(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 835 670**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 16585**

(51) Int Cl[7] : **H 04 L 9/18,** H 04 N 7/16 // G 06 K 19/07

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 20.12.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 08.08.03 Bulletin 03/32.

(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) :** *CP8 Société anonyme* — FR.

(72) **Inventeur(s) :** COURTOIS NICOLAS et PATARIN JACQUES.

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

(74) **Mandataire(s) :**

(54) PROCEDE DE DISTRIBUTION ANTI-PIRATAGE D'UN CONTENU NUMERIQUE PAR TRANSMISSION DIVERSIFIEE PRO-ACTIVE, DISPOSITIF EMETTEUR ET OBJET PORTATIF RECEPTEUR ASSOCIES.

(57) L'invention conceme un procédé de distribution anti-piratage d'un

contenu numérique par transmission diversifiée pro-active, un dispositif émetteur et un objet portatif récepteur associés.

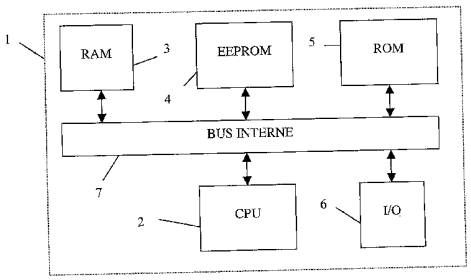
Le procédé, prévu pour mettre une même information (K_c) à disposition de plusieurs récepteurs (1) appartenant à un ensemble (G) de récepteurs, chaque récepteur stockant une information (SA_i) qui lui est propre, est caractérisé en ce qu'il consiste à:

-définir une relation $K_c = f(K, b_i, SA_i)$ où (f) est une fonction déterminée, (K) est une information commune à tous les récepteurs, et (b_i) est une information différente pour chaque récepteur et pour chaque valeur de l'information (K);

-donner à chaque récepteur, avant la mise à disposition de (K_c), accès à l'information (b_i); et

-transmettre l'information (K) à tous les récepteurs, juste avant la mise à disposition de (K_c);

de sorte que chaque récepteur peut calculer l'information (Ko) au moyen de ladite relation.



FR 2 835 670 - A1

Procédé de distribution anti-piratage d'un contenu numérique par transmission diversifiée pro-active, dispositif émetteur et objet portatif récepteur associés.

Actuellement de nombreuses chaînes de télévision payantes sont victimes de fraudes. En particulier on trouve souvent des cartes pirates qui permettent de visualiser leurs chaînes. La présente invention propose un nouveau système de transmission des clés de déchiffrement de l'image (ou de l'image elle-même) qui présente de nombreux avantages : le système est relativement simple à mettre en œuvre, et il permet de réagir rapidement en cas d'apparition de cartes pirates (flexibilité).

Si l'on obtient une carte pirate, on pourra de l'extérieur (c'est-à-dire juste en observant son fonctionnement) savoir de quels secrets elle dispose, ce qui permettra éventuellement de savoir de quelle vraie carte elle a obtenu ces secrets, mais surtout d'invalider rapidement toutes les cartes pirates sans invalider les cartes légitimes. En anglais, on parle de « traitor tracing » et en particulier de « black box (traitor) tracing ». Notons que l'invention proposée a de très bonnes propriétés d'efficacité et de sécurité par rapport aux autres systèmes proposés dans la littérature cryptographique (cf. les références). Notons aussi que cette invention ne se limite pas à la télévision : le procédé peut aussi être utilisé à chaque fois que l'on souhaite transmettre un même contenu à plusieurs récepteurs autorisés.

Le nouveau procédé est caractérisé par des débits très raisonnables qui sont compatibles avec les limitations de débit imposées par les canaux de communication. De plus, il se distingue des autres procédés par la très faible longueur de la donnée K qui est transmise en temps réel pour permettre d'accéder au contenu protégé : cette longueur peut être aussi courte que 64 bits.

L'invention concerne à cet effet un procédé pour mettre une même information (K_c) à disposition de plusieurs récepteurs appartenant à un ensemble (G) de récepteurs, chaque récepteur stockant une information (SA_i) qui lui est propre, caractérisé en ce qu'il comprend les étapes consistant à :

-définir une relation $K_c=f(K, b_i, SA_i)$ où (f) est une fonction déterminée, (K) est une information commune à tous les récepteurs, et (b_i) est une information différente pour chaque récepteur et pour chaque valeur de l'information (K) ;

-donner à chaque récepteur, avant la mise à disposition de (K_c), accès à l'information (b_i) ; et

-transmettre l'information (K) à tous les récepteurs, juste avant la mise à disposition de (K_c) ;

de sorte que chaque récepteur peut calculer l'information (K_c) au moyen de ladite relation.

Avantageusement, la fonction (f) est telle qu'à partir de la connaissance d'un (b_i) et d'un (SA_i), on ne connaît pas d'algorithme qui permette d'obtenir l'information (K_c) en un temps réaliste et avec une probabilité non négligeable, lorsqu'on ne connaît pas l'information (K).

