

①9 RÉPUBLIQUE FRANÇAISE
—
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
—
PARIS
—

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

2 613 158

②1 N° d'enregistrement national :

88 03887

⑤1 Int Cl⁴ : H 04 L 9/02.

①2

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 24 mars 1988.

③0 Priorité : JP, 26 mars 1987, n° 73344/1987.

④3 Date de la mise à disposition du public de la
demande : BOPI « Brevets » n° 39 du 30 septembre 1988.

⑥0 Références à d'autres documents nationaux appa-
rentés :

⑦1 Demandeur(s) : Société dite : MITSUBISHI DENKI KA-
BUSHIKI KAISHA. — JP.

⑦2 Inventeur(s) : Kenichi Takahira.

⑦3 Titulaire(s) :

⑦4 Mandataire(s) : Cabinet Weinstein.

⑤4 Procédé et système de transmission d'informations.

⑤7 L'invention comprend un procédé pour utiliser une carte de circuit intégré IC pour transmettre une information entre deux endroits et pour limiter l'accès à l'information seulement à des utilisateurs autorisés.

Ce procédé est caractérisé en ce qu'il comprend les opérations d'entrer ladite information dans une première mémoire d'un système à base de microprocesseur comprenant un premier microprocesseur qui empêche le transfert des contenus de ladite première mémoire audit moyen de lecture/écriture ou enregistrement en réponse à un mot de passe lu prédéterminé stocké dans ladite première mémoire; de présenter un premier mot de passe audit premier microprocesseur pour permettre le transfert de ladite information audit moyen de lecture/écriture; de transférer ladite information de ladite première mémoire audit moyen de lecture/écriture seulement lorsque ledit premier mot de passe coïncide avec le mot de passe lu prédéterminé stocké dans ladite mémoire; de diriger ladite information transférée audit moyen de lecture/écriture à un dispositif de reproduction; et de reproduire ladite information.

L'invention est utilisable pour la transmission d'informations confidentielles.

FR 2 613 158 - A1

D

L'invention concerne des cartes de circuits intégrés et plus particulièrement un système utilisant des cartes de circuits intégrés pour transmettre des informations sûres d'un utilisateur autorisé à un autre.

5 Traditionnellement, des informations commerciales hautement confidentielles ou sensibles ont été transférées d'une zone protégée à une autre à l'aide de documents scellés ou de courriers spéciaux. Plus récemment, des ordinateurs ont été utilisés pour
10 transférer des grands volumes d'informations confidentielles entre deux zones protégées, en utilisant un moyen de transmission tel que des lignes téléphoniques.

Bien qu'un joint de données électroniques
15 joignant deux zones protégées est hautement efficace pour assurer un accès limité aux informations transférées, ceci ne constitue pas une solution pratique pour toutes les situations exigeant un transfert sûr d'informations confidentielles. Par exemple la connexion par ordinateur
20 ou informatique est rigide et n'est pas mobile avec un utilisateur autorisé dont le travail quotidien implique des voyages entre différents endroits. Un autre exemple est une personne qui, pendant le déroulement normal des affaires reçoit seulement des faibles volumes
25 d'informations sensibles ou confidentielles sur une base sporadique et ne peut pas justifier les dépenses de se procurer une zone protégée à base d'ordinateur pour recevoir les informations. Pour cette personne l'information confidentielle est typiquement délivrée
30 dans des enveloppes scellées par des courriers spéciaux. Malheureusement, indépendamment de la manière de laquelle l'information dans l'enveloppe est enregistrée (c'est-à-dire imprimée sur papier ou contenue dans un milieu électronique tel qu'un disque électronique) il est
35 susceptible d'un accès non autorisé par la simple

ouverture de l'enveloppe et la lecture de l'information, soit visuellement soit électroniquement. Si l'information est enregistrée sur un disque magnétique il peut simplement être mis dans un poste de commande et en
5 utilisant un système de commande appropriée, les données peuvent devenir accessibles même si elles sont mises en format pour compléter un système d'opération particulier qui permet seulement un accès limité aux données du disque. Il y a par conséquent un besoin pour
10 un système de transfert d'information protégé qui ne peut pas être facilement rompu par une programmation spéciale de dispositifs de lecture et d'enregistrement. Plus généralement, il y a un besoin pour un système qui livre
15 des informations confidentielles à des utilisateurs autorisés dans des environnements qui ne se prêtent eux-mêmes pas à l'application de connexions de données électroniques reliant des zones protégées.

En raison de ce qui précède, un premier objet de la présente invention est de proposer un système de
20 transmission d'informations qui est comparativement peu cher, polyvalent et qui assure un haut degré de sécurité pour les informations pendant leur transfert.

Un objet encore plus particulier de la présente invention est de proposer un milieu pour enregistrer des
25 informations sensibles ou confidentielles de telle façon que l'information ne peut pas être lue par une personne non autorisée indépendamment de qui est en possession physique de ce milieu.

L'objet spécifique de l'invention est de
30 proposer un système et un procédé utilisant au moins une carte de circuit intégré pour transmettre des informations entre deux endroits et limiter l'accès à l'information seulement à un utilisateur autorisé, où l'information contenue dans la carte de circuit intégré
35 est accessible seulement après qu'un microprocesseur

incorporé à la carte de circuit intégré ait été adapté à une entrée d'un mot de passe par l'utilisateur avec un mot de passe stocké intérieurement. En réponse à la détection d'une correspondance entre les mots de passe
5 entré et stocké, le microprocesseur transfère l'information enregistrée d'une mémoire intégrée ou incorporée à un dispositif de reproduction qui peut soit être une partie intégrale de la carte ou un dispositif extérieur, qui reçoit l'information par voie d'une
10 interface ou jonction du type lecteur/enregistreur entre la carte et le dispositif de reproduction.

