RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 473 755**
(A n'utiliser que pour les commandes de reproduction).

A1

DEMANDE DE BREVET D'INVENTION

(21) **N° 80 00615**

(54) **Procédé et dispositif électronique de mémorisation et de traitement confidentiel de données.**

(51) Classification internationale (Int. Cl. ³). **G 06 K 5/00; G 06 F 7/04.**

(22) Date de dépôt..... 11 janvier 1980.

(33) (32) (31) Priorité revendiquée :

(41) Date de la mise à la disposition du public de la demande..... B.O.P.I. — « Listes » n° 29 du 17-7-1981.

(71) Déposant : Société dite : TRAITEMENT DE L'INFORMATION TECHNIQUES NOUVELLES, TITN, résidant en France.

(72) Invention de : Claude Guignard, Jean Mitaine et Pierre Paternoster.

(73) Titulaire : *Idem* (71)

(74) Mandataire : Michel Pierre,
173, bd Haussmann, 75360 Paris Cedex 08.

La présente invention a pour objet un procédé de mémorisation et de traitement confidentiel de données. Elle a également pour objet un dispositif électronique portatif assurant la mise en oeuvre de ce procédé.

Il est à l'heure actuelle connu d'utiliser des dispositifs portatifs, tels que tickets ou cartes, coopérant avec un système informatique de traitement de données qui comporte une unité de dialogue avec le porteur du dispositif, appelée terminal. Les applications d'un tel système sont assez variées : ouverture d'une porte, contrôle de tickets par exemple pour transports en commun, et nombreuses applications bancaires, parmi lesquelles on peut citer les distributeurs de billets de banque, les guichets automatiques permettant notamment la tenue des comptes en banque en même temps que la distribution de billets, et l'enregistrement direct d'une transaction commerciale sur un point de vente, une information étant alors enregistrée à la fois au niveau du terminal situé chez le commerçant et au niveau du dispositif portatif (carte), afin que le compte du porteur de la carte puisse être débité d'une somme inscrite au crédit du compte du commerçant.

Dans ces différentes applications, le traitement des informations peut consister en une simple reconnaissance de validité dans le cas d'un ticket

ou d'une carte d'accès par exemple, à laquelle peut s'ajouter la reconnaissance du porteur de la carte dès que celle-ci est personnalisée ; ce traitement peut s'accompagner d'une simple inscription sur la carte permettant de garder trace de l'opération effectuée, appelée dans toute la suite "transaction", ou donner lieu à des traitements complexes de tenue de fichiers ou de comptes (lecture et écriture), dans le cas notamment de terminaux connectés à un centre de traitement informatique.

Pour ce genre de systèmes se pose un problème général de sécurité, du fait des risques de perte ou de vol des dispositifs portatifs ainsi que des risques de fraude visant notamment à revalider un ticket ou une carte périmés par une opération précédente, ou à rendre inopérant le processus de reconnaissance du porteur d'une carte. Ce problème revêt une importance particulière dans les applications bancaires.

La présente invention a pour objet un procédé répondant à ces divers impératifs, ainsi qu'un dispositif électronique portatif mettant en oeuvre ce procédé et susceptible de coopérer avec un système informatique permettant le dialogue avec l'utilisateur du dispositif.

Plus précisément, le dispositif comporte principalement :

- une mémoire comportant au moins une zone dans laquelle sont enregistrés des éléments d'identification de l'utilisateur, ineffaçables, et une zone dans laquelle sont enregistrées successivement les transactions effectuées, ces transactions étant soit ineffaçables, soit effaçables seulement par une ca-

tégorie d'utilisateurs (banquier par exemple) ; ces deux zones sont chacune organisées en mots comportant un certain nombre de bits réservés à des informations de contrôle ;

- des moyens d'adressage de cette mémoire en écriture et en lecture, sous le contrôle d'une part des éléments d'identification et d'autre part des informations de contrôle accompagnant chacune des transactions ;
- des moyens d'interface assurant le couplage électrique entre le terminal et le dispositif ;
- un comparateur susceptible de recevoir d'une part des informations en provenance de la mémoire et d'autre part des informations en provenance de l'extérieur, telles que code d'accès, afin de réaliser des opérations de reconnaissance de l'utilisateur, fournissant le résultat de la comparaison à un élément de mémoire ;
- des moyens logiques de commande de synchronisation des différents composants du dispositif, recevant les informations de contrôle précédentes et le contenu de l'élément de mémoire.

Le procédé mis en oeuvre par ce dispositif comporte principalement, pour la réalisation de chaque transaction, les étapes suivantes :

- le test de la validité d'un code fourni au dispositif par l'utilisateur, par comparaison de cette information extérieure avec une information contenue dans la partie ineffaçable de la mémoire, cette comparaison s'effectuant entièrement de façon interne au dispositif ; la comparaison fournit une information également interne sur la validité du code extérieur ;
- la recherche d'une adresse, dans la mémoire du dis-

positif, qui soit disponible pour enregistrer des informations relatives à la transaction en cours, et l'inscription à cette adresse notamment de l'information de validité ;

- lorsque l'information de validité l'autorise, l'accès à la mémoire du dispositif afin de réaliser la transaction considérée.

D'autres objets, caractéristiques et résultats de l'invention ressortiront de la description suivante illustrée par les dessins annexés, qui représentent :

- la figure 1, le schéma d'un mode de réalisation du dispositif selon l'invention ;
- la figure 2, un schéma de l'organisation de la mémoire utilisée dans le dispositif de la figure précédente ;
- la figure 3, les principales étapes du procédé selon l'invention ;
- la figure 4, un mode de réalisation de la deuxième étape du procédé de la figure précédente ;
- la figure 5, un mode de réalisation de la troisième étape du procédé de la figure 3 ;
- la figure 6, un mode de réalisation de la quatrième étape du procédé de la figure 3 ;
- la figure 7, une variante de réalisation des moyens de commande utilisés dans le dispositif selon l'invention.

