KT_1) \oplus R_1 \| F(KG_i, KT_2) \oplus R_2 \| \ldots F(KG_i, KT_i) \oplus R_i \| \ldots\ldots F(KG_i, KT_m) \oplus R_m \|$.

où le symbole $\|$ représente l'opération de concaténation.

Le décodeur 4 du groupe i transfère à la carte à puce 6 (flèche 18) l'EMM_i correspondant à ce groupe. A la date de diffusion du programme crypté, l'opérateur diffuse de façon cyclique les ECM avec le programme crypté vers les décodeurs 4. Ces ECM contiennent le mot de contrôle CW utilisés pour crypter les données du programme transmis. Le décodeur 4 trie les ECM_i correspondant à la clé KT_i et les envoie à la carte à puce 6 qui mémorise le code secret généré. Tant que

l'opérateur n' pas diffusé une valeur R_i, la carte à puce ne pourra pas déchiffrer ce code secret pour retrouver la clé d'exploitation KT_i. Chaque clé KT_i demeure donc stockée dans la carte à puce 6.

Les valeurs R_i sont diffusées via les ECM en fonction de la clé ayant servi à chiffrer les mots de contrôle.

Dès que la clé KT_i est utilisée, l'opérateur envoie aux décodeur 4 l'ECM:

$$ECM = R_i \parallel F(CW, KT_i)$$

Ce mode de réalisation permet d'affecter aux différentes clés d'exploitation KT_i une période de validité suffisamment courte et imprévisible pour rendre la diffusion frauduleuse d'une clé KT_i fastidieuse après que la valeur R_i a été dévoilée.

Grâce à ce deuxième mode de réalisation, l'opérateur peut changer la clé KT_i de façon imprévisible en fonction de l'intérêt des programmes diffusés.

REVENDICATIONS

1. Procédé de contrôle d'accès à un programme crypté diffusé par un opérateur (1) à une pluralité de groupes d'abonnés, chaque groupe d'abonnés étant muni d'une clé de groupe KG, et chaque abonné étant susceptible de recevoir de l'opérateur (1) une clé d'exploitation KT chiffrée par la clé de groupe KG pour décrypter le programme diffusé, procédé caractérisé en ce qu'il comporte en outre les étapes suivantes :
avant la diffusion du programme crypté,
a- associer à la clé d'exploitation KT chiffrée une valeur aléatoire R pour générer un code secret ;
b- transmettre le code secret aux abonnés, et
c- transmettre la valeur aléatoire R aux abonnés pour calculer la clé d'exploitation KT seulement lorsque le programme crypté est diffusé.

2. Procédé selon la revendication 1, caractérisé en ce que le code secret est calculé par une fonction arithmétique réversible.

3. Procédé selon la revendication 2, caractérisé en ce que la fonction arithmétique réversible est l'opération logique XOR.

4. Procédé selon la revendication 1, caractérisé en ce que le code secret généré est mémorisé dans une carte à puce.

5. Procédé de contrôle d'accès à un programme crypté diffusé par un opérateur (1) à une pluralité de groupes d'abonnés, chaque groupe d'abonnés étant muni d'une clé de groupe KG, et chaque abonné étant susceptible de recevoir de l'opérateur (1) un nombre

entier m de clés d'exploitation KT_i pour décrypter le programme diffusé,

procédé caractérisé en ce qu'il comporte les étapes suivantes:

avant la diffusion du programme crypté,

a- associer à chaque clé d'exploitation KT_i chiffrée une valeur aléatoire R_i pour générer un nombre entier m de codes secrets distincts;

b- transmettre les codes secrets générés à chaque abonné;

c- transmettre aux abonnés une valeur aléatoire R_i pour calculer une clé d'exploitation KT_i parmi les m clés KT_i seulement lorsque le programme crypté est diffusé, et pendant la période de diffusion du programme crypté,

d- transmettre aux abonnés une nouvelle valeur aléatoire R_i pour changer la clé d'exploitation KT_i.