Un autre objectif spécifique de l'invention est l'utilisation d'une connexion de données électroniques dans des applications qui exigent un transfert rapide de
15 l'information sensible ou confidentielle. Lorsqu'il est utilisé en liaison avec une connexion de données, le mot de passe est préférablement complété par une clé d'encodage et de décodage qui est seulement connue par les utilisateurs autorisés et entrée dans la carte de
20 circuit intégré de façon à chiffrer ou déchiffrer l'information. Pendant son transfert sur une connexion de données, l'information est en un format chiffré qui n'est pas susceptible d'une traduction facile lorsqu'elle est interceptée.

25 Selon encore un autre objectif spécifique de l'invention, en permettant à l'utilisateur de chaque accès par mot de passe d'accéder seulement à des parties limitées de la mémoire, une pluralité d'émetteurs autorisés et de récepteurs peuvent partager la même
30 carte, mais n'ont pas la même information.

L'invention sera mieux comprise et d'autres buts, caractéristiques, détails et avantages de celle-ci apparaîtront plus clairement au cours de la description explicative qui va suivre faite en référence aux dessins

schématiques annexés donnés uniquement à titre d'exemple illustrant plusieurs modes de réalisation de l'invention et dans lesquels :

5 - la figure 1 est un schéma bloc d'un système de transmission d'informations selon un premier mode de réalisation de l'invention ;

10 - la figure 2 est un organigramme d'un programme de contrôle ou de commande pour un système à base de microprocesseur incorporé à une carte de circuit intégré d'un système de transmission d'informations ;

- la figure 3 est un schéma bloc d'un mode de réalisation alternatif de l'invention, utilisant le système illustré à la figure 1 pour accomplir une connexion de données électroniques ;

15 - la figure 4 est un schéma bloc d'un autre mode de réalisation alternatif de l'invention, où les dispositifs d'entrée et de reproduction pour le système de transmission d'informations selon l'invention forment les parties intégrales de la carte de circuit intégré ;

20 - la figure 5 est une représentation picturale de la carte de circuit intégré selon le mode de réalisation alternatif de la figure 4 ; et

- la figure 6 est une représentation schématique d'une mémoire incorporée à une carte de circuit intégré, où le champ des emplacements de mémoire est divisé en une pluralité de blocs, chacun isolé des autres pour l'utilisation par de multiples utilisateurs autorisés.

25 En se référant aux figures et tout d'abord à la figure 1, un dispositif de lecture/enregistrement conventionnel 11 est montré sous forme d'un système à base de microprocesseur auquel est incorporé un microprocesseur 13, une mémoire morte (ROM) 15 et une mémoire vive (RAM) 17 selon une architecture
30 conventionnelle définie par le bus 19. Egalement de façon

bien connue dans la technique, le dispositif de lecture/enregistrement 11 comprend une interface ou zone de jonction 21 pour permettre à l'utilisateur du dispositif de lecture/d'enregistrement de communiquer avec une carte de circuit intégré 23. Pour que l'utilisateur puisse transmettre et recevoir des informations à une carte de circuit intégré 3 où en provenance d'une telle carte, les dispositifs de visualisation ou de reproduction et de clavier 25 et 27 sont en communication avec une carte de circuit intégré à travers un dispositif d'attaque 29 et un tampon d'entrée 31, respectivement, contenu dans le dispositif de lecture/d'enregistrement 11.

L'information est reçue par la carte de circuit intégré 23, depuis le dispositif de lecture/d'enregistrement 11 à travers une jonction ou interface incorporée conventionnelle qui est complémentaire à l'interface 21 du dispositif de lecture/d'enregistrement. De la jonction 33, les données sont communiquées à un système à base de microprocesseur sur la carte de circuit intégré 23 à travers un bus entrée/sortie (I/O) 42. Le système à base de microprocesseur comprenant un microprocesseur 35 incorporé à la carte de circuit intégré ou IC 23 répond à un programme de commande 37a contenu dans une mémoire ROM 37 pour traiter, stocker, transmettre et recevoir des informations. Pour pouvoir lire ou écrire dans le système à base de microprocesseur, l'architecture du système selon la figure 1 exige que les données passent à travers le microprocesseur 35. Pour stocker les données, le système comprend aussi une mémoire RAM 39 incorporée à la carte IC 23 qui répond à des commandes du microprocesseur 35. Le programme de commande 37a du microprocesseur 35 divise la mémoire RAM 39 en des champs de mémoire fixe et variable respectivement 39a et 39b. L'information dans le champ ou secteur fixe 39a ne peut pas être fournie au bus

I/O 42 à travers le microprocesseur 35. Pour garantir une sécurité maximale, le champ fixe 39a peut être pré-programmé par le fabricant. Cependant le champ fixe est préférablement programmé par l'utilisateur initial, 5 comme cela sera expliqué ci-après.

Selon un aspect important de l'invention, le champ de mémoire fixe 39a de la mémoire RAM 39 de la carte IC 23 comprend un mot de passe lu qui doit correspondre à un mot de passe entrée dans la carte IC à 10 l'aide du clavier 27 à travers des moyens de lecture/écriture ou d'enregistrement (par exemple le dispositif de lecture/d'enregistrement 11 et le bus I/O 42) avant que l'information contenue dans le champ variable 39b de la mémoire RAM puisse être transférée par 15 le microprocesseur 35 au moyen de lecture/d'enregistrement pour être visualisée ou reproduite pour l'utilisateur au moyen du dispositif de représentation ou de visualisation 25. Bien que le bus de commande/données 41 reliant le microprocesseur 35, la mémoire ROM 37 et la 20 mémoire RAM 39 soit classique, le microprocesseur, sous l'effet de la commande du programme de commande 37a normalement empêche la lecture de l'information dans le champ de mémoire variable 39b de la mémoire RAM, dans la RAM au moyen de lecture/d'enregistrement. Le programme de 25 commande 37a fonctionne comme système actif pour le système à base de microprocesseur incorporé qui ignore où est isolé de toutes les entrées externes tant que le mot de passe correct n'ait pas été présenté. De ce fait l'accès à l'information contenue dans le champ de mémoire 30 variable 39b n'est seulement accessible à un utilisateur ayant connaissance indépendante du mot de passe lu. De façon préférée, le mot de passe lu est entré par un utilisateur initial et ensuite isolé de tous les accès

externes au moyen d'opérations appropriées et bien connues, dans le programme de contrôle 37a pour limiter l'accès au champ fixe 39a.