Sur ces différentes figures, les mêmes références se rapportent aux mêmes éléments. Par ailleurs, afin de simplifier l'exposé, la description qui suit est faite dans le cadre d'une application particulière : l'application bancaire "point de vente", mais il est clair que le procédé ou le dispositif décrits

sont utilisables pour toute application comportant des étapes de reconnaissance de l'utilisateur et d'inscription de la transaction effectuée. Par ailleurs, dans toute la suite de la description, on appelle "transfert" une opération de lecture ou d'écriture en mémoire, et "transaction" un ensemble de transferts, comportant une écriture, précédée ou non d'une ou plusieurs lectures.

La figure 1 est donc le schéma d'un mode de réalisation du dispositif selon l'invention.

Ce dispositif qui se présente généralement, dans l'application mentionnée plus haut, sous forme d'une carte, comporte principalement une mémoire permanente M, un ensemble de comparaison et de mémorisation de cette comparaison, constitué par des éléments C et B, et un circuit logique L de commande et de synchronisation des différents composants de ce dispositif.

Ce dispositif reçoit des informations de l'extérieur sur une borne 10, informations se présentant sous forme de données binaires en série, par mots de n bits. Ces informations sont dirigées vers un interface d'entrée-sortie I, commandé par le circuit L ; cet interface a pour fonction d'assurer le couplage électrique entre carte et terminal, ainsi que d'opérer une remise en forme des signaux. Les informations transitant par l'interface I peuvent être dirigées, toujours en série, soit vers un comparateur C, soit vers un registre à décalage R_D. Le registre à décalage est en communication avec un registre d'adresses R_A, en parallèle sur p bits. Ce registre R_A contient une adresse dans la mémoire M à laquelle il est désiré écrire ou lire ; à cet effet

le registre R_A est relié toujours en parallèle sur p bits à une partie sélecteur d'adresses (S) de la mémoire M. L'information lue ou écrite en mémoire à cette adresse est transmise au registre à décalage R_D (ou en provenance de ce dernier) en parallèle sur n bits, sur lesquels sont prélevés les q premiers bits, qui représentent des informations de contrôle, à destination du circuit de commande L. Le circuit L commande en outre le registre à décalage R_D, la mémoire M (commande 11) et l'incrémentation, unité par unité, du registre d'adresses R_A.

L'ensemble de comparaison mentionné précédemment comporte donc le comparateur C recevant l'information en provenance de l'interface I d'une part et du registre R_D, en série, d'autre part et un élément bistable B relié au comparateur C, qui a pour fonction de mémoriser le résultat de la comparaison effectuée dans l'élément C. Le bistable B est relié au circuit de commande L.

La figure 2 est un schéma illustrant l'organisation de la mémoire M.

Cette mémoire est organisée en P mots de n bits chacun ; elle est adressable par des mots de p bits si $2^p \geq P$; elle se divise en deux zones : une première zone (Z_I) comportant P_I mots de n bits, dans laquelle les informations sont inscrites lors de la construction du dispositif et sont ineffaçables sans destruction de ce dernier, et une seconde zone (Z_T) comportant P_T mots de n bits également, qui est initialement vierge en ce qui concerne les m derniers bits de chaque mot, et remplie au fur et à mesure des transactions effectuées avec le dispositif et éventuellement peut être effacée dans certaines conditions,

la carte étant alors dite "réinitialisée", afin d'être réutilisée pour d'autres séries de transactions.

Dans le cas de l'application "point de vente" évoquée plus haut, dans la zone ineffaçable Z_I sont enregistrées différentes informations d'identification telles que le code confidentiel d'accès à la mémoire, qui se subdivise de préférence en code affecté à la banque et code affecté au client de la banque, porteur de la carte, relevé d'identité bancaire, numéro de la carte, date d'émission, date d'échéance, identité de l'utilisateur, éventuellement des indications de limitation d'usage de la carte, etc. Ces informations se présentent chacune sous la forme d'un mot de m bits auxquels sont ajoutés q bits permettant l'accès contrôlé aux informations correspondantes, avec $m+q = n$.

La zone Z_T est réservée à l'inscription des transactions successives, chacune d'entre elles étant inscrite sur un mot de n bits. Ce mot se décompose comme précédemment en deux parties : une première partie de q bits est réservée au contrôle, la partie restante étant utilisée pour l'enregistrement de la transaction, c'est-à-dire des informations telles que date, type de l'opération et montant de l'opération.

Dans l'exemple considéré, le porteur peut donc réaliser P_T transactions.

Sur la figure, les q bits constituant la zone de contrôle ont été distingués à titre d'exemple en six bits notés B_{A1}, B_{A2}, B_T, B_{M1}, B_{M2} et B_C. L'utilisation de ces différents bits de contrôle est explicitée dans la description du procédé qui suit.

La mémoire est de préférence réalisée par

des circuits intégrés. Dans une variante de réalisation, la zone Z_T est effaçable par la banque, ce qui est réalisé par irradiation ultraviolette par exemple, la zone Z_I étant alors protégée lors de la construction de la carte par une couche métallique telle qu'une couche d'aluminium. Ce mode de réalisation permet la réutilisation de la même carte après ré-initialisation, pour P_T nouvelles transactions, ce qui diminue bien entendu le prix de revient du dispositif.

Dans ce dernier cas, du fait de la relative simplicité d'un effacement de la zone Z_T de la mémoire par ultraviolet, on utilise certains des q bits de contrôle pour réaliser un marquage, (par exemple deux d'entre eux B_{M1} et B_{M2} avec $B_{M1} = B_{M2} = 1$), des mots de la zone Z_T, après l'effacement de cette zone Z_T par une banque, de façon à permettre la détection d'éventuels effacements globaux frauduleux. Ce marquage ne peut bien entendu être réalisé que sous le code banque.