6. Procédé selon la revendication 5, caractérisé en ce que les valeurs aléatoires Ri sont transmises successivement aux abonnés à des dates imprévisibles.

7. Procédé selon la revendication 6, caractérisé en ce que chaque code secret est calculé par une fonction arithmétique réversible.

8. Procédé selon la revendication 7, caractérisé en ce que la fonction arithmétique réversible est l'opération logique XOR.

9. Procédé selon la revendication 6, caractérisé en ce que tant qu'une clé KT_i n'est pas utilisée, la valeur aléatoire R_i n'est pas transmise.

10. Procédé selon la revendications 7, caractérisé en ce que chaque code secret est mémorisé dans une carte à puce (6).

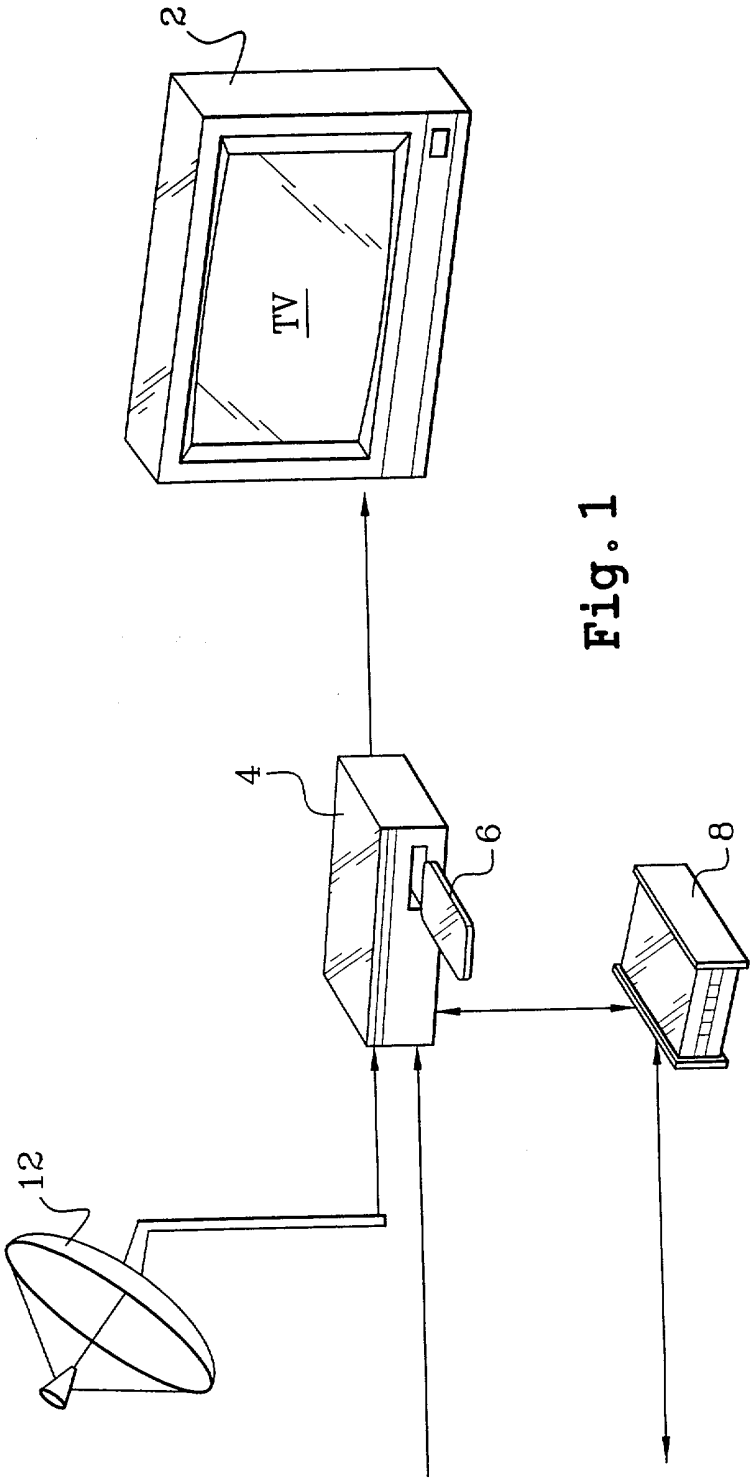


Fig. 1

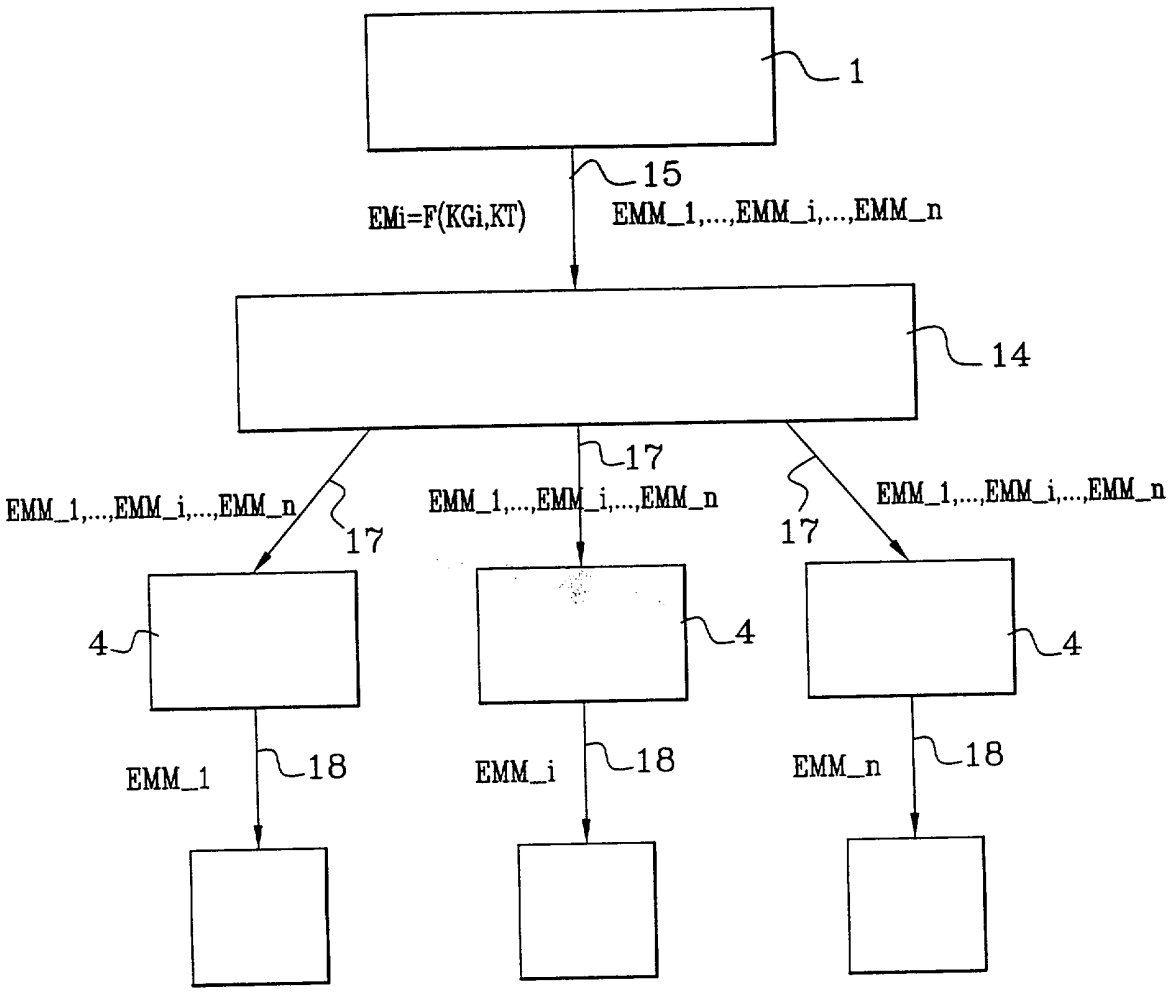

1
15
EMi=F(KGi,KT)
EMM_1,...,EMM_i,...,EMM_n
14
17
EMM_1,...,EMM_i,...,EMM_n
17
EMM_1,...,EMM_i,...,EMM_n
17
EMM_1,...,EMM_i,...,EMM_n
4
4
4
EMM_1
18
EMM_i
18
EMM_n
18