5 Pour entrer l'information dans le champ de mémoire variable 39b, le champ fixe 39a de la mémoire RAM 39 incorporé à la carte IC 23 comprend préférablement un mot de passe écrit pour écrire l'information dans la mémoire RAM aussi bien que le mot de passe lu pour la lecture de l'information dans celle-ci. Dans ce cas, le
10 champ fixe 39a de la RAM 39 comporte une section contenant un mot de passe écrit qui est placé dans la mémoire d'une manière similaire à celle du mot de passe lu.

En se référant à l'organigramme selon la figure
15 2 du programme de contrôle 37a, un utilisateur autorisé initial reçoit la carte IC et inscrit les mots de passe lu et écrit, qui sont placés par le microprocesseur 35 dans la mémoire de champ fixe 39a pendant l'opération A. Une fois les mots de passe inscrits, la structure du
20 programme de commande 37a et l'architecture du système à base de microprocesseur incorporées ne permettent pas l'accès des mots de passe par un utilisateur. Préférablement, après l'inscription des mots de passe, la carte IC est envoyée à un autre utilisateur autorisé.
25 Séparément, le mot de passe écrit est également envoyé à cet autre utilisateur.

Comme alternative, un système encore plus sûr peut être réalisé lorsque les mots de passe lu et écrit sont entrés dans le champ fixe 39a par le fabricant.
30 Lorsque chaque carte IC est distribuée, le fabricant notifie le mot de passe écrit à un émetteur ou expéditeur autorisé et le mot de passe lu à un récepteur ou destinataire autorisé. En rendant ainsi le système

complémentaire, aucun utilisateur autorisé connaît les deux mots de passe, ce qui procure une mesure supplémentaire de sécurité.

5 Selon l'invention, un utilisateur autorisé
ayant connaissance du mot de passe écrit soit par le fabricant ou par un utilisateur initial, présente le mot de passe à la carte IC 23 par l'intermédiaire des moyens de lecture/écriture ou d'enregistrement qui comprend le clavier 27, le dispositif de lecture/enregistrement 11 et
10 le bus I/O 42 sur la figure 1. Le microprocesseur 35 incorporé à la carte IC 23 lit le mot de passe pendant l'opération B et le compare à l'opération C au mot de passe écrit stocké dans la mémoire RAM 39. Lorsque la comparaison établit une concordance, le programme de
15 contrôle 39a avance à l'opération ou l'étape D où le microprocesseur 35 détermine si l'utilisateur souhaite lire ou écrire dans la mémoire 39. Puisque l'utilisateur a demandé un enregistrement des données, le programme de commande 39a exécute l'étape ou l'opération E. A l'étape
20 E, le microprocesseur 35 permet à l'utilisateur autorisé d'inscrire l'information dans la mémoire RAM 39 par l'intermédiaire du clavier 27. Avec l'information ainsi entrée, la carte IC 23 est retirée du dispositif de lecture/écriture ou enregistrement 11 et envoyée à
25 l'utilisateur qui a initialement inscrit les mots de passe pour lire l'information dans la carte IC. La carte IC peut être envoyée par tout service habituel tel qu'un courrier ordinaire ou par des services de courrier commercial.

30 Lorsque la carte IC 23 est reçue par l'utilisateur initial, il est inséré dans un lecteur/enregistreur conventionnel, comme cela est montré sur la figure 1. Pour avoir accès à l'information, le récepteur présente un mot de passe au microprocesseur 35
35 du système à base de microprocesseur sur la carte IC 23,

à l'aide du clavier 27, de l'interface 33 et du bus I/O 42. Quand à l'étape C le mot de passe présenté par le récepteur correspond au mot de passe lu qui a été préalablement stocké dans la mémoire RAM 39 incorporée à la carte IC 23, le microprocesseur 35 exécute les étapes ou opérations D et F en délivrant l'information contenue dans la mémoire RAM au bus I/O 42 pour la lecture par le dispositif de lecture/écriture 11. Le dispositif de lecture/écriture 11 transmet l'information au dispositif de reproduction 25 pour qu'elle soit visualisée pour l'utilisateur autorisé.

Après l'accès à l'information et sa visualisation, le récepteur peut devenir expéditeur ou émetteur en présentant d'abord au microprocesseur 35 intégré ou incorporé, par l'intermédiaire du dispositif de lecture/écriture 11, l'interface 33 et le bus I/O 42, un mot de passe qui est lu par le microprocesseur à l'étape B et mis en correspondance avec le mot de passe lu stocké dans la mémoire RAM 39 à l'étape C. Lorsqu'une coïncidence est déterminée à l'étape C, les données de l'information engendrées par le clavier 27 et présentées au microprocesseur sont entrées dans la mémoire RAM 39 à travers le bus I/O. Le récepteur devient maintenant émetteur et peut envoyer la carte IC avec sa nouvelle information soit à l'émetteur ou expéditeur initial à l'endroit où il se trouve ou l'envoyer au même émetteur à un endroit différent, où, le cas échéant, à un utilisateur autorisé complètement différent à un endroit différent.

