(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication: **0 298 831**
A1

(12) # DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt: **88401646.0**

(51) Int. Cl.[4]: **G 07 F 7/10**

(22) Date de dépôt: **28.06.88**

(30) Priorité: **07.07.87 FR 8709604**

(43) Date de publication de la demande:
11.01.89 Bulletin 89/02

(84) Etats contractants désignés:
BE CH DE ES FR GB IT LI NL SE

(71) Demandeur: **SCHLUMBERGER INDUSTRIES**
50, avenue Jean Jaurès
F-92120 Montrouge (FR)

(72) Inventeur: **Barakat, Simon**
3, Allée des Tilleuls
F-78570 Andrésy (FR)

(74) Mandataire: **Dronne, Guy**
SCHLUMBERGER INDUSTRIES Groupe Transactions Electronique 50, avenue Jean Jaurès
F-92120 Montrouge (FR)

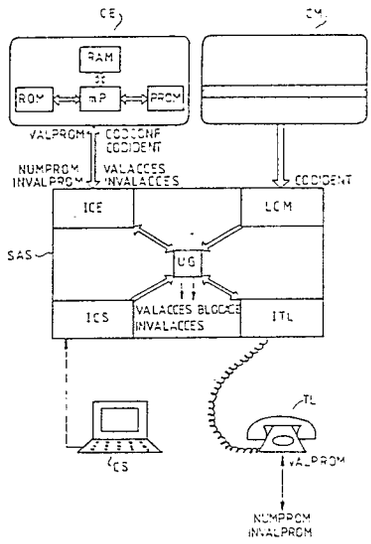
(54) **Procédé et dispositif anti-fraude pour un système à accès sélectif.**

(57) Procédé et dispositif de protection d'un système à accès sélectif contre une utilisation frauduleuse d'une carte magnétique à code confidentiel.

A chaque carte (CM) est affectée une classe correspondant à une zone d'une mémoire (PROM). Le nombre de classes est égal au nombre de zones et sensiblement inférieur au nombre de cartes (CM) susceptibles d'être présentées.

A chaque échec d'introduction de code confidentiel, un bit est modifié dans la zone de mémoire appropriée.

FIG.1



EP 0 298 831 A1

Description

PROCEDE ET DISPOSITIF ANTI-FRAUDE POUR UN SYSTEME A ACCES SELECTIF

La présente invention concerne un procédé et un dispositif destinés à empêcher l'utilisation frauduleuse, sur un système à accès sélectif, de titres d'accès usurpés, grâce à une détection efficace des opérations de recherche systématique des codes confidentiels affectés à ces titres d'accès.

Dans une de ses applications possibles, l'invention vise par exemple à empêcher l'utilisation frauduleuse, sur des caisses enregistreuses, de cartes de crédit magnétiques volées.

Le procédé de l'invention comprend, de façon connue, les étapes consistant à : obtenir, à chaque présentation au système d'un titre d'accès, le résultat d'une vérification de la validité d'un code confidentiel indiqué par l'utilisateur de ce titre, ce résultat étant interprété comme un succès en cas de validité de ce code et comme un échec dans le cas contraire; garder, dans une mémoire, une trace des échecs constatés à l'occasion de présentations successives de titres d'accès; et émettre un signal indicateur de fraude lorsque le nombre de ces échecs dépasse une limite prédéterminée.

L'invention est applicable dans tous les cas où chaque titre d'accès se compose de, ou contient, une information, généralement publique, qui permet de vérifier, grâce à une relation gardée secrète, la validité du code confidentiel que l'utilisateur du titre d'accès fournit de façon indépendante, par exemple par l'intermédiaire d'un clavier.

Dans l'un de ses modes de réalisation, elle est même efficace lorsqu'il existe a priori une possibilité de fraude basée sur une recherche systématique des numéros confidentiels de plusieurs titres d'accès à la fois.

Des possibilités d'usurpation de titres d'accès existent, par exemple, avec des cartes magnétiques de crédit volées, utilisées en conjonction avec une caisse enregistreuse qui possède un clavier au moyen duquel les clients désirant payer avec une carte de crédit magnétique doivent normalement indiquer leur code confidentiel.

Dans la mesure où l'invalidtié du code confidentiel indiqué par le porteur de la carte se traduit par un refus du paiement à effectuer, toute personne ayant accès à une telle caisse enregistreuse et détenant une carte magnétique volée est a priori en mesure de rechercher, par des essais successifs, le code confidentiel affecté à cette carte, puis d'utiliser ce code confidentiel pour débiter un compte bancaire dont il n'est pas titulaire.

Les chiffres du code confidentiel étant normalement au nombre de quatre, la recherche systématique conduit nécessairement au succès après un nombre d'essais au maximum égal à 10 000.