Avantageusement, la fonction f est telle qu'à partir de la connaissance d'un certain nombre de ($b_1..b_n$) pour un certain sous-ensemble (G') de récepteurs, on ne connaît pas d'algorithme qui permette, avant de connaître K actuelle, en un temps réaliste et avec une probabilité non négligeable, de produire un couple (b_i, SA_i) valide avec un (SA_i) légitime, i n'étant pas un des récepteurs 1..n de (G').

Avantageusement, la fonction f est de la forme :

$$f(K, b_i, SA_i) = b_i \oplus E_K(SA_i)$$

où E_K est une fonction dépendant de l'information (K) et où $\oplus$ désigne une loi de groupe.

Avantageusement, la fonction (E_K) est une fonction de chiffrement cryptographique, et (K) une clé secrète utilisée par cette fonction.

Avantageusement, les valeurs (b_i) sont envoyées chiffrées avec une clé (K_i) spécifique à chaque récepteur d'un certain ensemble (G) de récepteurs.

Avantageusement, chaque valeur (SA_i) est une valeur secrète connue du récepteur d'indice i.

Avantageusement, chaque (b_i) est constitué de deux valeurs b_{1i} et b_{2j}, et de même l'information propre de chaque récepteur est constituée de deux valeurs SA_i et SA_j, de sorte que chaque récepteur, identifié par le couple d'indices (i,j), combine les valeurs b_{1i} et b_{2j} correspondantes avec les valeurs SA_i et SA_j pour calculer des valeurs K_{c1} et K_{c2} au moyen de ladite relation, qui à leur tour sont combinées pour accéder à l'information K_C.

Avantageusement, l'information K_c est une clé permettant de déchiffrer un contenu numérique tel qu'une image de télévision..

Avantageusement, l'information K_c est utilisable pendant quelques minutes par les récepteurs, l'information K est envoyée quelques secondes en avance, et les b_i sont envoyés régulièrement en commençant plusieurs jours à l'avance.

Avantageusement, certains récepteurs trouvent au moins une partie de leurs valeurs b_i dans une liste de valeurs pré-stockées dans les récepteurs.

L'invention concerne aussi un objet portatif récepteur appartenant à un ensemble (G) d'objets portatifs, et comprenant des moyens de traitement

d'information et des moyens de mémorisation d'information, les moyens de mémorisation stockant une information (SA_i) qui est propre à l'objet portatif et une fonction (f) déterminée, caractérisé en ce qu'il comprend :

-des moyens pour avoir accès à une information (b_i) différente pour chaque objet portatif de l'ensemble (G) et pour chaque valeur de l'information (K) ; et

-des moyens pour calculer une information (K_c) au moyen d'une relation K_c= f(K, b_i, SA_i) où K est une information commune à tous les objets portatifs et transmise à ceux-ci.

L'invention concerne enfin un dispositif émetteur pour mettre une même information (K_c) à disposition de plusieurs récepteurs appartenant à un ensemble (G) de récepteurs, chaque récepteur stockant une information (SA_i) qui lui est propre, caractérisé en ce qu'il comprend :

-des moyens de calcul agencés pour calculer une information (b_i) à partir d'une relation K_c=f(K, b_i, SA_i) où (f) est une fonction déterminée, (K) est une information commune à tous les récepteurs, et l'information (b_i) est une information différente pour chaque récepteur et pour chaque valeur de l'information (K) ; et

-des moyens de transmission agencés pour transmettre à chaque récepteur, un certain temps avant la mise à disposition de (K_c), l'information (b_i) qui lui est associée, et pour transmettre l'information (K) à tous les récepteurs, juste avant la mise à disposition de (K_c).

D'autres détails et avantages de la présente invention apparaîtront au cours de la description suivante d'un mode d'exécution préféré mais non limitatif, en regard des dessins annexés sur lesquels :

La figure 1 représente un récepteur sous la forme d'un objet portatif du type carte à puce ; et

La figure 2 représente un dispositif émetteur associé.

1 Exemple de système

1.1 Description

Considérons un système de distribution d'une même information à de nombreux récepteurs valides. Par exemple, il peut s'agir d'un système de télévision payante. Notons K_c la clé de déchiffrement de l'information. Cette clé a par exemple une durée de vie de 10 minutes et peut avoir entre 64 et 128 bits. Nous allons décrire un procédé qui va permettre aux récepteurs de recalculer toutes les 10 minutes la nouvelle valeur de K_c. Notons qu'ici tous les récepteurs vont calculer une même valeur de K_c, alors qu'ils auront tous des secrets différents.

Considérons un récepteur, et appelons-le « récepteur d'indice i ». Ce récepteur possède ici au moins deux valeurs qui lui sont propres : une clé de chiffrement K_i, et une valeur secrète SA_i.