Pour éviter la possibilité d'une utilisation d'un dispositif de saisie électronique (par exemple un générateur de nombre aléatoire) pour déverrouiller l'information contenue dans la carte IC, le programme de commande 37a peut comprendre une caractéristique d'exclusion à l'étape G qui ignore tout mot de passe

entré pendant une période de temps prédéterminée après l'inscription d'un mot de passe qui ne correspond pas au mot de passe mémorisé. Des caractéristiques d'exclusion programmables de ce type sont bien connues dans la technique et n'ont pas besoin d'être explicitées plus en détail.

Comme autre moyen pour protéger l'information contre un accès non autorisé, un enrichissement du système précédent comporte un programme 37b de codage/décodage de logiciel stocké dans la mémoire ROM 37 et incorporé comme partie du système actif pour le système à base de microprocesseur contenu dans la carte IC 23. Avec le programme de codage/décodage 37b, après qu'un utilisateur autorisé a inscrit le mot de passe correct, l'utilisateur entre une clé de code dans la carte IC 23 par l'intermédiaire du clavier 27. A l'intérieur de la carte IC, le microprocesseur 35 exécute le programme de codage/décodage 37b pour chiffrer l'information et ensuite la placer en mémoire dans la mémoire RAM 39. La clé de code est utilisée par le programme de codage/décodage 37b comme partie de l'algorithme qui chiffre et déchiffre l'information protégée. De façon similaire, pour avoir accès à l'information stockée dans la carte IC 23 sous une forme ayant une signification, l'utilisation doit entrer à la fois le mot de passe lu correct et la clé de code correcte. Il sera apprécié par les hommes de l'art que des variations de programme de codage et de décodage de logiciel bien connues peuvent être utilisées pour la mise en oeuvre de cette caractéristique.

Dans certaines situations, il est souhaitable de prévoir une communication de l'information en une seule journée ou même en quelques heures. Typiquement un courrier ordinaire ou des services de courrier ne peuvent pas assurer une délivrance le jour même. Selon la

présente invention, un modem peut être relié au dispositif de lecture/écriture 11 de la figure 1 pour transmettre électroniquement l'information à un récepteur autorisé. Bien que ce mode de réalisation de l'invention soit quelque peu moins sûr que ceux qui ont été mentionnés précédemment dans la mesure où les deux utilisateurs doivent connaître les deux mots de passe et une jonction de données électroniques est utilisée, il est utile dans certaines situations où la sécurité doit être sacrifiée au profit de la rapidité.

La figure 3 illustre un système utilisant deux dispositifs de lecture/écriture 11a et 11b reliés par une paire de modems conventionnels 43a et 43b et une voie de transmission 45 telle que des lignes de téléphone commerciales. Pour exécuter un transfert électronique selon ce mode de réalisation, l'expéditeur ou l'émetteur entre l'information dans une première carte 23a à l'aide du dispositif de lecture/écriture 11a de la manière précédemment décrite. Pour transmettre les données, l'expéditeur entre le mot de passe lu dans la première carte 23a, on rendant ainsi accessible les données au dispositif de lecture/écriture 11a et au modem 40a. Comme cela est bien connu dans la technique, le premier modem 43a transmet l'information au second modem 43b à travers la voie de transmission 45. De façon préférable le second utilisateur autorisé à l'endroit contenant le second dispositif de lecture/écriture 11b a été préalablement averti de la transmission de l'information. Ce second utilisateur introduit un mot de passe écrit dans une seconde carte 23b par l'intermédiaire d'un clavier associé au dispositif de lecture/écriture 11b. Comme cela a été expliqué ci-avant en rapport avec la figure 1, le microprocesseur 35 incorporé à la seconde carte IC 23b compare le mot de passe reçu au mot de passe écrit enregistré et permet l'inscription de l'information dans

le champ variable 39b de sa mémoire RAM 39 seulement lorsqu'une coïncidence a été constatée. En supposant que le second utilisateur ait présenté le mot de passe écrit correct, l'information du modem 43b est transférée à la
5 mémoire RAM 39 de la carte IC 23b, par l'intermédiaire du dispositif de lecture/écriture 11b. Pour que l'information soit visualisée au second utilisateur, il/elle doit entrer le mot de passe lu approprié, comme précédemment expliqué, pour que le microprocesseur 35 incorporé à la
10 carte IC 23b permette la reproduction de l'information sur un dispositif de reproduction ou de visualisation associé au dispositif de lecture/écriture 11b.

Etant donné que le placement de l'information sur une ligne de transmission telle que des lignes
15 téléphoniques la rend susceptible à une interception par une troisième partie, l'information est préférablement enchiffrée par une clé de code comme décrit précédemment. De façon spécifique, lorsque l'information est lue dans la première carte IC 23a, elle est envoyée au modem 40a
20 dans une forme chiffrée pour sa transmission sur la voie de transmission 45. De ce fait une clé de code n'est pas entrée lorsque l'information est lue dans la première carte IC 23a. Seulement les utilisateurs autorisés aux endroits d'envoi et de réception connaissent la clé de
25 code correcte.