Plus généralement, l'ensemble des composants et circuits compris dans la carte sont disposés directement ou indirectement sur un support tel qu'une carte de circuit imprimé, ce support étant lui-même noyé dans un matériau étanche ou inséré dans un boîtier étanche, par exemple en matière plastique. Les divers accès à la carte en entrée et en sortie tels qu'alimentation, horloge, échange de données ou d'adresses mémoire, effacement électrique éventuel de la mémoire etc. pouvant se faire par voie de contact électrique. Toutefois, pour mieux préserver le caractère d'étanchéité de la carte, tous les accès en entrée et en sortie peuvent se faire par voie électromagné-

tique en prévoyant sur le support des bobines plates destinées à recevoir de l'extérieur un champ magnétique approprié. Divers moyens pourront être utilisés pour réduire le nombre de ces bobines, par exemple en utilisant des procédés de multiplexage ou en utilisant la fréquence du signal d'alimentation comme signal d'horloge.

La figure 3 est le schéma général du procédé selon l'invention.

La première étape (bloc repéré 1 sur la figure) est la mise en relation du dispositif portatif avec le système informatique avec lequel il est appelé à coopérer, c'est-à-dire dans le cadre décrit précédemment, l'insertion de la carte dans le terminal.

Lors de la seconde étape, repérée 2 sur la figure, il est procédé à la reconnaissance du porteur de la carte, c'est-à-dire au test de la validité du code que le porteur fournit au terminal, qui lui-même le transmet à la carte, par comparaison de ce code fourni extérieurement avec une information contenue dans la partie ineffaçable de la mémoire ; cette comparaison s'effectue entièrement de façon interne à la carte. Le déroulement de cette étape est décrit plus amplement figure 4.

L'étape suivante, référencée 3 sur la figure, consiste à rechercher dans la mémoire M de la carte une adresse (A_1) qui soit disponible (de préférence, la première) pour enregistrer les informations relatives à la transaction en cours, et inscrire à cette adresse A_1 notamment l'information de validité fournie par l'étape précédente ; plus généralement, lors de cette étape s'effectue le traitement des erreurs

détectées dans la transaction en cours ou déjà enregistrées en mémoire.

L'étape suivante (4) est celle de l'accès à la mémoire M du dispositif par le terminal, afin de réaliser la transaction considérée, à savoir écriture d'une transaction à l'adresse A_1 ou lecture d'une information précédemment enregistrée, à une adresse A_2. Il est à noter que, d'après ce qui précède, une erreur de code interdit toute transaction ultérieure sur le mot situé à l'adresse A_1.

Le procédé se termine par une étape 5 qui peut être la restitution de la carte par le terminal au porteur, ou la conservation de cette carte par le terminal en cas par exemple de détection de certaines erreurs, etc.

Lors de la phase d'initialisation du dispositif, l'étape 3 n'est pas réalisée, selon un mécanisme détaillé plus loin, ce qui est schématisé sur la figure par une flèche 6.

La figure 4 représente de façon plus détaillée un mode de réalisation de l'étape 2 de la figure 3. Elle sera décrite en faisant référence au schéma du dispositif de la figure 1.

Après l'étape 1 de la figure 3, intervient une étape 21 pendant laquelle le terminal envoie à la carte l'adresse (A_1), connue de ce dernier, où se trouve dans la mémoire M le code confidentiel du porteur. Cette adresse, reçue sur l'entrée 10 (figure 1) est transmise au registre R_A par l'intermédiaire successivement de l'interface I et du registre à décalage R_D. Dans une variante de réalisation, dans le cas où, comme décrit figure 2, les codes confidentiels (banque ou porteur) se trouvent au début de la mémoire

M, seul est pris en compte le bit de poids le plus faible, les autres étant forcés à zéro : en effet, un seul bit est suffisant pour distinguer un code banque d'un code porteur, et cette procédure permet par ailleurs d'éviter certains risques de fraudes, seuls les codes banque ou porteur pouvant alors être adressés. Le registre d'adresses R_A transmet cette adresse au sélecteur S, ce qui provoque (étape 22) la sortie de la mémoire du code considéré, en direction du registre à décalage R_D, lequel transmet le code au comparateur C.

Parallèlement (étape 25), le porteur fournit au terminal son code et le terminal le transmet au comparateur C par l'intermédiaire de l'entrée 10 et de l'interface I.

L'étape suivante (23) consiste en la comparaison à l'intérieur du comparateur C des deux codes ainsi reçus, l'un provenant de l'extérieur et l'autre de la mémoire M interne à la carte. Le résultat de la comparaison est, dans l'étape suivante (24), mémorisé par le bistable B, qui marque la fin de l'étape 2.

Dans une variante de réalisation se déroule, parallèlement à la comparaison de l'étape 23, une détection d'erreurs sur le code interne, c'est-à-dire celui qui est enregistré à l'adresse A_1 dans la mémoire M, tel qu'un effacement de bits par exemple. Cette détection peut être réalisée par exemple à l'aide d'un bit de parité ou de deux bits somme modulo 4, ces bits étant prélevés sur les $\underline{m}$ bits restant alloués au code lui-même, en dehors des $\underline{q}$ bits de contrôle. Cette détection peut être réalisée par exemple par un sommateur réalisant l'addition des bits

du code interne (étape 26) qui provoque le positionnement d'un ou plusieurs bistables (étape 27). La structure correspondante, non représentée sur la figure 1, est constituée par un additionneur et un ou plusieurs bistables connectés en parallèle avec le comparateur C et le bistable B.

La figure 5 représente de façon détaillée un mode de réalisation de l'étape 3 de la figure 3, c'est-à-dire la recherche d'une adresse (A_2) dans la mémoire M qui soit disponible pour l'enregistrement d'informations relatives à la transaction en cours.

Après l'étape 2 de la figure 1 est réalisée une étape 31 d'incrémentation du registre d'adresses R_A par le circuit de commande L.

