(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 654 237**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **89 14417**

(51) Int Cl[5] : G 06 K 19/073

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 03.11.89.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 10.05.91 Bulletin 91/19.

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

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

(71) **Demandeur(s) :** *Société dite: LABORATOIRE EUROPEEN DE RECHERCHES ELECTRONIQUES AVANCEES* — FR.

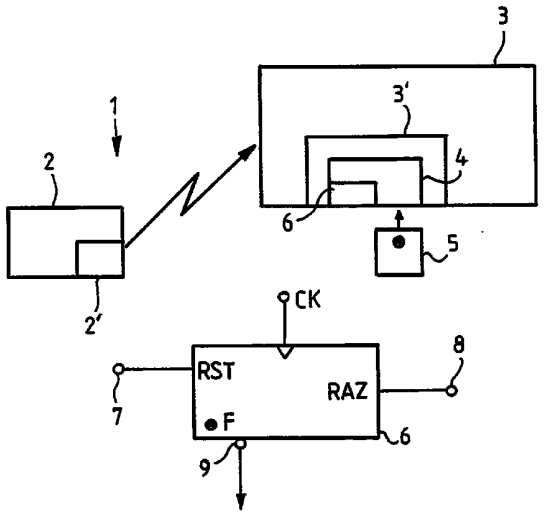
(72) **Inventeur(s) :** Diehl Eric, Hamon Joël et Leduc Michel.

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

(74) **Mandataire :** Chaverneff Vladimir Thomson-CSF.

(54) Procédé de protection contre l'inhibition non autorisée d'écriture de certaines zones de mémoire d'une carte à microprocesseur, et dispositif de mise en œuvre.

(57) Pour empêcher un pirate d'éviter la dévalidation d'une carte à microprocesseur dans un réseau de télévision à péage par exemple lors de la fin de la période de validité de cette carte, on vérifie que le lecteur de cartes est toujours en mesure d'écrire dans la mémoire de cette carte. Cette vérification consiste à surveiller la présence de la tension d'écriture de la carte.



FR 2 654 237 - A1

La présente invention se rapporte à un procédé de protection contre l'inhibition non autorisée d'écriture de certaines zones de mémoire d'une carte à microprocesseur, et à un dispositif de mise en oeuvre.

Dans un réseau de télévision à péage dont les décodeurs utilisent des cartes à microprocesseur, l'émetteur envoie, à la fin de la période de validité des cartes ou s'il s'aperçoit qu'il faut inhiber définitivement des cartes contrefaites (ayant toutes la même identité par suite d'une contrefaçon à l'identique), un signal commandant l'inscription dans ces cartes d'une donnée de fin de validité et/ou inhibant tout accès à la carte. La tension d'écriture d'une telle carte apparaît sur un conducteur déterminé du décodeur qu'un "pirate" peut facilement repérer (en général, il s'agit d'un conducteur sur lequel est présente une tension supérieure à la tension d'alimentation de service de la carte). Il suffit alors de couper ce conducteur pour empêcher la dévalidation de la carte.

Une solution connue, préconisée par la norme Eurocrypt actuelle, consiste à réserver dans la mémoire de la carte une zone dans laquelle sont inscrites les dates de début et de fin de validité de la carte, un programme commandant l'auto-destruction de la carte lorsque la période de validité de la carte est écoulée (l'émetteur communique constamment à la carte la date courante). La mémorisation de telles données dans la carte entraîne une diminution non négligeable de sa capacité de mémorisation, et de la capacité de transmission de données du réseau.

La présente invention a pour objet un procédé, simple et facile à mettre en oeuvre, de protection contre l'inhibition non autorisée d'écriture de certaines zones de la mémoire d'une carte à microprocesseur utilisée dans un réseau comportant au moins un centre de gestion ou émetteur et au moins un terminal ou récepteur comprenant des moyens coopérant avec des cartes à microprocesseur.

La présente invention a également pour objet un dispositif de mise en oeuvre du procédé, simple et peu onéreux.

Le procédé conforme à l'invention consiste, dans un réseau du type précité, à envoyer périodiquement une donnée quelconque à inscrire à au moins un emplacement de la mémoire de la carte, et à vérifier aussitôt dans la carte que cette donnée a bien été inscrite. De façon avantageuse, cette donnée est un simple bit dont la valeur est modifiée aléatoirement ou pseudo-aléatoirement. Ainsi, si quelqu'un venait à couper le fil d'amenée de tension d'écriture de la carte, ou à bloquer d'une quelconque manière l'écriture de cette carte, ce fait pourrait être détecté rapidement. Cette détection peut par exemple entraîner le blocage de toute transaction ultérieure de la carte.

