(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 659 768**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **90 03571**

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

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 14.03.90.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 20.09.91 Bulletin 91/38.

(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) :** *SEXTANT AVIONIQUE Société Anonyme* — FR.

(72) **Inventeur(s) :** Lignereux Françoise et Dupuis Serge.

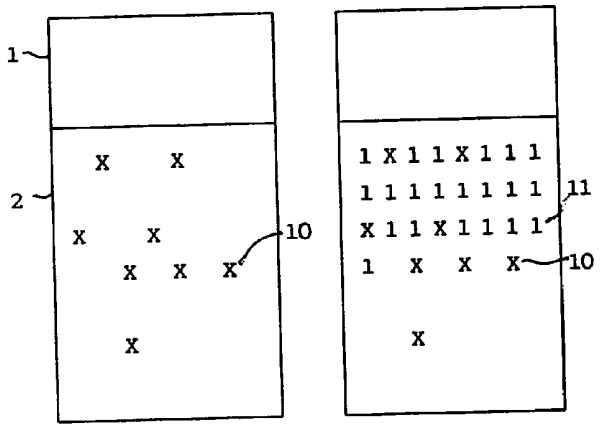
(73) **Titulaire(s) :**

(74) **Mandataire :** De Beaumont Michel Cabinet Conseil.

(54) Procédé de codage et de décodage de cartes à mémoire prépayées.

(57) La présente invention concerne un procédé de codage et de décodage de cartes à mémoire prépayées comprenant une première zone mémoire (1) à lecture seulement contenant des données d'identification de la carte et une deuxième zone mémoire (2) à lecture/écriture destinée à l'inscription de données (11) indiquant l'utilisation du service prépayé. Ce procédé consiste:

- lors du codage de la carte, à écrire un nombre déterminé de cellules (10) de la deuxième zone mémoire en des emplacements correspondant à des données de la première zone mémoire selon un algorithme déterminé; et
- lors du décodage de la carte, à valider la carte seulement si l'on reconnaît dans la première zone un numéro d'identification valable et dans la deuxième zone des cellules écrites aux emplacements fixés selon ledit algorithme à partir desdites données de la première zone mémoire.



FR 2 659 768 - A1

PROCÉDÉ DE CODAGE ET DE DÉCODAGE DE CARTES À MÉMOIRE PRÉPAYÉES

La présente invention concerne le domaine des cartes à mémoire prépayées et plus particulièrement un mode de codage et de décodage antifraude de telles cartes.

Une carte à mémoire prépayée consiste en un support contenant une mémoire et des connecteurs d'accès aux bornes d'alimentation, d'adressage, de lecture et d'écriture de la mémoire. Ces cartes à mémoire ne sont pas équipées de circuits de traitement des informations. Elles ne sont que des supports de mémorisation dans lesquels des données sont inscrites et lues.

La figure 1A illustre schématiquement l'organisation usuelle de la mémoire d'une carte prépayée classique. Cette mémoire est partagée en deux zones 1 et 2. La zone 1 est une zone à lecture seulement, protégée en écriture, dans laquelle on a initialement inséré des données d'identification et de service permettant d'autoriser le fonctionnement de la carte pour le service auquel elle est destinée. La zone 2 contient des cellules mémoire à lecture/écriture, dans lesquelles les cellules sont séquentiellement écrites tandis que le service est utilisé.

Pour un test initial de la carte, lors de sa fabrication, on procède généralement à une écriture dans un certain nombre de cellules séquentielles de la zone 2, les cellules inscrites étant marquées d'une croix et désignées par la référence 3 en figure 1A.

Ensuite, comme l'illustre la figure 1B, on écrit dans des cellules successives 4 au fur et à mesure de l'utilisation de la carte, les zones écrites étant marquées dans la figure par des 1. On notera que, matériellement, il n'y a pas de différence entre une zone 3 marquée d'une croix et une zone 4 marquée d'un 1 mais que ce mode de représentation a été choisi uniquement pour permettre de différencier les cellules écrites lors de la fabrication de la carte des cellules écrites lors de son utilisation.