Fig. 2

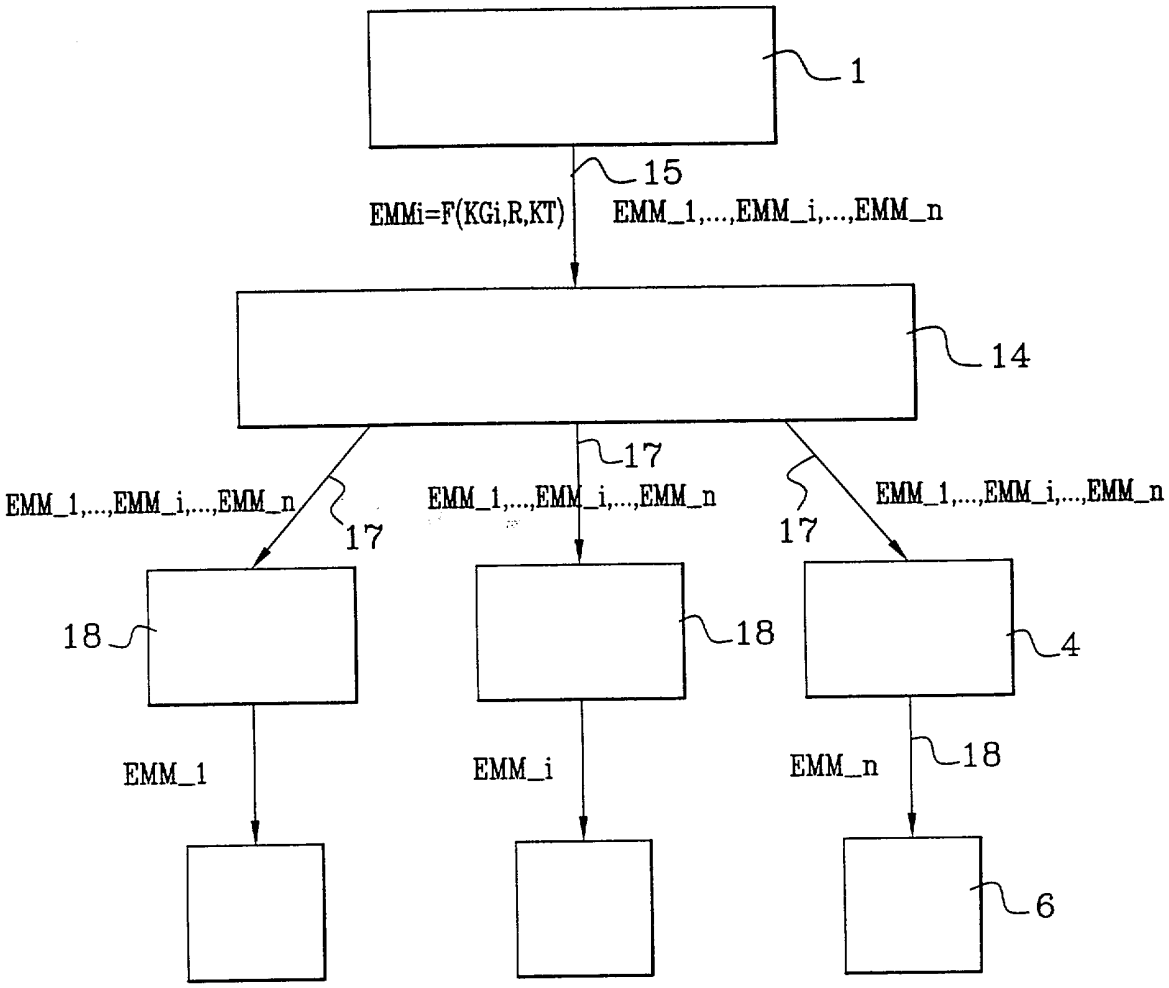

1
15
EMMi=F(KGi,R,KT)
EMM_1,...,EMM_i,...,EMM_n
14
17
EMM_1,...,EMM_i,...,EMM_n
17
EMM_1,...,EMM_i,...,EMM_n
17
EMM_1,...,EMM_i,...,EMM_n
18
18
4
EMM_1
EMM_i
EMM_n
18
6