Le dispositif de mise en oeuvre de l'invention, appliqué à un réseau comportant au moins un centre de gestion et au moins un terminal relié à ce centre de gestion, et équipé d'un lecteur de cartes à microprocesseur, comporte, dans le centre de gestion, des moyens de production périodique d'une information à inscrire dans la carte, et dans le lecteur de cartes du terminal des moyens de transmission à une carte de ladite information, et dans la carte des moyens de vérification d'écriture de ladite information, ces moyens de vérification commandant l'inhibition de préférence définitive d'au moins un moyen de lecture ou d'écriture de la carte.

La présente invention sera mieux comprise à la lecture de la description détaillée d'un mode de réalisation, pris comme exemple non limitatif et illustré par le dessin annexé dont la figure unique est un bloc-diagramme simplifié d'un réseau

conforme à l'invention.

L'invention est décrite ci-dessous en référence à un réseau de télévision à péage, mais il est bien entendu qu'elle n'est pas limitée à une telle application, et qu'elle peut s'appliquer à tout réseau du type comportant au moins un centre de gestion, de contrôle ou émetteur (appelé ici, pour simplifier, centre de gestion) et au moins un terminal ou récepteur (appelé ici, pour simplifier, terminal), relié au centre de gestion par tout moyen approprié (câble, ondes radio, faisceau hertzien...), ce terminal étant muni d'un dispositif lecteur de cartes à microprocesseur ("smart card").

Les cartes à microprocesseur utilisées dans un tel réseau ont généralement une durée de validité limitée (un ou plusieurs mois), en particulier afin de limiter tous risques de contrefaçon ou de "piratage".

Le réseau 1 de télévision à péage, représenté de façon simplifiée sur la figure unique du dessin, comporte un émetteur de programmes 2 et un grand nombre de récepteurs. Un seul de ces récepteurs, référencé 3, a été représenté sur le dessin. Le récepteur 3 comporte, en plus de ses circuits habituels, dans son décodeur 3', un lecteur 4 de cartes à microprocesseur. Une telle carte, référencée 5 a été représentée sur le dessin.

Afin de déterminer dans le décodeur si un utilisateur mal intentionné n'a pas bloqué l'arrivée de la tension d'écriture (en général une tension continue de 15 ou 21 V) de la carte utilisée, on fait produire par un circuit 2' de l'émetteur 2 (ce circuit 2' peut faire partie des circuits de cryptage de l'émetteur 2) un signal répétitif (ayant une période de 2 à 4s par exemple) qui doit être inscrit dans une zone déterminée de la mémoire de la carte 5. Ce signal répétitif peut par exemple être un simple bit "0" ou "1", dont la valeur est déterminée par un générateur pseudo-aléatoire. La zone déterminée peut comporter plusieurs emplacements différents choisis aléatoirement, afin de rendre la détection de cette inscription plus difficile.

Dans la carte 5, un compteur 6, recevant sur son entrée de signaux d'horloge CK des signaux d'horloge utilisés pour le microprocesseur de cette carte, réalise la détection de la présence de la tension d'écriture de la mémoire de cette carte. L'entrée 7 d'initialisation du compteur 6 reçoit, à la mise sous tension de la carte 5 (lors de son introduction dans le lecteur 4) un signal mettant à zéro ce compteur. L'entrée 8 de remise à zéro du compteur 6 reçoit la tension d'écriture de la carte, éventuellement divisée selon un rapport approprié (pour la ramener à 5V par exemple). La sortie 9 de débordement ("overflow") du compteur 6 est reliée à l'entrée de commande d'un circuit d'inhibition de lecture de la carte 5 ou de blocage quelconque de cette carte (par exemple une porte interposée dans le circuit d'alimentation du microprocesseur de la carte).

L'état de comptage maximal du compteur 6 est tel qu'il corresponde à, par exemple une ou deux périodes dudit signal répétitif. Ainsi, si l'écriture de la mémoire de la carte 5 (commandée par ce signal répétitif) a lieu normalement, le compteur 6 est remis à zéro (entrée 8) par l'écriture du signal répétitif, et n'atteint jamais son état maximal de comptage. Sinon, il atteint cet état maximal de comptage, et un signal de débordement apparaît à sa sortie 9 et bloque le fonctionnement de la carte 5.

REVENDICATIONS

1. Procédé de protection contre l'inhibition non autorisée d'écriture de certaines zones de mémoire d'une carte à microprocesseur utilisée dans un réseau comportant au moins un centre de gestion et au moins un terminal relié à ce centre de gestion, caractérisé par le fait qu'il consiste à envoyer périodiquement une donnée quelconque à inscrire à au moins un emplacement de la mémoire de la carte, et à vérifier aussitôt dans la carte que cette donnée a bien été inscrite.