Lors du fonctionnement d'une carte, le lecteur ou le central associé au service considéré, commence par lire les données d'identification dans la zone 1 pour vérifier qu'il s'agit bien d'une carte autorisée, puis vérifie dans la zone d'utilisation 2 s'il reste des cellules vierges, c'est-à-dire si la carte n'est pas épuisée.

Divers procédés ont été développés pour éviter la fraude de telles cartes, par exemple pour éviter que l'on puisse se servir du numéro d'identification d'une carte déjà complètement utilisée, ou qu'on puisse utiliser une carte partiellement écrite sans réaliser d'inscription dans la zone d'utilisation 2.

Une des approches pour éviter ce type de fraude consiste à mémoriser au niveau d'un poste de traitement central une liste de toutes les cartes déjà complètement utilisées. Toutefois, cette approche présente des limites du fait que, si un très grand nombre de cartes est en circulation, ce qui est par exemple le cas pour les cartes utilisées dans les cabines téléphoniques, la capacité du central fait que l'on est obligé de réduire périodiquement le nombre d'informations mémorisées dans la liste pour pouvoir en accepter de nouvelles. Ainsi, par exemple, on pourra garder seulement pendant un mois ou deux une information sur une carte épuisée. Ensuite, si une carte épuisée est réutilisée après effacement ou simulation d'effacement, le central ne pourra pas la détecter. De même, de tels centraux peuvent permettre de reconnaître des cartes n'allant pas jusqu'à l'épuisement mais étant très largement utilisées. Mais, à nouveau, ce type de mémorisation centrale est limité par sa capacité de mémorisation.

L'une des fraudes qui pourrait être envisagée consisterait à utiliser de vieilles cartes épuisées, jetées par leur propriétaire initial après utilisation, à recopier les informations des zones d'identification et de service, et à simuler la carte par des mémoires externes reliées au connecteur de la carte par des fils. Ceci permettrait de réutiliser ces cartes au moins une fois complètement et, étant donné le grand nombre de cartes en circulation, le fraudeur pourrait facilement obtenir de très nombreux services avec de telles cartes usagées et un appareil adapté.

Un objet de la présente invention est d'éviter ce type de fraude c'est-à-dire d'éviter la réutilisation de cartes épuisées et de limiter les possibilités de surutilisation de cartes partiellement consommées.

Pour atteindre cet objet, la présente invention prévoit un procédé de codage et de décodage de cartes à mémoire prépayées comprenant une première zone mémoire à lecture seulement contenant des données d'identification de la carte et une deuxième zone mémoire à lecture/écriture destinée à l'inscription de données indiquant l'utilisation du service prépayé, consistant, lors du codage de la carte, à écrire un nombre déterminé de cellules de la deuxième zone mémoire en des emplacements correspondant à des données de la première zone mémoire selon un algorithme déterminé ; et lors du décodage de la carte, à valider la carte seulement si l'on reconnaît dans la première zone un numéro d'identification valable et dans la deuxième zone des cellules écrites aux emplacements fixés selon ledit algorithme à partir desdites données de la première zone mémoire.

Selon un mode de réalisation de la présente invention, l'inscription des données d'utilisation dans la deuxième zone mémoire se fait selon un deuxième algorithme, d'apparence aléatoire.

Ces objets, caractéristiques et avantages ainsi que d'autres de la présente invention seront exposés plus en détail dans la description suivante de modes de réalisation particuliers faite en relation avec les figures jointes parmi lesquelles :

les figures 1A et 1B illustrent la structure de mémorisation d'une carte à mémoire prépayée classique ; et

les figures 2A, 2B et 2C illustrent la structure de mémorisation d'une carte à mémoire prépayée selon la présente invention.

La figure 2A illustre la structure de mémorisation d'une carte prépayée selon la présente invention. On y retrouve, comme dans le cas de la figure 1A, une zone 1 à lecture seulement de mémorisation de données d'identification et de service et une zone 2 de mémorisation de données d'utilisation.