La solution connue pour empêcher cette fraude consiste à tenir, dans une mémoire de la caisse enregistreuse, une liste des numéros ou codes d'identification des dernières cartes magnétiques, pour lesquelles le code confidentiel introduit par le client était faux.

La sécurite est obtenue en imposant une limite au nombre d'apparitions d'un même numéro sur cette liste, c'est-à-dire en imposant un nombre maximum d'échecs pour une même carte magnétique.

En cas de dépassement, la carte qui l'a provoqué est annulée.

Le principal défaut de cette technique connue est que la mémoire, dans laquelle est tenue la liste des numéros de cartes, se comporte comme un registre à décalage.

Lorsque la liste est pleine, tout nouvel échec élimine de la mémoire le numéro de la carte qui a fait l'objet de l'échec le plus ancien, de sorte que toute trace de ce dernier disparaît.

Le dispositif de sécurité peut donc être trompé en recherchant les codes confidentiels de plusieurs cartes magnétiques à la fois, en procédant par roulement et de façon telle que le rapport du nombre maximum de numéros mémorisés dans la liste, au nombre de cartes testées, reste inférieur au nombre limite d'échecs dont le dépassement produirait l'annulation d'une carte.

Dans ce contexte, le but de la présente invention est de proposer un procédé et un dispositif de sécurité qui, grâce notamment à une grande économie de l'espace mémoire, ne présente pas les défauts de la technique précédemment décrite.

A cette fin, le procédé de l'invention est essentiellement caractérisé en ce que l'opération consistant à garder trace des échecs comprend elle-même les opérations consistant à : définir, dans la mémoire, une pluralité de zones de mémoire; assigner à chaque titre d'accès présenté l'une des classes d'un ensemble de classes dont chacune correspond à une zone de mémoire; et tenir, dans chaque zone de la mémoire, le compte du nombre d'échecs dont font l'objet ceux des titres d'accès présentés qui appartiennent à la classe à laquelle correspond cette zone de mémoire, et en ce que l'opération d'émission d'un signal indicateur de fraude est conditionnée par le dépassement, par le nombre d'échecs enregistrés dans l'une quelconque des zones de la mémoire, d'un nombre limite assigné à cette zone et constituant ladite limite prédéterminée.

Selon le procédé de l'invention, appliqué à des cartes magnétiques, telles que des cartes de crédit, à chacune desquelles est affecté au moins un attribut intrinsèque, tel que le code confidentiel, ou un numéro d'identification, le numéro de la classe assignée à chaque carte magnétique est de préférence déduit de l'attribut intrinsèque de cette carte par l'application d'une fonction surjective prédéterminée.

Par exemple, le numéro de la classe assignée à chaque carte magnétique est donné par un ensemble d'au moins un chiffre extrait du numéro d'identification de cette carte, chaque chiffre étant extrait en fonction d'une position qu'il occupe dans ce numéro, et cette position étant prédéterminée et choisie plus proche de la fin du numéro d'identification, dans le sens de l'écriture de ce dernier, que du début de ce numéro, de façon que toutes les valeurs

possibles, de 0 à 9, de chaque chiffre extrait, soient sensiblement équiprobables pour l'ensemble des cartes présentées, ledit nombre limite étant alors le même pour toutes les zones de mémoire.

Dans une forme de réalisation simple de l'invention, la correspondance entre chaque classe et une zone de mémoire est telle que le numéro de chaque classe définit l'addresse de la zone de mémoire à laquelle elle correspond.

Pour éviter les fraudes faisant intervenir un grand nombre de cartes magnétiques, le procédé de l'invention peut comprendre une seconde opération d'émission d'un signal de fraude, conditionnée par le dépassement, par le nombre d'échecs enregistrés dans l'ensemble des zones de mémoire, d'une seconde limite prédéterminée.

Le dispositif de l'invention comprend, de façon connue : des moyens de saisie d'information propres à recevoir d'une part au moins un attribut intrinsèque du titre d'accès, cet attribut étant relié audit code confidentiel exact de celui-ci et d'autre part un code confidentiel indiqué par l'utilisateur du titre d'accès; des moyens de traitement reliés aux moyens de saisie, susceptibles de vérifier la validité du code confidentiel indiqué par l'utilisateur; et une mémoire reliée aux moyens de traitement, dans laquelle ces derniers enregistrent une donnée d'échec à chaque fois qu'un code confidentiel s'avère invalide.

Selon l'invention, ce dispositif est essentiellement caractérisé en ce que, la mémoire étant découpée en zones accessibles à des adresses différentes, les moyens de traitement sont conçus pour élaborer une adresse mémoire en fonction au moins dudit attribut du titre d'accès, et pour enregistrer la donnée d'échec dans la zone de mémoire correspondant à cette adresse.

La mémoire comprend avantageusement une mémoire à lecture seulement, dans laquelle chaque donnée d'échec est enregistrée sous la forme d'un seul bit.