L'étape suivante (32) est le test de l'un des bits de contrôle (B_T sur la figure 2) du mot situé à l'adresse contenue actuellement dans le registre R_A : ce mot est en effet transmis au circuit L qui réalise les différentes opérations de test des q bits de contrôle. Le bit B_T est par exemple égal à $\overline{1}$ lorsque le mot correspondant contient déjà une information et il est à zéro dans le cas contraire. Si le test indique que le bit B_T est égal à 1, l'incrémentation du registre R_A par le circuit de commande L se poursuit jusqu'à ce qu'un bit B_T égal à zéro soit détecté. A ce moment, le registre R_A conserve sa valeur, notée A_2.

Parallèlement à l'étape 31 d'incrémentation du registre R_A, on réalise (étape 35) dans le circuit L le test et le comptage des bits de contrôle B_C égaux à 1, bits sur le rôle desquels on revient ci-après.

En ce qui concerne le traitement des erreurs

précédemment détectées dans un premier temps (étape 33 sur la figure 5), le contenu du bistable B est recopié à l'emplacement de l'un des bits de contrôle, repéré B_C, situé à l'adresse considérée (A_2). On rappelle que le bistable B contient le résultat de la comparaison des codes interne et externe, c'est-à-dire l'indication d'une éventuelle erreur de code. Une différence entre les deux codes se traduit par un changement d'état du bit B_C (il devient par exemple égal à 1) et l'absence d'erreur par aucun changement d'état du bit B_C (zéro). Dans tous les cas, le contenu du bistable est écrit dans la mémoire M, à l'adresse A_2, ce qui présente un avantage sur le plan de la sécurité : en effet, une détection extérieure par exemple par observation de variations de tension d'alimentation, est alors impossible. Par ailleurs, cette solution est plus simple sur le plan technologique du fait qu'il n'est pas nécessaire de tester le contenu du bistable B avant toute écriture.

C'est donc l'existence de telles erreurs de codes qui est détectée lors de l'étape 35 par le circuit L.

Par ailleurs, afin d'interdire toute écriture ultérieure dans un mot où une erreur de code a été inscrite, il est possible soit de faire changer d'état le bit B_T en même temps que la recopie du bit B_C (étape 33) lorsque celui-ci indique une erreur, soit, lors de la recherche d'une zone libre, de tester à la fois B_T et B_C.

L'étape suivante (34) consiste à tester la valeur des bits de marquage B_{M1} et B_{M2} décrits figure 2. Lors de cette étape est également réalisé le test des bistables correspondant à la détection

des erreurs du code interne décrite figure 4.

Ces différents résultats de test sont mémorisés par le circuit logique de commande L, qui autorise ou n'autorise pas le transfert d'informations de la carte vers le terminal, dans une étape 36 : le transfert d'informations contenues dans la mémoire M n'est pas autorisé lorsque le test des bits de marquage est négatif, ou lorsque le nombre d'erreurs de code est trop grand, c'est-à-dire supérieur à un seuil pré-défini, les erreurs prises en compte étant consécutives ou non, etc. Dans le cas contraire, le circuit de commande L autorise le transfert du contenu du registre R_A, c'est-à-dire l'adresse A_2, vers le terminal par l'intermédiaire du registre à décalage R_D, de l'interface I et de la borne 10.

Dans une variante de réalisation, lorsque le circuit L arrête la transaction en cours à cause des erreurs détectées, celui-ci adresse un message au terminal indiquant éventuellement la ou les erreurs détectées.

A ce moment, qui marque la fin de l'étape 3 de la figure 3, le terminal a accès à la mémoire de la carte.

Il est à noter que l'adresse A_2 est donc obtenue par des incrémentations successives du registre R_A à partir de l'adresse A_1 du code, ce qui présente des avantages tant sur le plan de la simplicité technologique que sur le plan de la sécurité de fonctionnement.

La figure 6 représente plus en détails un mode de réalisation de l'étape 4 de la figure 3.

La première phase (41) consiste en l'envoi par le terminal à la carte, de l'adresse (A_3) de la

mémoire M à laquelle le terminal désire accéder, cette adresse étant soit une adresse où on désire faire une lecture, soit l'adresse A_2 fournie par la carte dans la phase précédente, dans le cas où on désire faire une écriture en mémoire.

Cette adresse A_3 est fournie dans une étape 43 à la mémoire M par l'intermédiaire de l'interface I, du registre à décalage R_D et du registre d'adresses R_A. Dans l'étape suivante (44), la mémoire M fournit l'ensemble des q bits de contrôle présents à cette adresse au circuit de commande L, et notamment les bits de contrôle d'accès B_{A1} et B_{A2}.

Parallèlement, le terminal fournit à la carte un ordre d'écriture ou de lecture, suivi dans le cas de l'écriture par l'information à enregistrer en mémoire. Le code écriture ou lecture est transmis au circuit de commande L par le registre R_D dans une étape 42 ; une étape 45 représente l'autorisation ou la non autorisation du transfert demandé en fonction de la valeur des bits de contrôle d'accès correspondants, fournis par l'étape 44. Si l'opération envisagée est interdite, celle-ci n'est pas effectuée par commande du circuit L. A cette interdiction peut s'ajouter, dans une variante de réalisation, l'envoi d'une information provenant du circuit de commande L vers le terminal, par l'intermédiaire du registre à décalage R_D, explicitant l'interdiction. Cela est illustré sur la figure par un bloc 46.

Dans le cas où la comparaison 45 montre que l'opération envisagée est autorisée, celle-ci est réalisée dans l'étape 47 par l'écriture ou la lecture à l'adresse A_3 indiquée dans le registre R_A, étant entendu que dans le cas d'une écriture, le terminal

fournit une information qui transite par le registre à décalage R_D (étape 48).

La figure 7 représente une variante de réalisation de l'invention dans laquelle le décodage des informations par le circuit de commande (L) est réalisé à l'aide d'une logique combinatoire.