Fig. 3

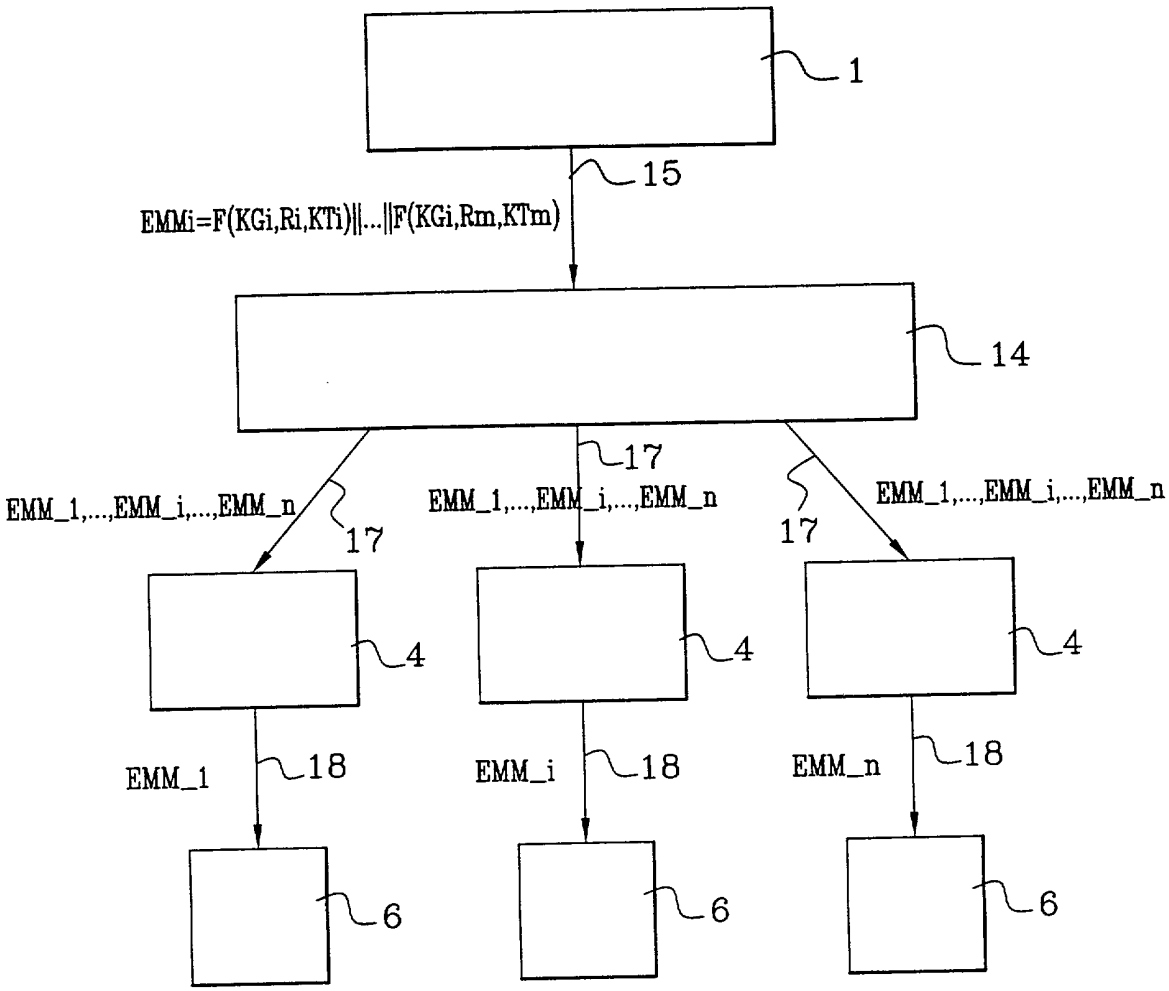

1
15
EMMi=F(KGi,Ri,KTi)||...||F(KGi,Rm,KTm)
14
17
EMM_1,...,EMM_i,...,EMM_n
17
EMM_1,...,EMM_i,...,EMM_n
17
EMM_1,...,EMM_i,...,EMM_n
4
4
4
EMM_1
18
EMM_i
18
EMM_n
18
6
6
6

Fig. 4

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2825877

N° d'enregistrement national

FA 603340
FR 0107658

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

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	EP 1 051 036 A (LUCENT TECHNOLOGIES INC) 8 novembre 2000 (2000-11-08) * page 4, ligne 23 - page 8, ligne 58 *	1-10	H04N7/16
A	WO 99 09743 A (SCIENTIFIC ATLANTA) 25 février 1999 (1999-02-25) * page 10, ligne 1 - page 19, ligne 24 * * page 22, ligne 22 - page 23, ligne 19 * * page 33, ligne 1 - ligne 23 * * page 76, ligne 17 - page 77, ligne 2 * * figures 1-6 *	1-10	
A	US 6 055 314 A (SPIES, TERRENCE R ET AL) 25 avril 2000 (2000-04-25) * colonne 9, ligne 52 - colonne 13, ligne 52 * * figures 4-8 *	1-10	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			H04N

Date d'achèvement de la recherche	Examinateur
20 février 2002	Van der Zaal, R

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

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0107658 FA 603340

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 20-02-2002