Selon un mode de réalisation préféré de l'invention, la mémoire est constituée par la mémoire PROM d'une carte à mémoire, tandis que les moyens de traitement comprennent le microprocesseur de celle-ci.

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui en est faite ci-après, à titre indicatif et nullement limitatif, en référence aux dessins annexés, parmi lesquels :

- La figure 1 représente une partie de l'architecture fonctionnelle d'une caisse enregistreuse à accès sélectif, à laquelle a été intégré le perfectionnement de l'invention, et
- la figure 2 est un organigramme représentant le déroulement du procédé de l'invention.

L'invention concerne un procédé et un dispositif permettant d'empêcher l'utilisation frauduleuse d'un titre d'accès usurpé, en association avec un système à accès sélectif.

Par système à accès sélectif, on entend précisément un système susceptible d'accorder à chacun des utilisateurs potentiels un certain privilège, tel que l'accès à un service ou la remise d'un produit, sous réserve que cet utilisateur présente à ce système un titre d'accès valide, dont la validité est confirmée par celle d'un code confidentiel également fourni par l'utilisateur.

Les exemples de systèmes à accès sélectifs sont nombreux.

Un système informatique gérant une base de données, à laquelle les utilisateurs ne peuvent accéder qu'après avoir indiqué d'une part leur nom ou leur code utilisateur et d'autre part le code confidentiel exact qui leur a été affecté, constitue un système à accès sélectif; une caisse enregistreuse, qui est dotée d'un lecteur de cartes magnétiques de crédit et d'un clavier au moyen duquel le possesseur de la carte indique son code confidentiel, et qui n'accepte le paiement par carte qu'après vérification de la validité du code confidentiel, constitue un autre système à accès sélectif.

Dans le premier exemple, le titre d'accès de l'utilisateur est de nature immatérielle : il est constitué, par exemple, par une suite de lettres; dans le second exemple, le titre d'accès de l'utilisateur est de nature matérielle : c'est une carte magnétique; ces deux cas sont cependant semblables en ce sens que, dans les deux cas, les titres d'accès sont personnalisés, vis-à-vis de l'utilisateur, par des attributs intrinsèques généralement dépourvus de caractère confidentiel, à savoir le nom propre de l'utilisateur dans le premier exemple, et le numéro ou le code d'identification de la carte magnétique de l'utilisateur dans le second exemple.

Dans ces deux exemples également, l'accès au système n'est obtenu qu'après indication, par l'utilisateur, d'un code confidentiel qui lui a été assigné, et vérification de la validité de ce code; cette vérification est par exemple réalisée par la comparaison d'une fonction du code confidentiel, elle-même gardée secrète, avec l'attribut intrinsèque du titre d'accès.

Si la comparaison révèle une disparité, son résultat conduit à un échec pour ce qui concerne l'accès au système, alors que ce résultat conduit à un succès, c'est-à-dire à l'accès au système, si la comparaison révèle une identité.

Ainsi, bien que, sur la figure 1, le système à accès sélectif SAS représente, de façon schématique, une caisse enregistreuse, l'invention est applicable, comme le percevra l'homme de l'art, à tout autre système à accès sélectif, et notamment à un système informatique gérant une base de données.

La caisse enregistreuse SAS comprend notamment, de façon connue, une unité de gestion UG reliée à plusieurs organes périphériques, dont un lecteur de cartes magnétiques LCM, un circuit d'interface de console ICS et un circuit d'interface téléphonique ITL.

Le lecteur LCM permet de lire un attribut de chaque carte magnétique CM, par exemple le numéro ou code d'identification CODIDENT de cette carte.

L'interface ICS, reliée à la console CS, est susceptible de recevoir le code confidentiel CODCONF tapé par l'utilisateur de la carte CM.

Selon l'invention, la caisse enregistreuse SAS est également dotée d'un circuit d'interface pour carte électronique ICE, permettant un échange bidirec-

tionnel d'informations entre l'unité de gestion UG et une carte électronique à microprocesseur CE. Les circuits d'interface tels que ICE, et les cartes électroniques telles que CE, sont bien connus de l'homme de l'art, de sorte que leur description détaillée est ici superflue. Il suffit, pour la compréhension de la présente invention, de rappeler que les cartes électroniques à microprocesseur CE comprennent un microprocesseur mP généralement relié à une mémoire à lecture seulement non programmable ROM, à une mémoire à lecture seulement programmable PROM, et à une mémoire vive RAM. Cette carte CE est traditionnellement dotée de moyens, non représentés, permettant au microprocesseur mP non seulement de lire, mais aussi d'écrire, des données dans la mémoire à lecture seulement PROM.