Selon l'invention, à la fabrication, on introduit dans la zone d'utilisation des informations correspondant également à des données contenues dans la zone d'identification telle que le numéro d'identification de la carte. Ces informations sont inscrites sous forme d'écriture dans des cellules 10 de la zone d'utilisation, marquées de croix dans la figure, la position de ces cellules étant déterminée par un algorithme secret à partir de données contenues dans la zone d'identification.

On notera que cela ne réduit sensiblement pas la capacité disponible de la zone d'utilisation puisque, de toute manière, on utilisait déjà dans l'art antérieur une inscription préalable de certaines des cellules de la zone d'utilisation dans des buts de test. Les cellules 10 pourront également servir à la réalisation d'un test de bon fonctionnement de la carte.

La figure 2B illustre une carte selon la présente invention, dans laquelle on a procédé à une écriture séquentielle de cellules 11 de la zone d'utilisation 2 au cours de la consommation du service que la carte est destinée à assurer.

Comme dans le cas de la figure 1B, on a marqué par des croix les cellules 10 qui ont été écrites selon le code correspondant aux données d'identification et par des 1 les cellules 11 écrites et correspondant à une utilisation de la carte. En fait, matériellement, ces deux types d'écriture ne se distingueront pas, on notera seulement que des cellules ont été écrites ou non.

Ainsi, une fois que la carte a été partiellement écrite, comme cela est illustré en figure 2B, on ne reconnaît plus dans la zone écrite les cellules qui ont été préalablement écrites. Un observateur de la carte ne pourra plus déterminer ces cellules.

Pour lire une carte codée selon la présente invention, le lecteur analysera d'une part les données d'identification dans la zone à lecture seulement 1 et vérifiera également que des cellules prédéterminées 10 de la zone 2 ont été écrites conformément à l'algorithme secret déterminant ces cellules à partir du numéro d'identification. C'est seulement si ces cellules sont écrites que la carte sera validée. Ainsi, un fraudeur ne pourra pas remettre à zéro la zone d'utilisation de la carte car alors le lecteur ne validerait plus cette carte. Le fraudeur devra laisser un grand nombre de cellules écrites, ou rechercher par tâtonnement les cellules préinscrites ce qui serait extrêmement long et difficile.

Enfin, la figure 2C illustre une carte utilisée de la même façon que celle de la figure 2B mais dans laquelle l'écriture de la zone d'utilisation ne se fait pas selon un ordre séquentiel naturel. En effet, selon un aspect de la présente invention, pour dérouter encore le fraudeur éventuel et lui interdire d'utiliser des cartes partiellement utilisées, on pourra prévoir que l'inscription des cellules 10 indiquant une utilisation de la carte se fasse selon un algorithme prédéterminé, spécifique de la carte, ce qui fait que le fraudeur pourra encore plus difficilement reconnaître les cellules écrites correspondant à des données d'identification dans la zone d'utilisation.

Ainsi, la présente invention permet d'éviter la réutilisation de cartes complètement écrites sauf à effectuer des tâtonnements longs et fastidieux et de limiter fortement l'utilisation abusive de cartes partiellement écrites.

Comme cela a été exposé précédemment, la présente invention permet d'éviter la fraude, de préférence en relation avec des systèmes centraux d'établissement de listes de cartes abusivement utilisées, pour éviter qu'un fraudeur ne réutilise abusivement des cartes seulement partiellement utilisées.

Bien entendu, la présente invention est susceptible de diverses variantes et pourra se combiner avec d'autres systèmes antifraude déjà connus.

REVENDICATIONS

1. Procédé de codage et de décodage de cartes à mémoire prépayées comprenant une première zone mémoire (1) à lecture seulement contenant des données d'identification de la carte et une deuxième zone mémoire (2) à lecture/écriture destinée à l'inscription de données (11) indiquant l'utilisation du service prépayé, caractérisé en ce qu'il consiste :

- lors du codage de la carte, à écrire un nombre déterminé de cellules (10) de la deuxième zone mémoire en des emplacements correspondant à des données de la première zone mémoire selon un algorithme déterminé ; et

- lors du décodage de la carte, à valider la carte seulement si l'on reconnaît dans la première zone un numéro d'identification valable et dans la deuxième zone des cellules écrites aux emplacements fixés selon ledit algorithme à partir desdites données de la première zone mémoire.