Sur cette figure, on a représenté, pour rester dans le cadre de l'exemple précédent, huit informations d'entrée du circuit L, à savoir les six bits de contrôle B_{A1}, B_{A2}, B_{M1}, B_{M2}, B_C et B_T, ainsi qu'un signal binaire L identifiant un ordre de lecture ou d'écriture, et un signal C identifiant la nature du code de l'utilisateur : code du porteur ou code de la banque. Le circuit logique décrit à titre d'exemple figure 7 correspond aux conventions suivantes :

- $B_T = 0$: zone de transaction libre ;
- $B_C = 1$: erreur de code ;
- $L = 1$: ordre de lecture ;
- $C = 1$: code banque ;
- $B_{M1} = B_{M2} = 1$: marquage correct ;
- $B_{A1} = B_{A2} = 0$: lecture ou écriture uniquement par la banque ;

  $B_{A1} = 1$ et $B_{A2} = 0$: lecture ou écriture par la banque ou le porteur ;

  $B_{A1} = 0$ et $B_{A2} = 1$

  $B_{A1} = B_{A2} = 1$: écriture ou lecture interdites.

Le circuit de la figure 7 fournit un signal A, égal à 1 lorsque l'opération de transfert est autorisée, qui obéit à l'équation logique suivante :

$$A = \overline{B_{A2}} \cdot (\overline{B_T} + L) \cdot (\overline{B_C} + L) \cdot (B_{M1} \cdot B_{M2} + L + C) \cdot (B_{A1} + C)$$

A cet effet, le circuit de la figure 7 est

constitué de la façon suivante : les bits B_{A2}, B_T et B_C sont chacun inversés à l'aide des inverseurs 71, 72 et 73 respectivement ; une porte logique ET 74 réalise l'opération correspondante sur les bits B_{M1} et B_{M2} ; des portes logiques OU 75, 76, 77 et 78 réalisent les opérations correspondantes respectivement sur :

- le bit B_T inversé et le bit L ;
- le bit B_C inversé et le bit L ;
- les bits C et L et le résultat de l'opération $(B_{M1}.B_{M2})$;
- les bits C et B_{A1} ;

Une porte logique ET 79 réalise l'opération correspondante sur le bit inversé B_{A2} et les signaux fournis par les portes 75 à 78 ; la porte 79 fournit le signal A.

Quel que soit le mode de réalisation du circuit logique de commande, lors de la phase d'initialisation de la carte pendant laquelle la partie ineffaçable de la mémoire est enregistrée, les q bits de contrôle de tous les mots, comme les m autres bits, sont à zéro : il n'y a alors aucune restriction d'accès pour toute la mémoire. Le code utilisé est alors égal à zéro, avec des bits B_{A1} et B_{A2} égaux à zéro, ce qui signifie conventionnellement que l'étape 3 de la figure 3 ne doit pas se dérouler.

Enfin, il est à noter que toutes les opérations décrites ci-dessus en faisant référence au code du porteur de la carte se déroulent de façon analogue dans le cas où l'utilisateur du dispositif est la banque elle-même, en remplaçant le code porteur par le code banque.

REVENDICATIONS

1. Dispositif électronique de mémorisation et de traitement confidentiel d'informations destiné à coopérer avec un système informatique comportant un terminal, ce dispositif comportant au moins une mémoire et des moyens d'adressage de cette mémoire, et étant caractérisé par le fait que la mémoire (M) comporte au moins une zone ineffaçable (Z_I) dans laquelle sont enregistrés des éléments d'identification de l'utilisateur du dispositif et une zone (Z_T) dans laquelle sont enregistrées successivement les transactions effectuées, ces deux zones étant chacune organisées en mots, chacun des mots comportant un nombre q de bits réservés au contrôle ; que les moyens d'adressage (R_A) réalisent l'adressage de cette mémoire M en écriture ou en lecture, sous le contrôle d'une part des éléments d'identification et d'autre part des bits de contrôle ;
le dispositif comportant en outre :
- des moyens d'interface (I) assurant le couplage électrique entre le terminal et le dispositif ;
- un comparateur (C) recevant d'une part des informations en provenance de la mémoire (M) et d'autre part des informations en provenance de l'extérieur, afin de réaliser des opérations de reconnaissance de l'utilisateur, fournissant le résultat de la comparaison à un élément de mémoire (B) ;
- des moyens logiques de commande et de synchronisation (L) des éléments ci-dessus, recevant les bits de contrôle et le contenu de l'élément mémoire (B).

2. Dispositif selon la revendication 1, caractérisé par le fait que la mémoire (M) est une

mémoire à semiconducteurs dont la zone de transactions (Z_T) est effaçable.

3. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que les q bits de contrôle comportent au moins deux bits de conditions d'accès (B_{A1}, B_{A2}) pour caractériser l'utilisateur (porteur ou banque) du dispositif et la nature du transfert autorisable (écriture ou lecture), au moins un bit de marquage (B_M), au moins un bit de transaction (B_T) dont la valeur indique l'état disponible ou inscrit du mot mémoire correspondant et un bit d'erreur de code (B_C), indiquant une éventuelle erreur dans les éléments d'identification.

4. Dispositif selon l'une des revendications précédentes, caractérisé par le fait qu'il comporte de plus un registre à décalage (R_D) connecté entre la sortie de la mémoire (M), l'interface (I), les moyens d'adressage qui comportent un registre d'adresses (R_A) et le comparateur (C).

5. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que l'élément de mémoire (B) est distinct de la mémoire (M), et qu'il est constitué par un élément bistable.

6. Dispositif selon l'une des revendications précédentes, caractérisé par le fait que les moyens logiques de commande (L) comportent des portes logiques ET et OU, réalisant la combinaison logique des bits de contrôle, du contenu de l'élément mémoire (B), d'un signal binaire (L) indiquant la nature du transfert demandé (écriture ou lecture) et d'un signal binaire (C) indiquant la nature de l'utilisateur (porteur ou banque), et fournissant, selon le résultat de la combinaison, un signal (A) d'autorisation ou d'inter-

diction de la transaction considérée.