Bien entendu, l'écriture de données dans la mémoire PROM est irréversible, de sorte que celle-ci se comporte, pour l'écriture, comme une mémoire consomptible. De ce fait, la mémoire PROM est non volatile. De surcroît, les cartes électroniques CE sont également dotées, de façon classique, de moyens prohibant l'accès, de l'extérieur de la carte, aux informations enregistrées dans la mémoire PROM. En fait, ces propriétés sont celles qui sont recherchées pour la mise en oeuvre de l'invention, pour laquelle le recours spécifique à l'emploi d'une carte électronique reste facultatif.

Le commerçant, possesseur de la caise enregistreuse SAS, doit insérer une carte électronique CE dans le circuit ICE pour permettre le fonctionnement de la caisse.

Il doit en outre demander, au service chargé de la distribution et du contrôle des cartes électroniques CE, de valider, par l'émission d'un signal VALPROM sur le réseau téléphonique, via le téléphone TL, et les circuits ITL, UG et ICE, l'utilisation d'une nouvelle carte électronique CE ou la validation d'une carte électronique qui a été invalidée par dépassement d'un quota prédéterminé par le nombre total d'échecs enregistrés dans cette carte, comme décrit en référence à la dernière opération de l'organigramme de la figure 2.

Le signal VALPROM est par exemple mémorisé dans la mémoire PROM de la carte électronique CE.

L'insertion d'une carte magnétique CM dans le lecteur LCM déclenche un ensemble d'opérations dont un enchaînement possible est illustré sur l'organigramme de la figure 2.

Le microprocesseur mP vérifie que la carte électronique CE a été validée en recherchant si la donnée VALPROM est présente dans la mémoire avec une valeur représentative de sa validité.

Dans le cas contraire, le microprocesseur mP envoie au circuit ICE un signal de blocage INVALPROM qui inhibe le fonctionnement de la caisse SAS.

La carte électronique CE, lorsqu'elle est validée, reçoit, via le lecteur LCM, l'unité UG et l'interface ICE, le code d'identification CODIDENT de la carte magnétique CM, généralement constitué par un simple numéro de série.

Parallèlement, la carte électronique CE reçoit le code confidentiel CODCONF introduit par l'utilisateur de la carte CM au moyen de la console CS, via l'interface ICS, l'unité UG et l'interface ICE.

De préférence, chaque chiffre du code CODCONF est lui-même codé dans la console CS et décodé par le microprocesseur mP, de manière à éviter toute interception frauduleuse du code confidentiel CODCONF, par exemple sur la ligne reliant la console CS au circuit d'interface ICS.

Le microprocesseur mP, disposant du code d'identification CODIDENT et du code confidentiel CODCONF vérifie la validité de ce dernier en recherchant, de façon en soi connue, si les conditions de compatibilité qui doivent exister entre CODIDENT et CODCONF sont effectivement satisfaites.

Si tel est le cas, le microprocesseur mP émet un ordre VALACCES autorisant l'accès au système SAS, c'est-à-dire le paiement au moyen de la carte CM, sur la caisse enregistreuse SAS.

En cas d'invalidité de CODCONF s'engage un processus opératoire qui constitue l'essentiel de l'invention.

Dans ce cas en effet, le procédé, objet de l'invention ne traite plus la carte magnétique CM comme le titre d'accès qui est défini de façon univoque par son code d'identification CODIDENT, mais comme un élément indifférencié d'une classe à laquelle correspond une zone de la mémoire PROM.

Pour cela, la mémoire PROM étant virtuellement ou physiquement découpée en une pluralité de zones de mémoire accessibles à des adresses différentes, le procédé consiste à assigner, à la carte CM dont le code CODCONF est invalide, l'une des classes d'un ensemble de classes dont le nombre est égale à celui des zones de mémoire.

Par exemple, la mémoire PROM utilisable pour la mise en oeuvre de l'invention comprend 4 Koctets, et est considérée comme constituée de 1 000 zones de 32 bits chacune.

La classe de chaque carte magnétique est déterminée par les trois derniers chiffres de CODIDENT, c'est-à-dire les trois chiffres de poids le plus faible.

Comme il existe de nombreuses cartes dont les numéros d'identification CODIDENT respectifs présentent les mêmes trois derniers chiffres, l'application qui, du code CODIDENT, conduit à la classe de carte CM ayant ce code, est dite "surjective". Par ailleurs, comme chacun des trois derniers chiffres du code CODIDENT varie de 0 à 9, cette application définit 1 000 classes, c'est-à-dire autant de classes qu'il y a de zones de mémoire PROM.

Enfin, comme toutes les valeurs, de 0 à 9 de chacun des trois derniers chiffres de CODIDENT sont équiprobables, une carte magnétique CM prise au hasard a une probabilité homogène, égale à 0.001, d'appartenir à n'importe laquelle des classes.