2. Procédé selon la revendication 1, caractérisé par le fait que la vérification consiste à détecter la présence d'une tension d'écriture sur la carte.

3. Procédé selon l'une des revendications précédentes, caractérisé par le fait que si ladite donnée n'a pu être inscrite dans la mémoire de la carte, il y a blocage de toute transaction ultérieure de la carte.

4. Dispositif de protection contre l'inhibition non autorisée d'écriture de certaines zones de mémoire d'une carte à microprocesseur utilisée dans un réseau comportant au moins un centre de gestion (2) et au moins un terminal (3), caractérisé par le fait que le centre de gestion comporte des moyens de production périodique d'une information à inscrire dans la carte (2').

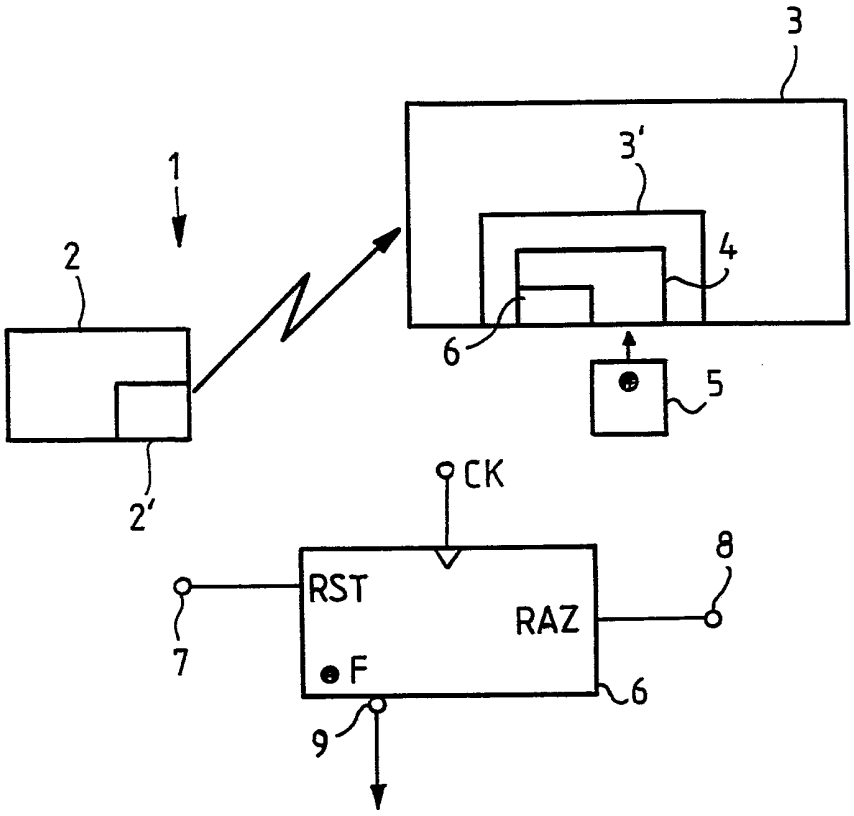
5. Dispositif selon la revendication 4, caractérisé par le fait que le lecteur de cartes (4) du terminal comporte des moyens de transmission à une carte (5) de ladite information.

6. Dispositif selon l'une des revendications 4 ou 5, caractérisé par le fait que la carte à microprocesseur (5) comporte des moyens de vérification d'écriture (6) de ladite information.

7. Dispositif selon la revendication 6, caractérisé par le fait que les moyens de vérification comportent un

compteur (6) alimenté en signaux d'horloge prélevés dans la carte et dont l'entrée de remise à zéro reçoit la tension d'écriture de la carte (8).

8. Dispositif selon la revendication 6 ou 7, caractérisé par le fait que les moyens de vérification sont reliés à un moyen d'inhibition de la carte.


3
3'
1
2
4
6
5
2'
CK
8
RST
RAZ
7
F
6
9

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

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

2654237

N° d'enregistrement national

FR 8914417
FA 433577

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	FR-A-2606199 (EUROTECHNIQUE) * abrégé; revendications 1, 2 * ---	1-4, 6, 8
A	US-A-3906460 (HALPERN) * abrégé; revendications 1, 2, 10, 17 * * colonne 1 - colonne 2, ligne 50 * -----	1-6

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G06K
G07F

Date d'achèvement de la recherche	Examinateur
20 JUILLET 1990	BEAUCE G.Y.G.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
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 03.82 (P0413)