L'organisme chargé de la transmission va générer une clé secrète K, puis va calculer, pour tous les indices i, la valeur suivante :

$$b_i = K_c \oplus E_K(SA_i),$$

où E désigne une fonction de chiffrement, ou plus généralement une fonction à sens unique, utilisant la clé K, et où $\oplus$ désigne une loi de groupe (par exemple le XOR bit par bit, ou l'addition modulo 256), et il va transmettre toutes ces valeurs b_i , chiffrées respectivement avec une clé K_i. Par exemple, il va régulièrement transmettre toutes les valeurs b_i plusieurs jours à l'avance.

Ainsi, un récepteur qui sera en mode réception sera capable, plusieurs jours à l'avance, de déchiffrer la valeur b_i (au moyen de sa clé K_i).

Puis, quelques secondes seulement avant que la clé K_c devienne utile, l'émetteur va envoyer la clé secrète K à tous les récepteurs. Cette clef peut être très courte, par exemple 64 bits. Dès lors, ceux-ci vont être capables de calculer K_c en calculant $y = E_K(SA_i)$, puis $K_c = b_i \oplus y^{-1}$ (si l'opération de groupe est le XOR bit par bit, alors $y^{-1}=y$).

Notons que le facteur « temps » joue ici un rôle très important : avant l'émission de K, aucun des récepteurs ne peut calculer la valeur de K_c, et ils ont tous en mémoire des valeurs b_i et SA_i différentes. Puis, dès l'émission de K, ils vont tous, à partir de cette même et unique valeur K et de leurs valeurs différentes SA_i et b_i, pouvoir recalculer la même valeur K_c.

On rappelle qu'une fonction à sens unique est une fonction qui peut être calculée dans un sens sans information particulière, mais qui ne peut pas être calculée de façon inverse, sauf éventuellement si l'on connaît certains paramètres. Il s'agit notamment d'une fonction de hachage telle que MD5 ou SHA.

1.2 « Black Box Traitor Tracing », ou comment réagir en cas d'apparition de cartes pirates

Si des cartes pirates apparaissent, il est possible de réagir : d'une part en détectant le (ou les) secrets qui sont dans la carte (voir ci-dessous), ensuite en invalidant toutes les cartes qui possèdent ce (ces) mêmes secrets (voir ci-dessous). Et ceci sans changer les autres cartes en circulation, qui vont continuer à fonctionner.

1.3 Détection du (ou des) secrets

Supposons tout d'abord que les secrets d'un seul vrai récepteur se trouvent dans une carte pirate. On va séparer les cartes valides en deux ensembles

ayant approximativement le même nombre d'éléments : A et B. Puis, on transmet à la carte pirate les vrais b_i pour A et des faux b_i pour B, et on observe si elle est encore capable de déchiffrer les images correctement. Si oui, son secret appartient à A, sinon à B. On recommence ensuite avec deux nouveaux sous-ensembles. Ainsi, s'il y a environ 2^n indices i possibles, en environ n essais on va trouver de quel indice il s'agit.

Notons qu'il n'est pas nécessaire d'aller lire les secrets contenus dans la carte : il suffit d'observer son fonctionnement. Si plusieurs secrets sont présents dans une même carte, le procédé indiqué permet de détecter un 1^{er} secret. Puis, on n'envoie plus les b_i correspondant à ce secret, et on détecte un $2^{ème}$ secret, etc. On peut aussi imaginer que la carte pirate possède les secrets de plusieurs vrais récepteurs et qu'elle utilise ces secrets de façon complexe : la détection devient alors plus difficile mais reste en général possible tant que le nombre de secrets contenus dans la carte pirate n'est pas trop grand.

1.3.1 Invalidation des cartes ayant ce (ces) secret(s)

Il suffit de ne plus transmettre les b_i correspondant à ces secrets.

2 Le schéma général de base

On va résumer le principe de base qui est le cœur de l'invention, dans toute sa généralité, et dans les chapitres suivants on va décrire des améliorations, variantes, et versions plus générales qui en sont dérivées.

Soit G un ensemble de récepteurs légitimes. Le but est de leur transmettre (et seulement à eux) un contenu K_c, consistant en toute sorte d'information (données, programme, clef cryptographique, etc...), notamment un contenu numérique. Le contenu K_c peut notamment être une clef pour accéder à un

programme de télévision payante. Le contenu K_c est identique pour tous les récepteurs et, typiquement, il va changer très rapidement pour éviter sa redistribution frauduleuse.

Le principe de base de l'invention est de transmettre K_c à tous les récepteurs légitimes par le moyen d'une autre clef K envoyée en clair, de sorte que chaque récepteur connaisse un moyen de calculer K_c à partir de K, qui soit complètement différent de celui utilisé par les autres récepteurs.