La classe de la carte CM ayant été définie, le microprocesseur mP lit le nombre enregistré dans la zone de la mémoire PROM qui correspond à cette classe.

Par exemple, si le code d'identification CODIDENT est 16244962357, la classe est 357, et le microprocesseur lit le contenu de la zone de mémoire PROM

d'adresse 357, c'est-à-dire, en d'autres termes, le contenue de la 357ième zone de mémoire PROM.

Si le nombre lu dans cette zone 357 est égal à un premier nombre limite, correspondant à 32 bits mis à "1" dans l'exemple choisi, le microprocesseur mP émet un ordre INVALPROM, qui inhibe le fonctionnement de la caisse enregistreuse SAS. Dans cette hypothèse, le commerçant possesseur de cette caisse n'en peut recouvrer l'utilisation normale qu'après avoir reçu, sous la forme d'un signal VALPROM transmis sur le réseau téléphonique, l'autorisation d'utiliser une nouvelle carte électronique CE, comme décrit précédemment.

Si le nombre lu dans la zone 357 de la mémoire PROM n'est pas égal à cette limite de 32 bits, il est augmenté d'une unité, c'est-à-dire modifié par la mise à "1" du premier bit qui, dans la série de 32 bits enregistrée dans cette zone, est un bit "0".

Cette opération correspond à l'enregistrement, dans la mémoire PROM de l'échec d'accès à la caisse SAS pour la carte magnétique CM, ou pour toute autre carte CM appartenant à la même classe qu'elle.

Ensuite, le microprocesseur mP lit tous les bits enregistrés dans toute la mémoire PROM, dont chacun correspond à un échec d'accès, et compare le total à un second nombre limite prédéterminé, par exemple 96.

En cas d'égalité, le microprocesseur mP émet un signal INVALPROM.

En cas d'inégalité, le microprocesseur mP émet un signal INVALACCES. Ce dernier signal a pour effet d'informer le commerçant, et le porteur de la carte, de l'invalidité du code confidentiel, de refuser provisoirement le paiement par carte, mais d'autoriser une nouvelle introduction du code confidentiel.

Les calculs montrent qu'en l'absence de test utilisant une comparaison entre le nombre total d'échecs enregistrés dans la mémoire PROM et un second nombre limite, et avec les exemples numériques précédemment cités (mémoire PROM de 4 Koctets découpée en 1 000 zones de 32 bits), la probabilité pour qu'une carte électronique CE soit périmée à la suite de 12 000 échecs n'est que de 1%; elle est de l'ordre de 50% pour 16 800 échecs.

Comme les utilisateurs de cartes magnétiques se trompent statistiquement une fois sur dix dans l'indication de leur code confidentiel, cela signifie qu'une carte électronique CE peut, avec une probabilité de 99%, traiter, en l'absence de fraude, 120 000 opérations de paiement par carte magnétique.

Par la mise en oeuvre de l'invention, et toujours sur la base de l'exemple numérique ci-dessus, la probabilité pour qu'une personne, ignorant le code confidentiel CODCONF d'une carte magnétique, le découvre par essais successifs sur une caisse enregistreuse SAS équipée d'une carte électronique CE neuve (ce qui correspond à 32 essais possibles pour 10 000 possibilités) n'est égale qu'à 0.32%.

En revanche si cette personne dispose de N cartes cette possibilité, en l'absence de surveillance du nombre total d'échecs enregistrés dans la PROM, augmente considérablement avec N, puisqu'elle est égale à $1-(1-0.032)^N$. La comparaison du nombre total d'échecs à un second nombre limite permet d'écarter cet autre type de fraude.

L'assignation, à la carte magnétique CM, d'une classe définie par les trois derniers chiffres du code CODIDENT, constitue bien entendu un exemple non limitatif. Une telle assignation a l'avantage de conduire à une répartition homogène des cartes magnétiques CM dans les différentes classes et à l'utilisation d'un même nombre limite dans chaque zone (32 pour l'exemple choisi). Néanmoins, ces caractéristiques, bien qu'avantageuses, ne sont pas indispensables.

Quel que soit le mode d'attribution d'une classe à chaque carte magnétique présentée, il importe seulement, pour assurer la plus grande longévité et le meilleur usage possibles de la mémoire PROM, que le nombre de classes soit inférieur au nombre de cartes magnétiques CM, et que le nombre limite surveillé dans chaque zone de la mémoire PROM, c'est-à-dire en fait la dimension de cette zone, soit relié, à la probabilité pour qu'une carte magnétique quelconque CM soit affectée à la classe correspondant à cette zone, par un coefficient de proportionnalité qui se trouve être le même pour toutes les zones.