Comme autre simplification du système général, la nécessité de la présence de moyens de lecture/écriture externe pour lire et écrire les données dans une carte IC telle qu'un dispositif de lecture/écriture conventionnel
30 et un bus I/O peut être éliminé en prévoyant des dispositifs de reproduction et d'entrée sous forme de parties intégrales de la carte I/C. En se référant aux figures 4 et 5, un dispositif de reproduction ou de visualisation 47 tel qu'un dispositif à cristaux liquides
35 49 sur la figure 5 communique avec le microprocesseur 35

incorporé de la carte IC 23' par l'intermédiaire d'un
moyen de lecture/écriture qui est réalisé par une
extension de la ligne de bus de commande/données 41 et
d'un dispositif d'attaque 51. De façon similaire, un
5 dispositif d'entrée 54 incorporé à la carte IC 23' est
également relié à l'extension d'une ligne de bus de
commande/données 41 par un tampon d'entrée 53. Comme cela
est montré sur la figure 5, le dispositif d'entrée 54
peut être une matrice de rangées de clavier 55 avec un
10 nombre suffisant de rangées de clavier pour assurer que
toutes les commandes appropriées et informations puissent
être inscrites. Pour une polyvalence maximale, la carte
IC 23' de la figure 5 comporte préférentiellement l'interface
33 et le bus I/O 42 conventionnels pour relier la carte
15 IC au dispositif de lecture/écriture 11 de la figure 1.
Bien que les rangées de touches ou de clavier 55 et le
dispositif de représentation à cristaux liquides 49 sont
desservis par la ligne de bus 41, le programme de
commande ne peut pas être atteint et aucune perte de mot
20 de passe ou de sécurité d'information n'intervient. Les
hommes de l'art apprécieront cependant qu'un programme
d'application tel que le programme de codage/décodage 37b
présente un certain risque en utilisant l'architecture
selon la figure 4. Un tel risque peut être la contre-
25 partie acceptable pour l'avantage de données d'entrée et
de sortie incorporées, dépendant de l'environnement de
l'utilisation envisagée de la carte IC.

Comme autre variation du système de sécurité
précédent, le programme de commande 37 du système à base
30 de microprocesseur sur la carte IC 23 est modifié pour
permettre l'inscription d'un nouveau mot de passe lu sur
l'ancien mot de passe lu dans le champ fixe 39a de la
mémoire RAM 39 pour que la carte puisse être envoyée à
plusieurs individus sans nécessité d'une prolifération de
35 la connaissance d'un mot de passe lu unique maintenu dans

le champ fixe 39 de la RAM 39. Un tel système alternatif peut être simplement rendu complémentaire par une structuration du programme de commande 39a de façon à répondre à une commande d'entrée prédéterminée en provenance du clavier 27 pour retourner à l'étape A après un premier jeu de mots de passe lu et écrit ait été entré dans le champ fixe 39a. Après le retour à l'étape A, des mots de passe lu et écrit nouveaux sont inscrits sur les mots de passe précédemment entrés.

10 Conformément au sujet d'un nombre augmenté d'utilisateurs possibles, la figure 6 illustre que le champ variable 39a de la mémoire RAM 39 incorporé à la carte IC 23 peut être divisé en une pluralité de sections 57. Le programme de commande 37a permet un accès de l'utilisateur seulement à la section 57 contenant un mot de passe lu ou écrit qui coïncide avec le mot de passe entré par l'utilisateur. En utilisant une telle carte IC conformément à l'invention, un groupe d'émetteurs et un groupe de récepteurs peut utiliser la carte de telle façon que pour chaque transfert d'informations unique, utilisant la carte, aussi peu que seulement un émetteur et un récepteur puisse avoir accès. Pendant le même transfert de la carte IC cependant, d'autres paires d'émetteurs/récepteurs peuvent transférer l'information sans connaissance de l'information accessible à la première paire d'émetteurs/récepteurs.

20 La carte IC peut être mise en circulation tout d'abord parmi un groupe d'utilisateurs qui entre des mots de passe de la manière expliquée en rapport avec l'étape A de la figure 2. La carte est ensuite envoyée à un second groupe. Chaque membre de ce second groupe connaît un mot de passe écrit entré par l'un des membres du premier groupe. Pour entrer l'information, les mêmes étapes de la figure 2 sont exécutées par le système à base de microprocesseur incorporé à la carte IC ;

5 cependant, dans ce mode de réalisation, seulement une section du champ variable identifiée par les mots de passe lu et écrit est accessible à l'information. La lecture de l'information est exécutée de la manière expliquée en rapport avec les figures 1 et 2.

10 On apprécie de ce qui précède, qu'un système et un procédé sont proposés pour le transfert peu cher d'une information sensible ou confidentielle d'une façon qui procure un degré de sécurité contre un accès non autorisé à l'information, qui n'était précédemment seulement possible en utilisant des terminaux d'ordinateurs relativement chers dans des zones protégées.

15 Contrairement au système antérieur, l'information protégée est inaccessible sous toute forme qui soit à un utilisateur non autorisé. Seulement les personnes ayant connaissance du mot de passe lu ou écrit peuvent avec succès avoir accès à la mémoire incorporée à la carte IC. L'homme du métier appréciera que les mots de passe lu et écrit peuvent être les mêmes. Comme autre simplification
20 du système, la clé de code peut également être formé par la même séquence de données qui comprend les mots de passe.

REVENDEICATIONS

1. Procédé pour utiliser au moins une carte de circuit intégré (IC) pour transmettre une information entre deux endroits et pour limiter l'accès à l'information seulement à des utilisateurs autorisés, selon lequel au moins une carte (IC) comporte un premier système à base d'ordinateur incorporé qui permet une lecture ou écriture par l'intermédiaire de moyens de lecture/écriture, ce procédé étant caractérisé en ce qu'il comprend les opérations :

- d'entrer ladite information dans un première mémoire dudit système à base de microprocesseur comprenant un premier microprocesseur qui empêche le transfert des contenus de ladite première mémoire audit moyen de lecture/écriture ou enregistrement en réponse à un mot de passe lu prédéterminé stocké dans ladite première mémoire ;

- de présenter un premier mot de passe audit premier microprocesseur pour permettre le transfert de ladite information audit moyen de lecture/écriture ;

- de transférer ladite information de ladite première mémoire audit moyen de lecture/écriture seulement lorsque ledit premier mot de passe coïncide avec le mot de passe lu prédéterminé stocké dans ladite mémoire ;

- de diriger ladite information transférée audit moyen de lecture/écriture à un dispositif de reproduction ; et

- de reproduire ladite information.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend des opérations :

de présenter un second mot de passe au microprocesseur précité, à travers les moyens de lecture/écriture précités, et

de transférer ladite information dudit moyen de lecture/écriture dans la première mémoire précitée seulement lorsque ledit second mot de passe coïncide avec un mot de passe écrit prédéterminé stocké dans ladite première mémoire.