7. Procédé de mémorisation et de traitement confidentiel d'informations à l'aide d'un dispositif électronique portatif selon l'une des revendications précédentes, en relation avec un système informatique comportant un terminal, caractérisé par le fait qu'il comporte les étapes suivantes :

- le test (2) de la validité d'un code fourni au dispositif par le terminal, sur commande extérieure, par comparaison de ce code extérieur avec un code interne contenu dans la zone ineffaçable (Z_I) de la mémoire (M) du dispositif, cette comparaison s'effectuant entièrement de façon interne au dispositif et fournissant une information interne sur la validité du code extérieur ;
- la recherche (3) d'une adresse (A_2), dans la mémoire (M) du dispositif, qui corresponde au premier mot disponible pour l'enregistrement d'informations relatives à la transaction en cours, et l'inscription à cette adresse notamment de l'information de validité ;
- lorsque l'information de validité l'autorise, l'accès à la mémoire du dispositif (4) afin de réaliser la transaction considérée.

8. Procédé selon la revendication 7, caractérisé par le fait que l'étape de test (2) comporte les étapes suivantes :

- l'envoi (21) du terminal vers le dispositif de l'adresse (A_1) du code interne ;
- le transfert (22) de la mémoire (M) vers le comparateur (C) du code interne ;
- le transfert (25) du terminal vers le comparateur (C) du code extérieur ;

- la comparaison (23) des codes interne et extérieur, fournissant l'information de validité ;
- la mémorisation de l'information de validité dans l'élément de mémoire (B).

9. Procédé selon la revendication 8, caractérisé par le fait que le code dont est testée la validité est soit un code porteur, soit un code banque, ces deux codes étant inscrits au début de la mémoire (M) du dispositif, et que le procédé comporte de plus, après l'étape d'envoi (21) de l'adresse (A_1) du code interne, une étape de forçage à zéro de tous les bits constituant cette adresse, sauf le bit de poids le plus faible.

10. Procédé selon la revendication 3 et l'une des revendications 7 et 8, caractérisé par le fait que l'étape de recherche d'une adresse (3) comporte les étapes suivantes :
- l'incrémentation (31) pas à pas des moyens d'adressage (R_A) ;
- le test (32) de celui (B_T) des bits de contrôle dont la valeur indique l'état disponible ou inscrit du mot mémoire correspondant ;
- dans le cas où le test précédent (32) indique l'état d'inscription du mot mémoire correspondant, le test et le comptage (35) de celui (B_C) des bits de contrôle dont la valeur indique une erreur de code précédente, et la reprise du procédé à l'étape d'incrémentation (31) ;
- dans le cas où le test précédent (31) indique l'état de disponibilité du mot mémoire correspondant, l'inscription du contenu de l'élément de mémoire (B) à l'emplacement de celui (B_C) des bits de contrôle dont la valeur indique une erreur de code ;

- le test des bits de marquage (B_M) ;
- la transmission au terminal de l'adresse (A_2) obtenue précédemment dans le cas où les tests des bits de contrôle opérés précédemment autorisent la transaction.

11. Procédé selon l'une des revendications 7 à 10, caractérisé par le fait que l'étape (4) d'accès à la mémoire (M) comporte les étapes suivantes :

- la transmission (41) par le terminal d'une adresse (A_3) de mémoire (M) qui est soit identique à celle qui est fournie par l'étape (3) de recherche d'une adresse (A_2) dans le cas où la transaction considérée entraîne une écriture en mémoire, soit différente dans le cas où la transaction entraîne une lecture ;
- la transmission (44) des bits de contrôle du mot mémoire correspondant aux moyens de commande (L) ;
- l'émission (42) par le terminal d'un ordre de lecture ou d'écriture en mémoire à l'adresse (A_3) considérée, suivi dans le cas d'une écriture par la transaction à mémoriser ;
- l'autorisation ou la non autorisation (45) par les moyens de commande (L) de la nature de l'ordre demandé à celle qui est autorisée par les bits de contrôle ;
- l'exécution (47) de l'ordre dans le cas où il est autorisé.