Ce moyen sera typiquement une valeur b_i, envoyée longtemps à l'avance, qu'il retrouve dans sa mémoire. Juste avant que K_c doive être mise à disposition des récepteurs, on envoie une unique valeur K à tous les récepteurs de l'ensemble G, de telle sorte que chaque récepteur peut calculer K_c au moyen d'une fonction f qu'il détient et qui prend en entrée K, b_i, et une valeur SA_i qui lui est propre. Pour tout indice i du groupe de récepteurs, on a donc :

$$K_c = f(K, b_i, SA_i).$$

Le moment où K devra être envoyée aux récepteurs sera à apprécier en fonction des circonstances, de façon à assurer qu'un fraudeur ne soit pas capable, dans le délai séparant l'envoi de K et la mise à disposition de K_c , de recalculer K_c , ou tout du moins d'en faire un usage frauduleux. Typiquement, K sera envoyée quelques secondes ou quelques minutes avant la mise à disposition de K_c.

2.1 Variantes du schéma de base

Variante 1

Pour certaines applications, il n'est pas nécessaire que les valeurs SA_i soient secrètes : elles peuvent être publiques.

Variante 2

Pour certaines applications, lorsque les valeurs SA_i sont secrètes, on peut envoyer les valeurs b_i en clair aux récepteurs.

Variante 3

La fonction E, au lieu d'être une fonction de chiffrement, peut plus généralement être une fonction à sens unique utilisant une clé K, par exemple une fonction de hachage cryptographique telle que SHA-1.

Variante 4 - Pré-stockage de valeurs b_i

Plutôt que d'envoyer des valeurs b_i, il est possible de les avoir pré-calculées et pré-stockées chez le récepteur, par exemple en mémoire flash, sur le disque dur, sur un CD-ROM, ou sur un DVD. On peut également les diffuser localement, par exemple par le câble de l'immeuble ou par les ondes hertziennes.

3 Le schéma généralisé.

Le schéma décrit plus haut avec ces variantes peut être dupliqué ou démultiplié, ce qui apporte des gains considérables en termes de performances et détection de coalitions des fraudeurs. D'abord, nous allons décrire une version dupliquée, pour enfin expliquer le principe général qui permet d'utiliser le schéma plusieurs fois en parallèle et tous les bénéfices qui en découlent.

3.1 2ème exemple de système

Ici, chaque récepteur possède, à la place de la valeur SA_i qui lui était propre, deux valeurs SA_i et SA_j , de sorte que plusieurs récepteurs peuvent avoir le même SA_i ou le même SA_j, mais pas simultanément le même SA_i et le même SA_j. Ainsi chaque récepteur est caractérisé par un couple d'indices (i, j) qui lui est propre.

De plus, chaque récepteur peut posséder deux clés de déchiffrement K_i et K_j, de sorte que plusieurs récepteurs peuvent avoir le même K_i ou le même K_j, mais pas simultanément le même K_i et le même K_j. Les K_i peuvent servir à transmettre les b_i aux récepteurs de façon secrète (sauf dans la variante où les b_i sont publics).

L'organisme chargé des transmissions va générer deux valeurs secrètes K_{c1} et K_{c2}. Ensuite, elles sont combinées pour accéder à la clef principale K_c ou pour accéder directement au contenu. Par exemple, on peut avoir :
$K_c = K_{c1} \# K_{c2}$, où # est une loi de groupe.

Puis il génère une clé K et il calcule tous les

$$b_{1i} = K_{c1} \oplus E_K(SA_i)$$

et $$b_{2j} = K_{c2} \oplus E_K(SA_j)$$

où E désigne une fonction de chiffrement, ou plus généralement une fonction à sens unique, utilisant la clé K, et où $\oplus$ désigne une loi de groupe, et il va transmettre tous ces b_{1i} chiffrés avec la clé K_{1i} et tous les b_{2j} chiffrés avec la clé K_j. Par exemple, il va régulièrement transmettre tous les b_{1i} et b_{2j} plusieurs jours à l'avance.

Ainsi un récepteur qui sera en mode réception sera capable plusieurs jours à l'avance de déchiffrer la valeur b_{1i} (au moyen de sa clé K_i) et la valeur b_{2j} (au moyen de sa clé K_j).

Puis, quelques secondes seulement avant que la clé K_c devienne utile, l'émetteur va envoyer la clé secrète K à tous les récepteurs. Dès lors, ceux-ci vont être capables de calculer K_c en calculant $y = E_K(SA_i)$, $z = E_K(SA_j)$, puis $K_{c1} = b_{1i} \oplus y^{-1}$, $K_{c2} = b_{2j} \oplus z^{-1}$, puis et enfin $K_c = K_{c1} \# K_{c2}$.

L'avantage de cette 2ème version est qu'elle permet de transmettre moins de valeurs b_i que la 1ère version (car plusieurs récepteurs ont les mêmes b_{1i} ou b_{2j}). Typiquement, on peut s'arranger pour ne transmettre qu'un nombre de b_{1i} et de b_{2j} qui est de l'ordre de la racine carrée du nombre de récepteurs.