3. Procédé selon la revendication 2, caractérisé en ce que l'opération de transférer l'information précitée du moyen de lecture/écriture précité à la première mémoire précitée comprend l'opération d'encoder ladite information selon une clé de code engendrée par ledit moyen de lecture/écriture.

4. Procédé selon la revendication 3, caractérisé en ce que l'opération de transférer l'information précitée de la première mémoire précitée au moyen de lecture/écriture précité comporte l'opération d'entrer la clé de code précitée en vue du décodage de ladite information.

5. Procédé selon la revendication 1, caractérisé en ce qu'au moins une carte (IC) comprend deux cartes (IC) physiquement séparées, une première et une seconde carte, de telle façon que les opérations d'entrer l'information précitée, de présenter le premier mot de passe et de transférer ladite information intervient dans ladite première carte (IC) et l'opération de diriger ladite information comprend :

entrer ladite information dans une seconde mémoire incorporée à ladite seconde carte (IC) à travers une voie de transmission ;

présenter le second mot de passe précité à un second microprocesseur d'un second système à base de microprocesseur, incorporé à ladite seconde carte (IC) pour permettre le transfert de ladite information de ladite première mémoire à ladite seconde mémoire dans ledit second système à base de microprocesseur, et

transférer ladite information de ladite seconde mémoire au dispositif de reproduction précité seulement lorsque le second mot de passe coïncide avec un mot de passe lu prédéterminé stocké dans ladite seconde mémoire.

5 6. Procédé selon la revendication 1, caractérisé en ce que le premier mot de passe précité stocké dans la première mémoire est entré à l'aide de moyens de lecture/écriture.

10 7. Système pour empêcher l'accès à des informations confidentielles par des personnes non autorisées pendant le transfert desdites informations confidentielles entre des premier et second utilisateurs autorisés, caractérisé en ce qu'il comprend au moins une carte de circuit intégré comportant des circuits à base
15 de microprocesseur comportant une mémoire contenant lesdites informations confidentielles, des premiers moyens pour présenter des données audit circuit à base de microprocesseur ou de les libérer de ceux-ci, lesdits circuits à base de microprocesseur comprenant des seconds
20 moyens pour transférer des données entre lesdits premiers moyens et ladite mémoire, au moins un clavier pour engendrer lesdites données à présenter par lesdits premiers moyens auxdits circuits à base de microprocesseur, des moyens de reproduction sensibles
25 auxdits premiers moyens pour visualiser ladite information confidentielle, lesdits seconds moyens comportant des moyens de comparaison pour comparer un premier mot de passe desdites données engendrées par ledit clavier et présentées au circuit à base de
30 microprocesseur par lesdits premiers moyens avec un mot de passe lu précédemment stocké dans ladite mémoire, et transférer ladite information confidentielle de ladite mémoire auxdits premiers moyens seulement lorsque le premier mot de passe coïncide avec ledit mot de passe lu.

8. Système selon la revendication 8, caractérisé en ce que les moyens de comparaison comportent des moyens pour comparer un second mot de passe desdites données engendrées par ledit clavier et présentées auxdits circuits à base de microprocesseur par les premiers moyens précités avec un mot de passe écrit, précédemment stocké dans ladite mémoire, et pour transférer l'information confidentielle desdits premiers moyens à ladite mémoire seulement lorsque le second mot de passe coïncide avec ledit mot de passe écrit.

9. Système selon la revendication 7, caractérisé en ce que les premiers moyens précités comportent un bus entrée/sortie et un dispositif de lecture/écriture.

10. Système selon la revendication 7, caractérisé en ce que le premier moyen précité comporte une extension d'un bus de commande/données incorporé à ladite carte (IC) pour connecter les circuits à base de microprocesseur précités au clavier précité et les moyens de reproduction ou visualisation précités, où le clavier est une matrice de rangées de clavier ou de touches montée sur ladite carte (IC) et lesdits moyens de reproduction sont également montés sur ladite carte (IC).

11. Système selon la revendication 8, caractérisé en ce que la mémoire précitée est divisée entre au moins un groupe de champ fixe et variable, ledit champ fixe comportant les mots de passe lu et écrit précités et le champ variable contenant l'information confidentielle précitée.

12. Système selon la revendication 11, caractérisé en ce que la mémoire précitée comporte une pluralité de groupes précités et les moyens de comparaison comportent des moyens permettant l'accès seulement par les premiers moyens précités à

l'information confidentielle à un groupe pour qui une coïncidence est détectée entre le premier mot de passe précité et le mot de passe lu précité.

5 13. Système selon la revendication 7,
caractérisé en ce que les premiers moyens précités
comportent des premier et second dispositifs de
lecture/écriture reliés par un joint de données
électroniques et ladite carte (IC) précitée comprend une
première carte reliée audit premier dispositif de
10 lecture/écriture et seconde carte reliée audit second
dispositif de lecture/écriture.

 14. Système selon la revendication 13,
caractérisé en ce que les première et seconde cartes (IC)
précitées comportent chacune des circuits à base de
15 microprocesseur précités ayant la mémoire précitée et
lesdits seconds moyens précités.