Revendications

1. Procédé de protection d'un système à accès sélectif contre une utilisation frauduleuse d'au moins un titre d'accès auquel est affecté un code confidentiel, comprenant les opérations consistant à: obtenir, à chaque présentation d'un titre d'accès au système, le résultat d'une vérification de la validité d'un code confidentiel indique par l'utilisateur de ce titre, ce résultat étant interprété comme un succès en cas de validité de ce code et comme un échec dans le cas contraire; garder, dans une mémoire, une trace des échecs constatés à l'occasion de présentations successives de titres d'accès; et émettre un signal indicateur de fraude lorsque le nombre de ces échecs dépasse une limite prédéterminée, caractérisé en ce que l'opération consistant à garder trace des échecs comprend elle-même les opérations consistant à : définir, dans la mémoire, une pluralité de zones de mémoire; assigner à chaque titre d'accès présenté l'une des classes d'un ensemble de classes dont chacune correspond à une zone de mémoire; et tenir, dans chaque zone de la mémoire, le compte du nombre d'échecs dont font l'objet ceux des titres d'accès présentés qui appartiennent à la classe à laquelle correspond cette zone de mémoire, et en ce que l'opération d'émission d'un signal indicateur de fraude est conditionnée par le dépassement, par le nombre d'échecs enregistrés dans l'une quelconque des zones de la mémoire, d'un nombre limite assigné à cette zone et constituant ladite limite prédéterminée.

2. Procédé suivant la revendication 1, appliqué au cas où lesdits titres d'accès sont des cartes magnétiques, telles que des cartes de crédit, à chacune desquelles est affecté au moins un attribut intrinsèque, tel que le code confidentiel ou un numéro d'identification, caractérisé en ce que le numéro de la classe assignée à chaque carte magnétique est déduit de l'attribut intrisèque de cette carte par l'application d'une fonction surjective prédéterminée.

3. Procédé suivant la revendication 2, caractérisé en ce que le numéro de la classe assignée à chaque carte magnétique est donné par un ensemble d'au moins un chiffre extrait du numéro d'identification de cette carte, chaque chiffre étant extrait en fonction d'une position qu'il occupe dans ce numéro, et cette position étant prédéterminée et choisie plus proche de la fin du numéro d'identification que du début, de façon que toutes les valeurs possibles, de 0 à 9, de chaque chiffre extrait, soient sensiblement équiprobables pour l'ensemble des cartes présentées, ledit nombre limite étant alors le même pour toutes les zones de mémoire.

4. Procédé suivant l'une quelconque des revendications 1 à 3, caractérisé en ce que le numéro de chaque classe définit l'adresse de la zone de mémoire à laquelle elle correspond.

5. Procédé suivant l'une quelconque des revendications 1 à 4 caractérisé en ce qu'il comprend une seconde opération d'émission d'un signal de fraude, conditionnée par le dépassement, par le nombre d'échecs enregistrés dans l'ensemble des zones de mémoire, d'une seconde limite prédéterminée.

6. Dispositif de protection contre une utilisation frauduleuse, sur un système à accès sélectif, d'au moins un titre d'accès auquel est affecté un code confidentiel, comprenant : des moyens de saisie d'information propres à recevoir d'une part au moins un attribut intrinsèque du titre d'accès, cet attribut étant relié audit code confidentiel exact de celui-ci et d'autre part un code confidentiel indiqué par l'utilisateur du titre d'accès; des moyens de traitement reliés aux moyens de saisie, susceptibles de vérifier la validité du code confidentiel indiqué par l'utilisateur; et une mémoire reliée aux moyens de traitement, dans laquelle ces derniers enregistrent une donnée d'échec à chaque fois qu'un code confidentiel s'avère invalide, caracérisé en ce que, la mémoire étant découpée en zones accessibles à des adresses différentes, les moyens de traitement sont conçus pour élaborer une adresse mémoire en fonction au moins dudit attribut du titre d'accès, et pour enregistrer la donnée d'échec dans la zone de mémoire correspondant à cette adresse.

7. Dispositif suivant la revendication 6, caractérisé en ce que la mémoire est une mémoire à lecture seulement.

8. Dispositif suivant la revendication 7, caractérisé en ce que chaque donnée d'échec s'exprime par un seul bit.

9. Dispositif suivant l'une quelconque des revendications 6 à 8, caractérisé en ce que ladite mémoire comprend une mémoire PROM d'une carte à mémoire.

10. Dispositif suivant l'une quelconque des revendications 6 à 9, caractérisé en ce que lesdits moyens de traitement comprennent un microprocesseur d'une carte à mémoire.