3.2 Le schéma généralisé démultiplié.

Au lieu de dupliquer le schéma de base, on peut plus généralement le démultiplier. Ainsi chaque b_i est composé d'une ou plusieurs valeurs : (b_{1i}, b_{2j}, b_{3k}, ...) et chaque récepteur est caractérisé par une liste d'indices (i,j,k,..) et des adresses (SA_i, SA_j, SA_k, ..) correspondantes. Le récepteur caractérisé par la liste (i,j,k,..) utilise les valeurs (b_{1i}, b_{2j}, b_{3k}, ...) correspondantes avec (SA_i, SA_j, SA_k, ...) pour déchiffrer les valeurs K_{ci} (K_{c1}, K_{c2}, K_{c3}, ...) qui doivent être combinées pour calculer une clef d'accès au contenu K_C, ou le contenu lui-même.

Chaque récepteur va être identifié par une liste d'indices, de préférence unique, sous forme (i), (i,j) ou (i,j,k,..) qui permet de l'identifier (ou d'identifier un petit groupe de récepteurs suspects). De façon équivalente, on peut dire que le récepteur est caractérisé par son ensemble de clefs ou d'adresses selon deux interprétations possibles, qui est son ensemble (SA_i, SA_j, SA_k, ...). Ainsi, on peut combiner ce schéma avec tout autre schéma de traitor tracing à clef secrète connu, par exemple celui décrit dans l'article *Tracing*

Traitors, Crypto'94, de Benny Chor, Amos Fiat, and Moni Naor,. Pour cela, il faut que le protocole de traitor tracing classique spécifie la façon de distribuer des secrets (SA_i, SA_j, SA_k, ...) à des récepteurs et la façon de calculer la clef principale K_C à partir des K_{Ci}. Cela doit se faire, selon le schéma utilisé, de sorte que pour un certain nombre C de récepteurs qui mettent leur clefs commun pour construire un décodeur pirate, on puisse néanmoins identifier un ou tous les pirates, ou tout au moins désactiver tous les décodeurs pirates sans empêcher des récepteurs légitimes non pirates d'accéder au contenu. Selon le procédé de l'invention, comme déjà expliqué plus haut, il y a de nombreuses façons de savoir quelles sont les clefs contenues dans une carte pirate, sans désassembler la carte, simplement en observant son fonctionnement sur une émission qui ne contient qu'une partie des b_i corrects. Cette propriété de black-box tracing est conservée dans les généralisations du schéma de base, et ainsi on peut ne plus envoyer de b_i correspondant à un ou plusieurs secrets SA_i qui sont contenus dans la carte pirate. En même temps, pour les récepteurs légitimes, on peut avoir à leur envoyer (à l'avance, et de préférence chiffrée avec une clef secrète) une nouvelle valeur de SA_i.

3.3 Variantes du schéma généralisé

Toutes les variantes décrites dans le paragraphe 2.1 pour le schéma de base peuvent également s'appliquer au schéma démultiplié décrit dans la partie 3. De plus, il y a d'autres groupes de variantes spécifiques au schéma général dupliqué ou démultiplié :

Groupe de variantes 1 : ces variantes consistent à utiliser d'autres façons de distribuer des secrets (SA_i, SA_j, SA_k, ...) à des récepteurs.

Groupe de variantes 2 : ces variantes consistent à utiliser d'autres façons de calculer la clef principale K_C à partir des K_{Ci}.

Groupe de variantes 3 : variantes où la clef K utilisée dans le calcul des différentes valeurs (b_{1i}, b_{2j}, b_{3k}, ...) n'est pas la même pour toutes ces valeurs. Par exemple on peut utiliser une clef pour les b_{1i} et une autre pour les b_{2j}.

Groupe de variantes 4 : variantes où la fonction f(K, b_i, SA_i) utilisée pour les valeurs b_{1i}, b_{2j} etc... n'est pas la même pour toutes ces valeurs. Par exemple on peut utiliser une fonction différente pour les b_{1i} qui sert à calculer K_{c1}, et une autre fonction pour les b_{2j} qui sert à calculer K_{c2}.

Groupe de variantes 5 : variantes où la clef secrète K_i utilisée pour transmettre les b_{1i} et les b_{2j} n'est pas la même pour tous les récepteurs qui utilisent le même i, ou diffère pour les b_{1i} et les b_{2i}.