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 1051036	A	08-11-2000	AU	3024400 A	09-11-2000
			BR	0007333 A	07-08-2001
			CN	1273490 A	15-11-2000
			EP	1051036 A2	08-11-2000
			JP	2001036517 A	09-02-2001
WO 9909743	A	25-02-1999	US	6157719 A	05-12-2000
			AU	1581699 A	08-03-1999
			AU	8670598 A	22-02-1999
			AU	8679798 A	22-02-1999
			AU	8679898 A	22-02-1999
			AU	8764298 A	22-02-1999
			AU	8823398 A	22-02-1999
			AU	8823698 A	22-02-1999
			BR	9810966 A	20-11-2001
			BR	9810967 A	30-10-2001
			BR	9815606 A	22-01-2002
			BR	9815607 A	13-11-2001
			DE	69802288 D1	06-12-2001
			DE	69802540 D1	20-12-2001
			EP	1010323 A1	21-06-2000
			EP	1010324 A1	21-06-2000
			EP	1010325 A1	21-06-2000
			EP	1013091 A1	28-06-2000
			EP	1000508 A1	17-05-2000
			EP	1000509 A1	17-05-2000
			EP	1000511 A2	17-05-2000
			JP	2001513587 T	04-09-2001
			JP	2001512842 T	28-08-2001
			WO	9907145 A1	11-02-1999
			WO	9907146 A1	11-02-1999
			WO	9907147 A1	11-02-1999
			WO	9907148 A1	11-02-1999
			WO	9907149 A1	11-02-1999
			WO	9909743 A2	25-02-1999
			WO	9907150 A1	11-02-1999
			US	6105134 A	15-08-2000
			US	6292568 B1	18-09-2001
			US	6252964 B1	26-06-2001
			US	2001001014 A1	10-05-2001
			US	2001046299 A1	29-11-2001
			US	2001053226 A1	20-12-2001
US 6055314	A	25-04-2000	AUCUN		

EPO FORM P0465