FIG. 1

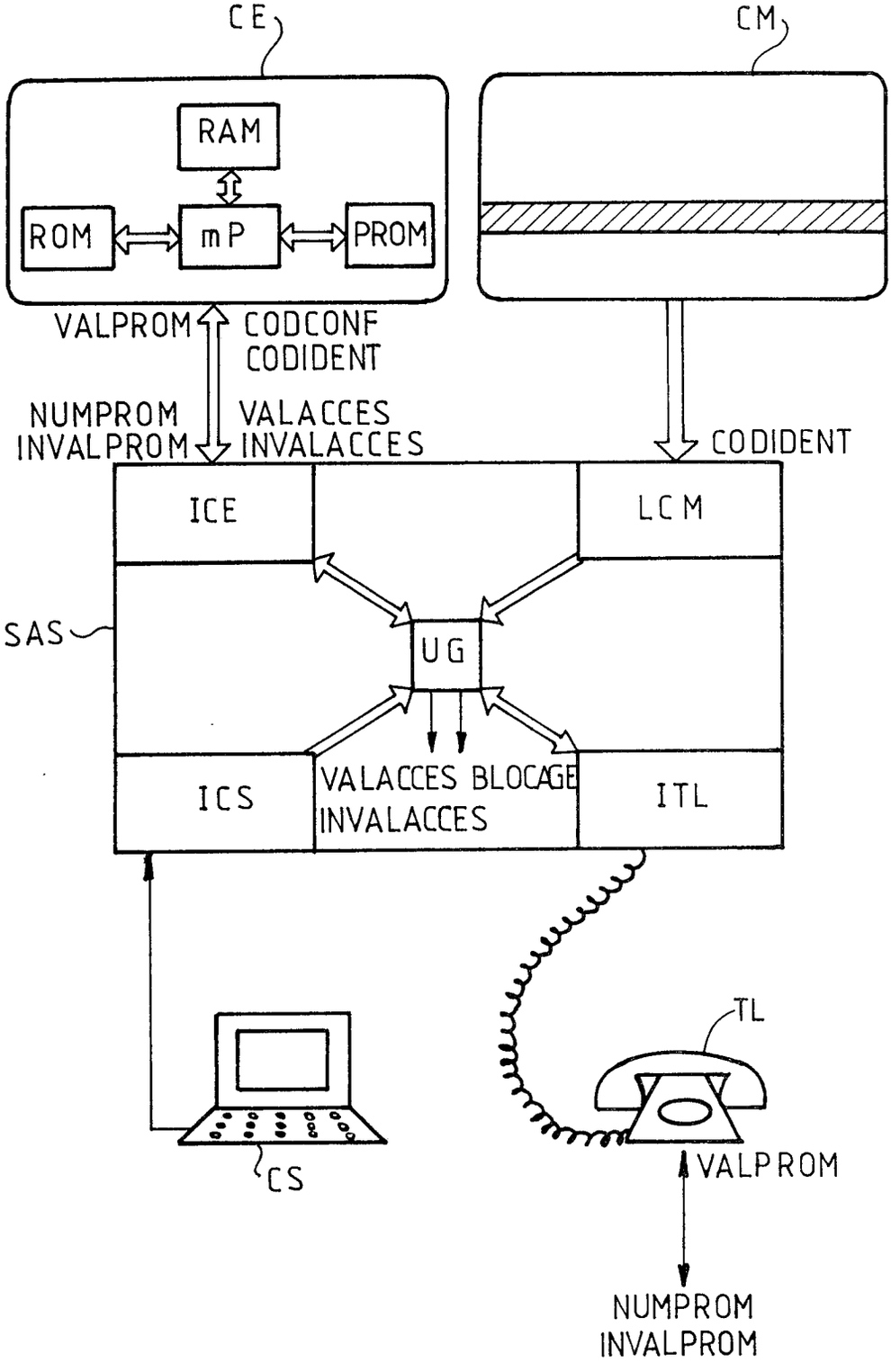
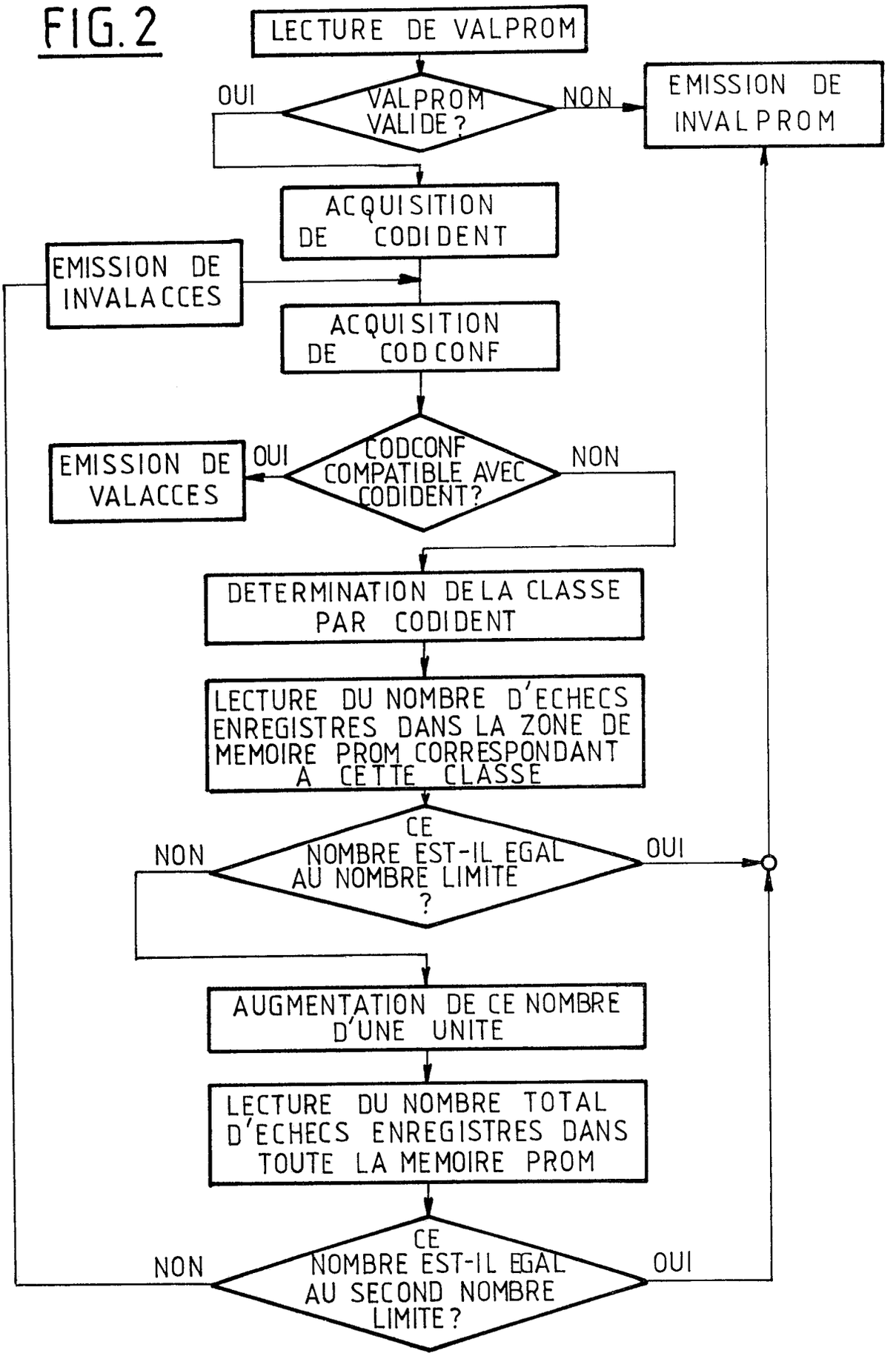