L'invention va maintenant être brièvement décrite dans sa mise en œuvre au moyen de dispositifs de traitement d'information. Elle concerne un procédé pour mettre une même information (K_c) à disposition de plusieurs récepteurs appartenant à un ensemble (G) de récepteurs, à partir d'un émetteur comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, chaque récepteur comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, les moyens de mémorisation du récepteur stockant une information (SA_i) qui lui est propre, caractérisé en ce qu'il comprend les étapes consistant à :

-définir, dans les moyens de mémorisation d'information de chaque récepteur, une relation $K_c=f(K, b_i, SA_i)$ où (f) est une fonction déterminée, (K) est une information commune à tous les récepteurs, et (b_i) est une information différente pour chaque récepteur et pour chaque valeur de l'information (K) ;

-donner aux moyens de traitement de chaque récepteur, avant la mise à disposition de (K_c), accès à l'information (b_i) ; et

-transmettre l'information (K) à tous les récepteurs, juste avant la mise à disposition de (K_c), grâce aux moyens de traitement de l'émetteur ; de sorte que chaque récepteur peut calculer l'information (K_c) au moyen de ladite relation, grâce à ses moyens de traitement.

La figure 1 rappelle la constitution générale d'un récepteur 1 du type carte à puce. Il comprend des moyens de traitement d'information ou CPU 2, des moyens de mémorisation d'information 3,4,5 de différents types (RAM, EEPROM, ROM), des moyens d'entrée/sortie 6 permettant à la carte de coopérer avec un terminal lecteur de carte, et un bus 7 permettant à ces différents éléments de dialoguer entre eux. C'est par le biais du terminal (non représenté) que la carte dialogue avec un dispositif émetteur distant.

La figure 2 rappelle la constitution générale d'un dispositif émetteur 10. Il comprend des moyens de traitement d'information ou processeur 11, des moyens de mémorisation d'information 12 pouvant être de différents types (RAM, EEPROM, ROM), des moyens d'entrée/sortie classiques 13 permettant à l'émetteur de coopérer avec le monde extérieur, et un bus 14 permettant à ces différents éléments de dialoguer entre eux. L'émetteur comprend aussi des moyens de transmission 15 spécialement agencés pour communiquer selon l'invention avec l'ensemble de récepteurs auquel il est associé. Dans le cas d'un système de télévision payante, ces moyens de transmission sont agencés pour émettre des images et au moins l'information K précitée, notamment par ondes radio.

REVENDICATIONS

1. Procédé pour mettre une même information (K_c) à disposition de plusieurs récepteurs (1) appartenant à un ensemble (G) de récepteurs, chaque récepteur stockant une information (SA_i) qui lui est propre, caractérisé en ce qu'il comprend les étapes consistant à :
-définir une relation $K_c=f(K, b_i, SA_i)$ où (f) est une fonction déterminée, (K) est une information commune à tous les récepteurs, et (b_i) est une information différente pour chaque récepteur et pour chaque valeur de l'information (K) ;
-donner à chaque récepteur, avant la mise à disposition de (K_c), accès à l'information (b_i) ; et
-transmettre l'information (K) à tous les récepteurs, juste avant la mise à disposition de (K_c) ;
de sorte que chaque récepteur peut calculer l'information (K_c) au moyen de ladite relation.

2. Procédé selon la revendication 1, caractérisé en ce que la fonction (f) est telle qu'à partir de la connaissance d'un (b_i) et d'un (SA_i), on ne connaît pas d'algorithme qui permette d'obtenir l'information (K_c) en un temps réaliste et avec une probabilité non négligeable, lorsqu'on ne connaît pas l'information (K).

3. Procédé selon la revendication 1, caractérisé en ce que la fonction f est telle qu'à partir de la connaissance d'un certain nombre de ($b_1..b_n$) pour un certain sous-ensemble (G') de récepteurs, on ne connaît pas d'algorithme qui permette, avant de connaître K actuelle, en un temps réaliste et avec une probabilité non négligeable, de produire un couple (b_i, SA_i) valide avec un (SA_i) légitime, i n'étant pas un des récepteurs 1..n de (G').

4. Procédé selon la revendication 1 caractérisé en ce que la fonction f est de la forme :

$f(K, b_i, SA_i) = b_i \oplus E_K(SA_i)$

où E_K est une fonction dépendant de l'information (K) et où $\oplus$ désigne une loi de groupe.

5. Procédé selon la revendication 4, caractérisé en ce que la fonction (E_K) est une fonction de chiffrement cryptographique, et (K) une clé secrète utilisée par cette fonction.

6. Procédé selon la revendication 1, caractérisé en ce que les valeurs (b_i) sont envoyées chiffrées avec une clé (K_i) spécifique à chaque récepteur d'un certain ensemble (G) de récepteurs.

7. Procédé selon la revendication 1, caractérisé en ce que chaque valeur (SA_i) est une valeur secrète connue du récepteur d'indice i.

8. Procédé selon la revendication 1, caractérisé en ce que chaque (b_i) est constitué de deux valeurs b_{1i} et b_{2j}, et de même l'information propre de chaque récepteur est constituée de deux valeurs SA_i et SA_j, de sorte que chaque récepteur, identifié par le couple d'indices (i,j), combine les valeurs b_{1i} et b_{2j} correspondantes avec les valeurs SA_i et SA_j pour calculer des valeurs K_{c1} et K_{c2} au moyen de ladite relation, qui à leur tour sont combinées pour accéder à l'information K_C.