FIG. 1

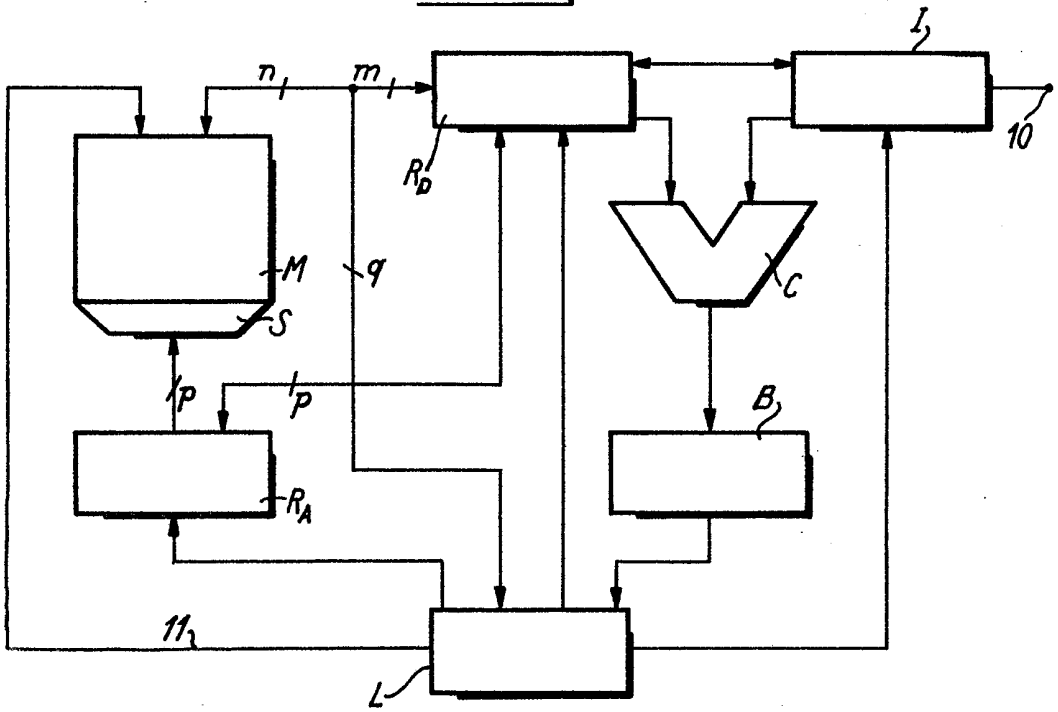

I
n
m
10
R_D
M
q
S
C
P
P
B
R_A
11_1
L

FIG. 2

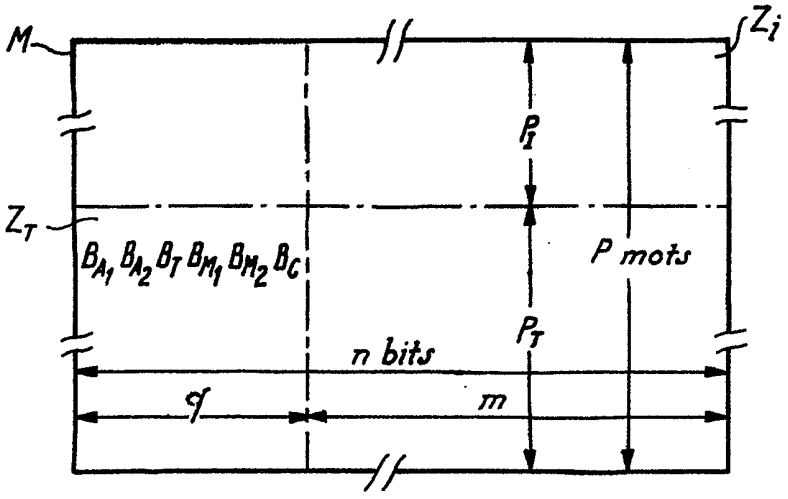

M
Z_i
P_I
Z_T
B_{A_1} B_{A_2} B_T B_{M_1} B_{M_2} B_C
P mots
P_T
n bits
q
m

FIG. 3

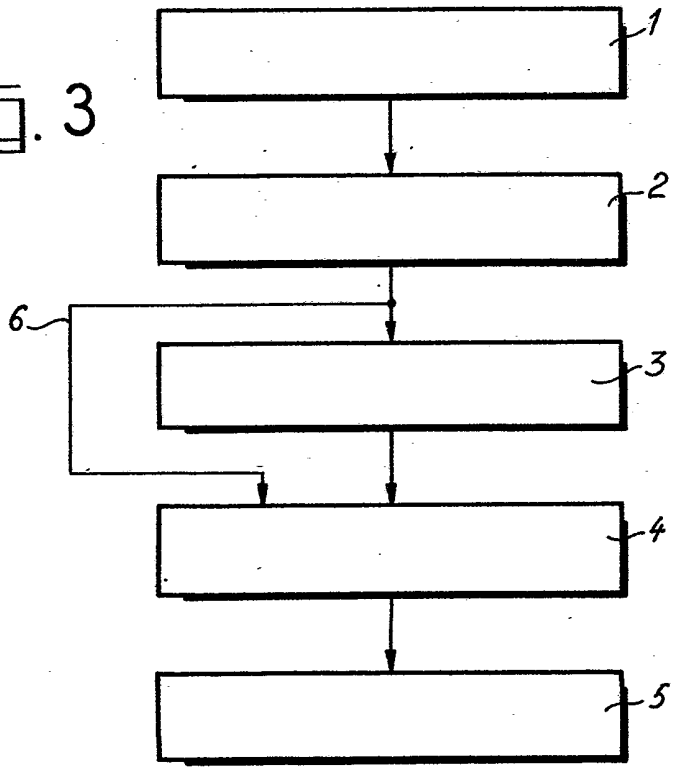
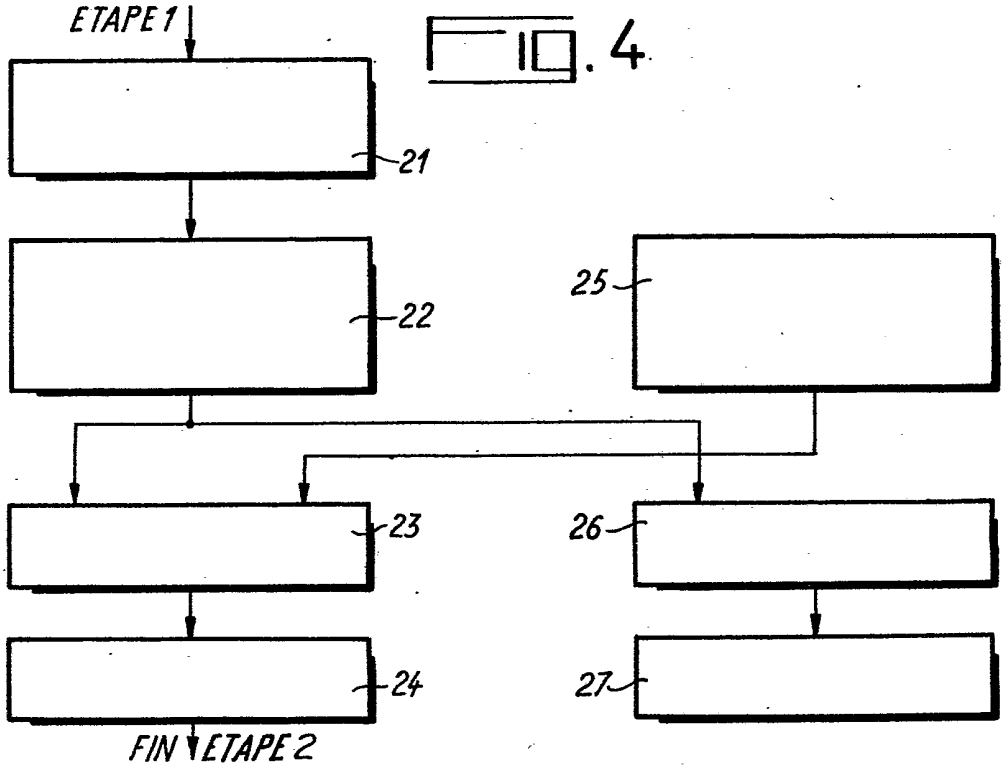