CE
CM
RAM
ROM
mP
PROM
VALPROM
CODCONF
CODIDENT
NUMPROM
INVALPROM
VALACCES
INVALACCES
CODIDENT
ICE
LCM
SAS
UG
ICS
VALACCES BLOCAGE
INVALACCES
ITL
TL
CS
VALPROM
NUMPROM
INVALPROM

FIG.2


LECTURE DE VALPROM
VALPROM VALIDE ?
OUI
NON
EMISSION DE INVALPROM
ACQUISITION DE CODIDENT
EMISSION DE INVALACCES
ACQUISITION DE CODCONF
CODCONF COMPATIBLE AVEC CODIDENT ?
EMISSION DE VALACCES
OUI
NON
DETERMINATION DE LA CLASSE PAR CODIDENT
LECTURE DU NOMBRE D'ECHECS ENREGISTRES DANS LA ZONE DE MEMOIRE PROM CORRESPONDANT A CETTE CLASSE
CE NOMBRE EST-IL EGAL AU NOMBRE LIMITE ?
NON
OUI
AUGMENTATION DE CE NOMBRE D'UNE UNITE
LECTURE DU NOMBRE TOTAL D'ECHECS ENREGISTRES DANS TOUTE LA MEMOIRE PROM
CE NOMBRE EST-IL EGAL AU SECOND NOMBRE LIMITE ?
NON
OUI

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande

EP 88 40 1646

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl.4)
A	FR-A-2 349 181 (TRANSAC) * En entier * ---	1,5,6	G 07 F 7/10
A	US-A-3 731 076 (M. NAGATA) * Résumé; figure 4; colonne 5, ligne 54 - colonne 6, ligne 39 * ---	1-4,6	
A	FR-A-2 471 000 (ELECTRONIQUE MARCEL DASSAULT) * Revendications; figures 1,2 * ---	1,6-9	
A	EP-A-0 160 833 (TOSHIBA) * Résumé; revendications * -----	1,6-10	

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.4)

G 07 F
G 07 C

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	06-10-1988	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 : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0402)