9. Procédé selon la revendication 1, caractérisé en ce l'information K_c est une clé permettant de déchiffrer un contenu numérique tel qu'une image de télévision..

10. Procédé selon la revendication 1, caractérisé en ce que l'information K_c est utilisable pendant quelques minutes par les récepteurs, l'information K est envoyée quelques secondes en avance, et les b_i sont envoyés régulièrement en commençant plusieurs jours à l'avance.

11. Procédé selon la revendication 1, caractérisé en ce que certains récepteurs trouvent au moins une partie de leurs valeurs b_i dans une liste de valeurs pré-stockées dans les récepteurs.

12. Objet portatif récepteur (1) appartenant à un ensemble (G) d'objets portatifs, et comprenant des moyens de traitement d'information (2) et des moyens de mémorisation d'information (3,4,5), les moyens de mémorisation stockant une information (SA_i) qui est propre à l'objet portatif et une fonction (f) déterminée, caractérisé en ce qu'il comprend :

-des moyens pour avoir accès à une information (b_i) différente pour chaque objet portatif de l'ensemble (G) et pour chaque valeur de l'information (K) ; et

-des moyens pour calculer une information (K_c) au moyen d'une relation $K_c = f(K, b_i, SA_i)$ où K est une information commune à tous les objets portatifs et transmise à ceux-ci.

13. Dispositif émetteur (10) pour mettre une même information (K_c) à disposition de plusieurs récepteurs (1) appartenant à un ensemble (G) de récepteurs, chaque récepteur stockant une information (SA_i) qui lui est propre, caractérisé en ce qu'il comprend :

-des moyens de calcul (11) agencés pour calculer une information (b_i) à partir d'une relation $K_c=f(K, b_i, SA_i)$ où (f) est une fonction déterminée, (K) est une information commune à tous les récepteurs, et l'information (b_i) est une

information différente pour chaque récepteur et pour chaque valeur de l'information (K) ; et

-des moyens de transmission (15) agencés pour transmettre à chaque récepteur, un certain temps avant la mise à disposition de (K_c), l'information (b_i) qui lui est associée, et pour transmettre l'information (K) à tous les récepteurs, juste avant la mise à disposition de (K_c).