FIG. 4



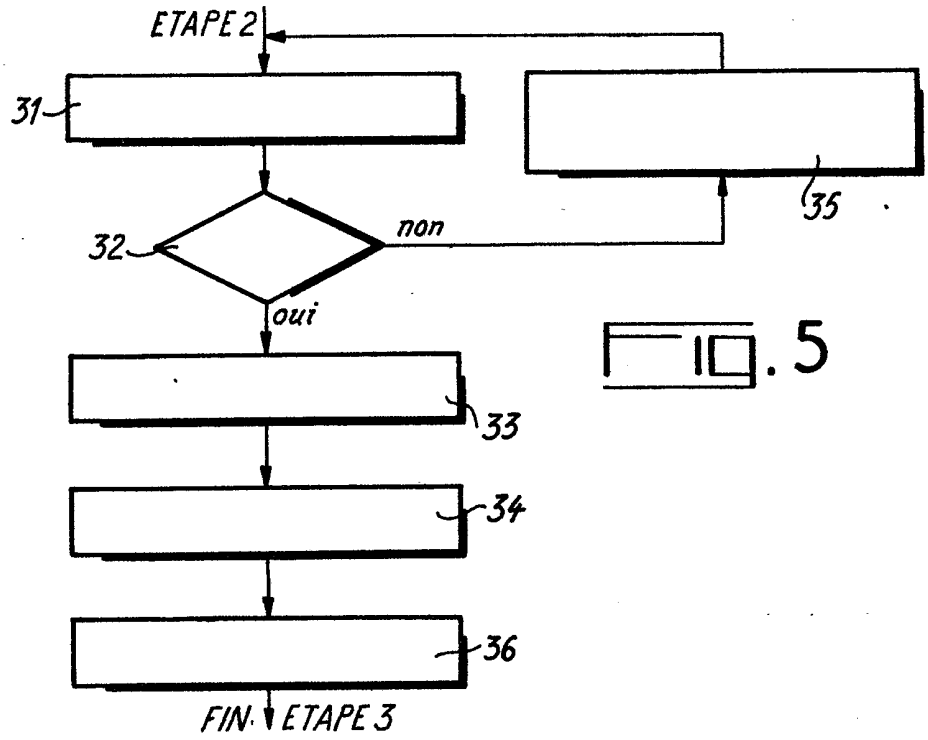

ETAPE 2
31
35
32
non
oui
33
34
36
FIN ETAPE 3

FIG. 5

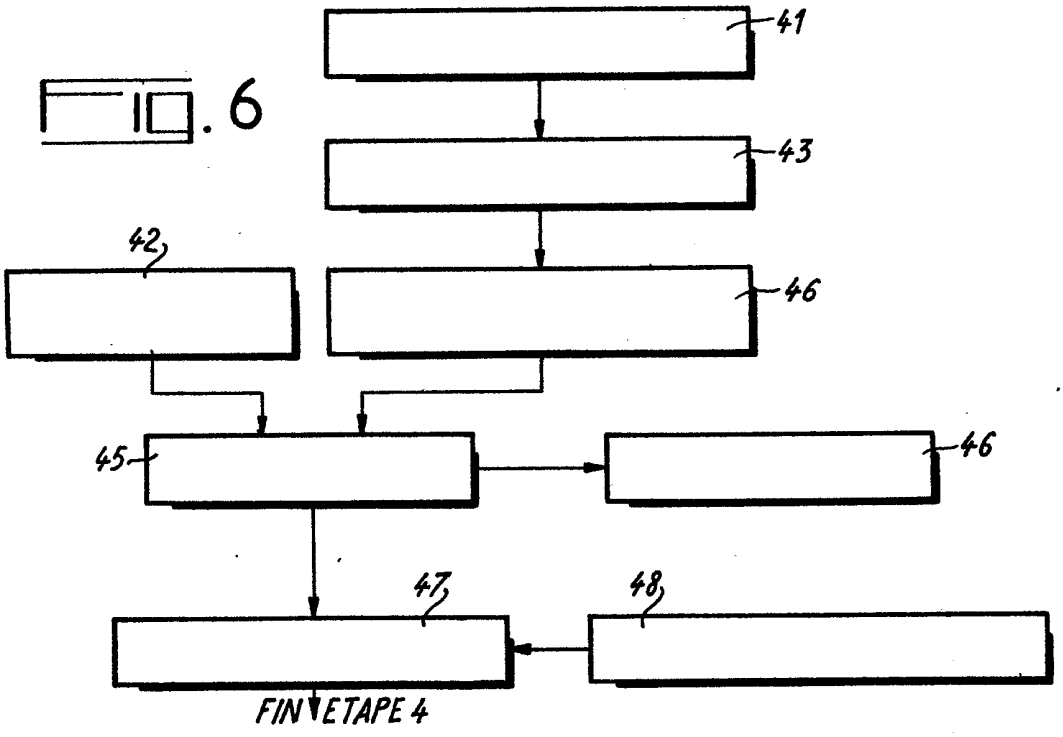

41
43
42
46
45
46
47
48
FIN ETAPE 4

FIG. 6

FIG.7