2. Procédé de codage et de décodage selon la revendication 1, caractérisé en ce que l'inscription des données d'utilisation dans la deuxième zone mémoire se fait selon un deuxième algorithme, d'apparence aléatoire (figure 2C).

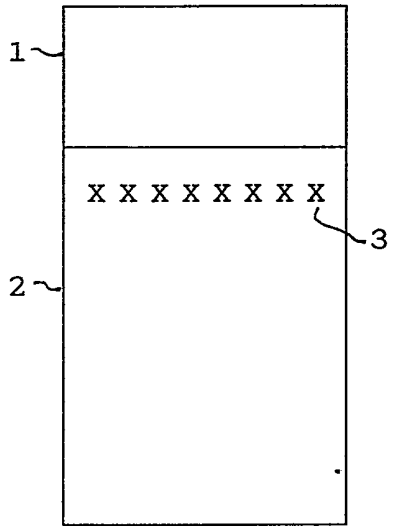


FIG 1A

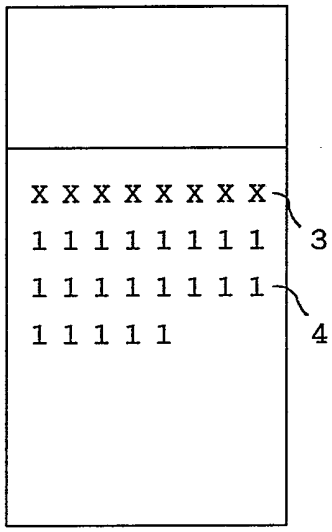


FIG 1B

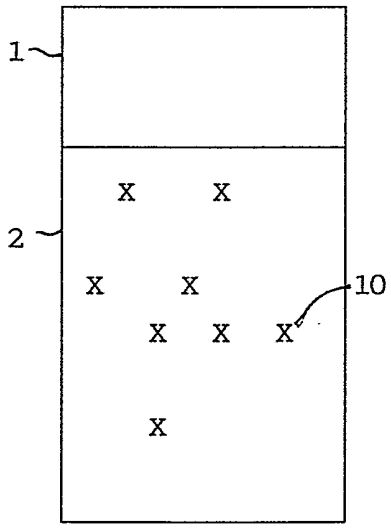


FIG 2A

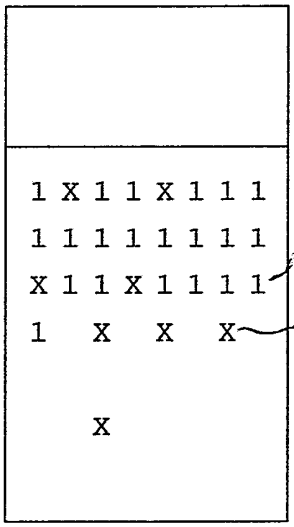


FIG 2B

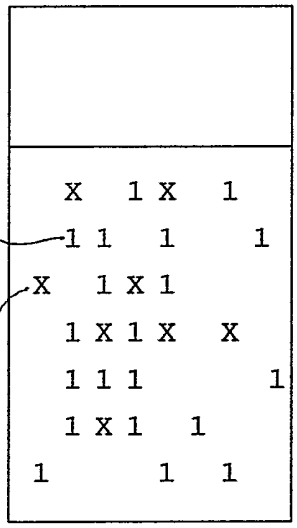


FIG 2C

REPUBLIQUE FRANÇAISE

2659768

N° d'enregistrement national

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

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

FR 9003571
FA 440109

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	FR-A-2522850 (ELECTRONIQUE MARCEL DASSAULT) * revendications ; figures * ---	1
X	US-A-3869700 (K.A. COOK) * abrégé; figures * * colonne 1, lignes 36 - 60 * * colonne 2, lignes 32 - 52 *	1
A		2

A	GB-A-2052819 (H. STOCKBURGER) * abrégé; figures * * page 3, lignes 59 - 105 * -----	1, 2

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G07F

Date d'achèvement de la recherche: 14 NOVEMBRE 1990

Examinateur: DAVID J.Y.H.

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)