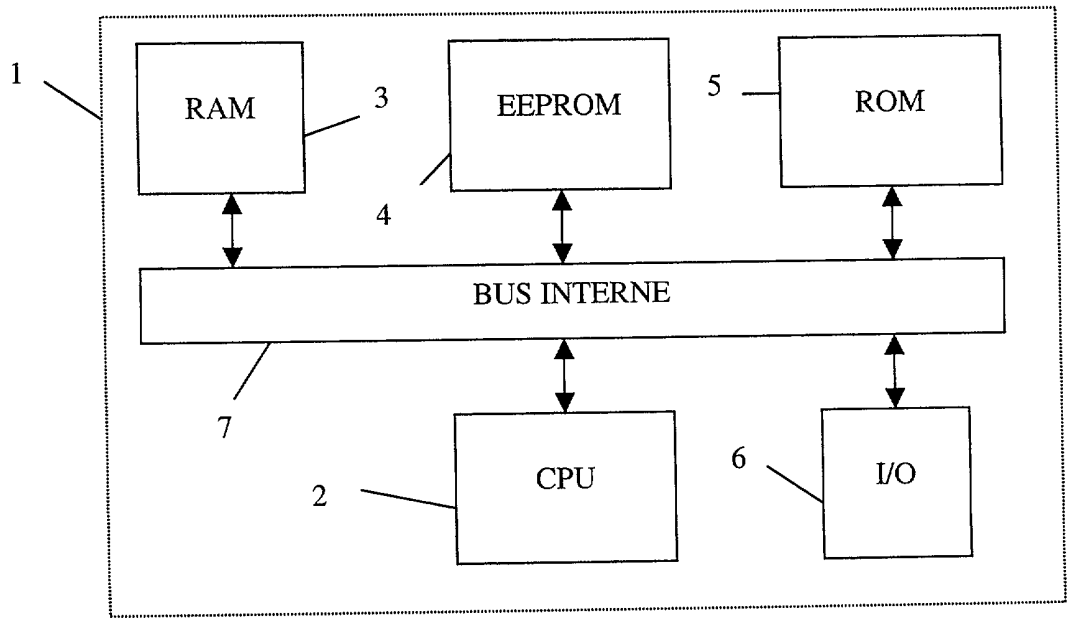

1
RAM
3
EEPROM
5
ROM
4
BUS INTERNE
7
CPU
2
6
I/O

FIG. 1

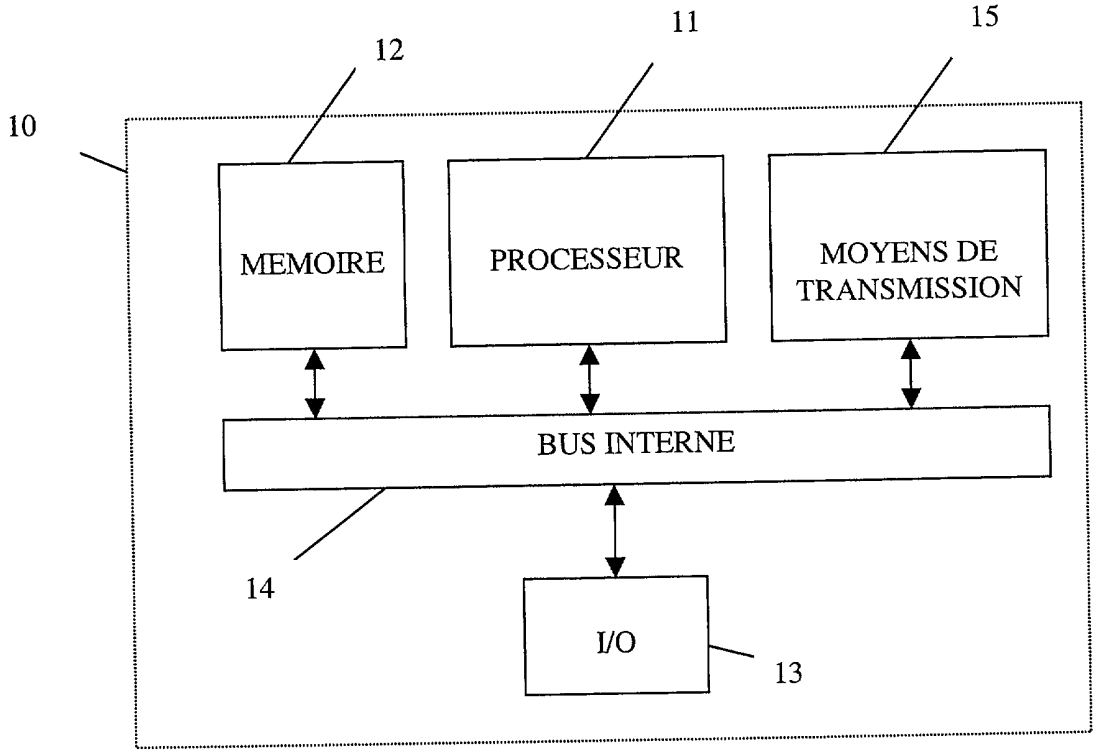

12
11
15
10
MEMOIRE
PROCESSEUR
MOYENS DE TRANSMISSION
BUS INTERNE
14
I/O
13

FIG. 2

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2835670
N° d'enregistrement national

FA 612425
FR 0116585

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		
X	MAYER A ET AL: "Generalized secret sharing and group-key distribution using short keys" COMPRESSION AND COMPLEXITY OF SEQUENCES 1997. PROCEEDINGS SALERNO, ITALY 11-13 JUNE 1997, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 11 juin 1997 (1997-06-11), pages 30-44, XP010274905 ISBN: 0-8186-8132-2 * abrégé * * page 36 - page 40 * ---	1-13	H04L9/12 H04L9/10
D,A	CHOR B ET AL: "Tracing traitors" ADVANCES IN CRYPTOLOGY (CRYPTO). SANTA BARBARA, AUG. 21 - 25, 1994, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, vol. CONF. 14, 1 août 1994 (1994-08-01), pages 257-270, XP002097845 ISBN: 3-540-58333-5 * le document en entier * ---	1-13	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) H04L H04N
A	KIAYIAS A ; YUNG M: "Self protecting pirates and black-box traitor tracing" ADVANCES IN CRYPTOLOGY - CRYPTO 2001, , PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2139), SPRINGER-VERLAG, 23 août 2001 (2001-08-23), pages 63-79, XP002210279 Berlin, Germany ISBN: 3-540-42456-3 * page 63 - page 66 * * page 69 - page 74 * --- -/--	1-13	

1

Date d'achèvement de la recherche	Examinateur
19 août 2002	Carnerero Álvaro, 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

EPO FORM 1503 12.99 (P04C14)

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2835670

N° d'enregistrement national

FA 612425
FR 0116585

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	DENG R H ET AL: "Authenticated key distribution and secure broadcast using no conventional encryption: a unified approach based on block codes" GLOBAL TELECOMMUNICATIONS CONFERENCE, 1995. CONFERENCE RECORD. COMMUNICATION THEORY MINI-CONFERENCE, GLOBECOM '95., IEEE SINGAPORE 13-17 NOV. 1995, NEW YORK, NY, USA,IEEE, US, 13 novembre 1995 (1995-11-13), pages 1193-1197, XP010164413 ISBN: 0-7803-2509-5 * page 1193, colonne de droite, alinéa 2 * -----	1-13	

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

1

Date d'achèvement de la recherche	Examinateur
19 août 2002	Carnerero Álvaro, 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

EPO FORM 1503 12.99 (P04C14)