1/4

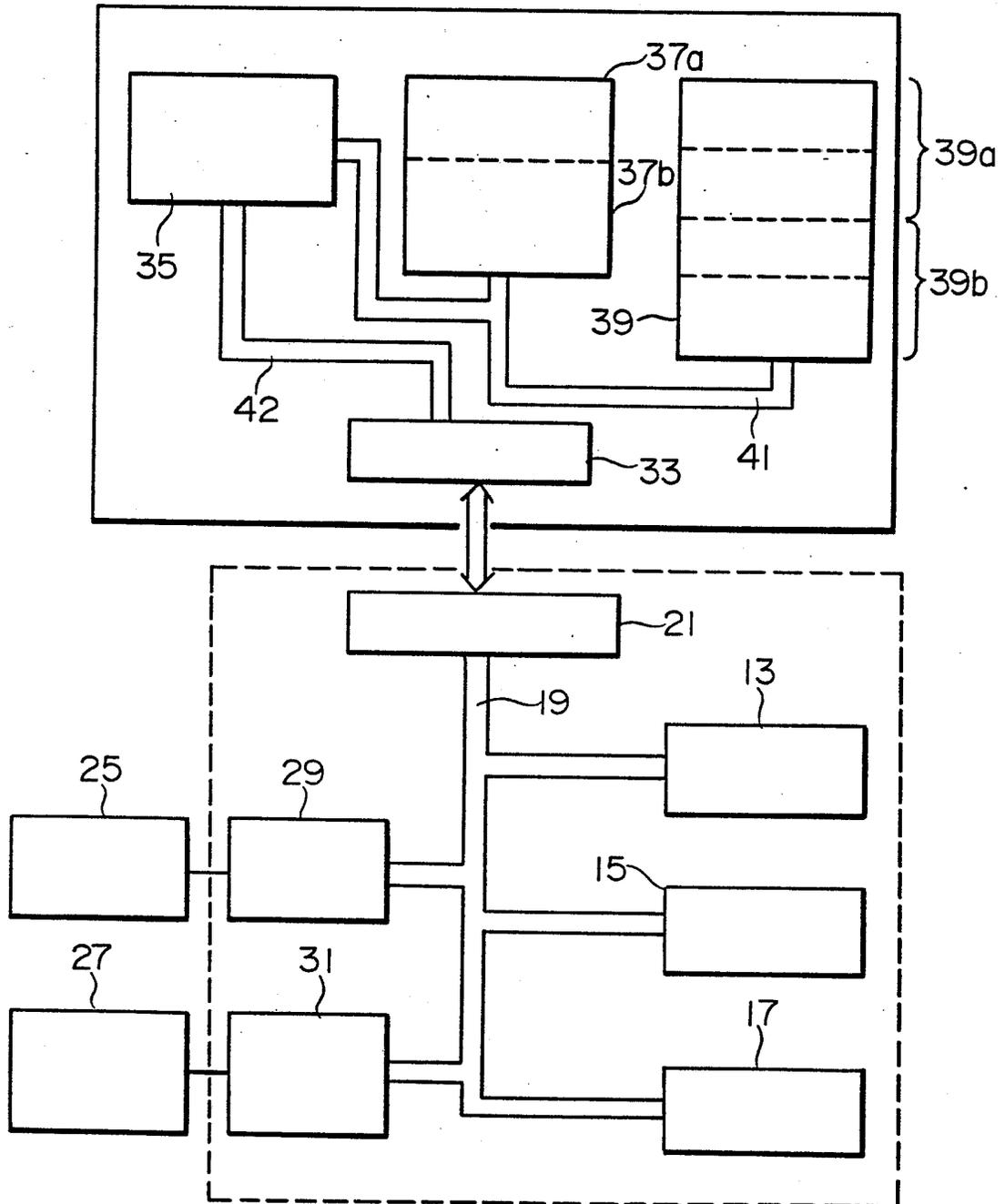
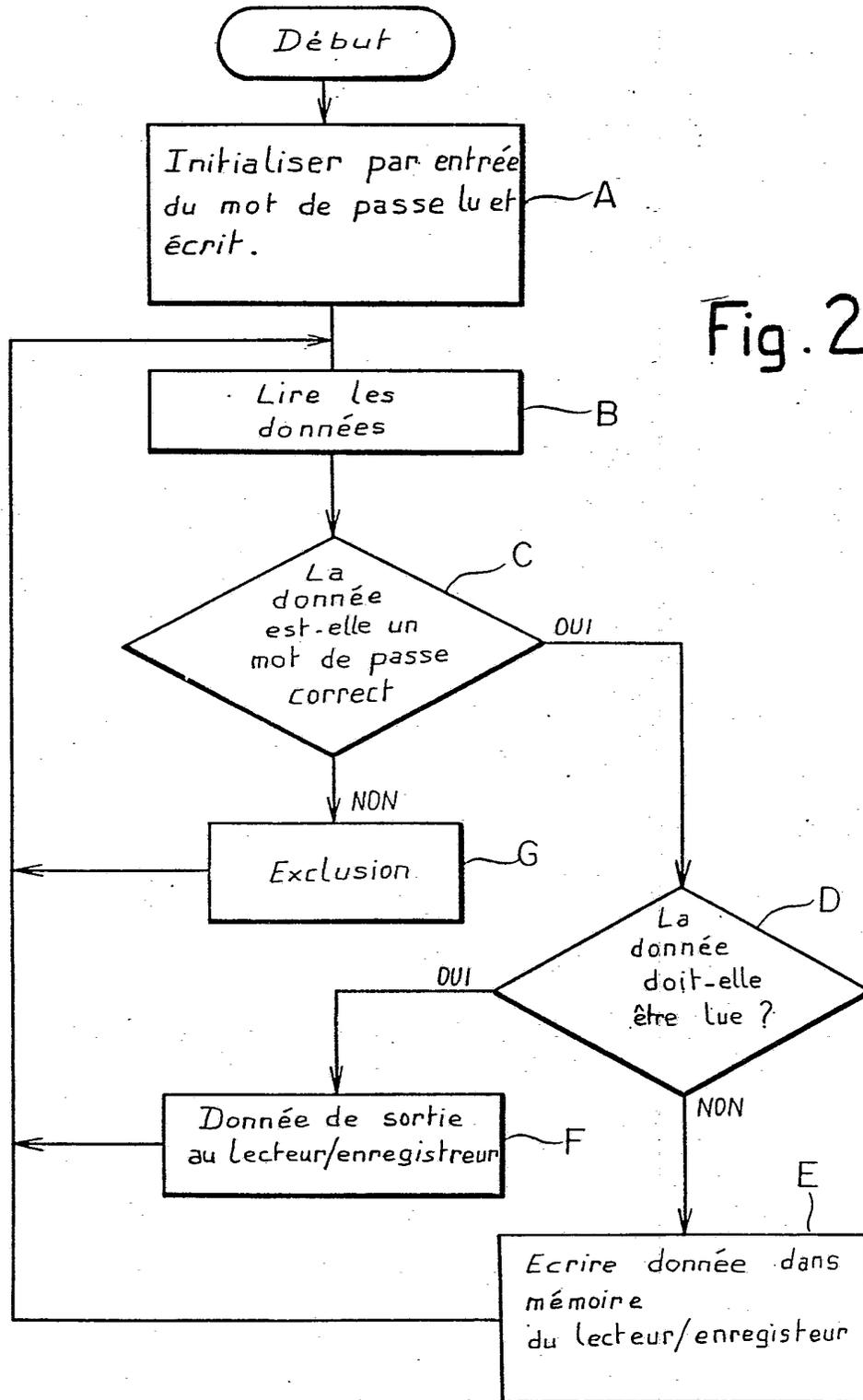


Fig. 1

2/4



3/4

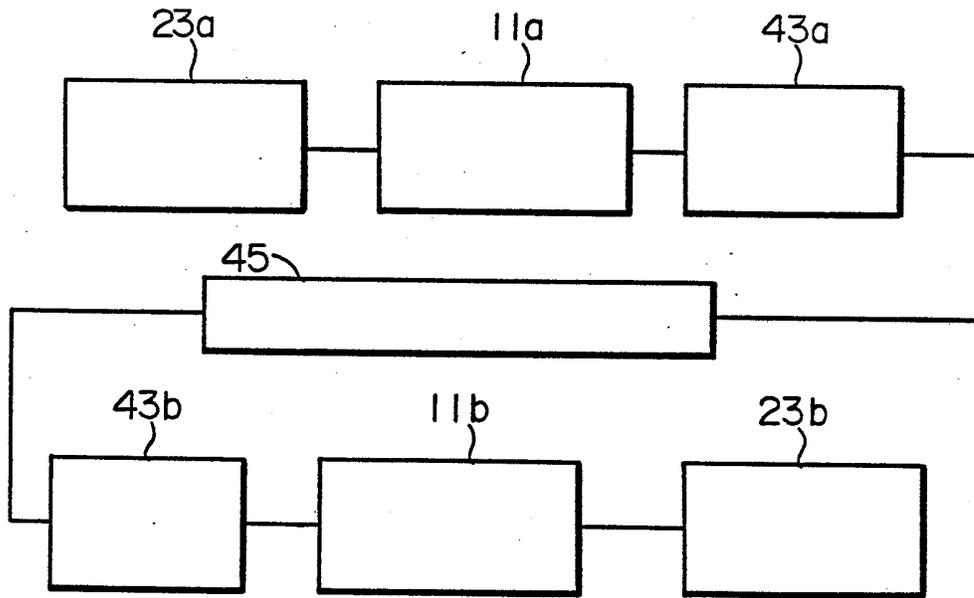


Fig. 3

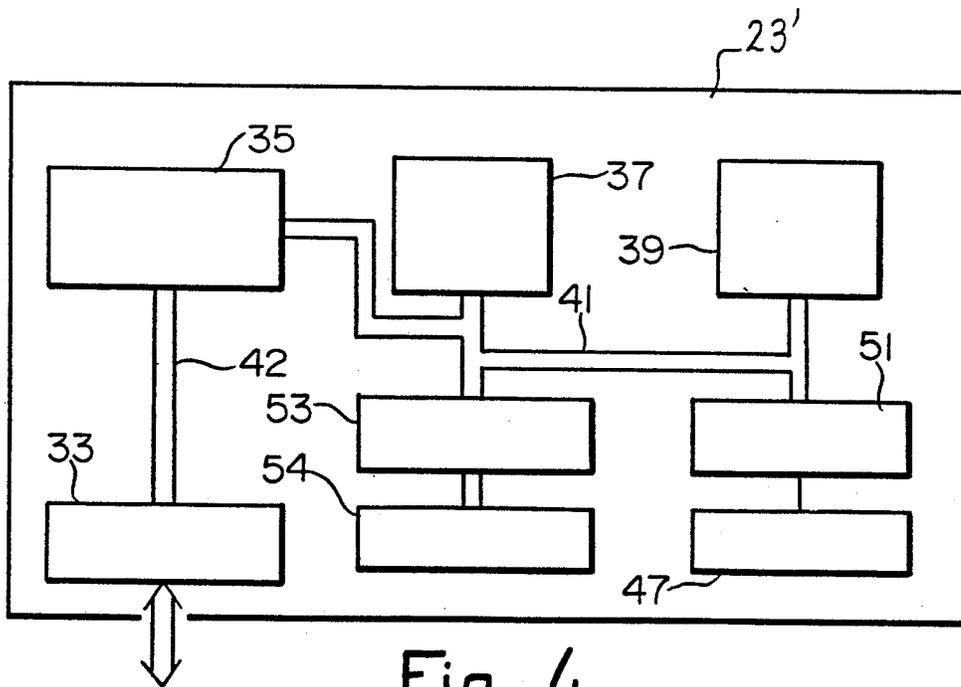


Fig. 4

4/4

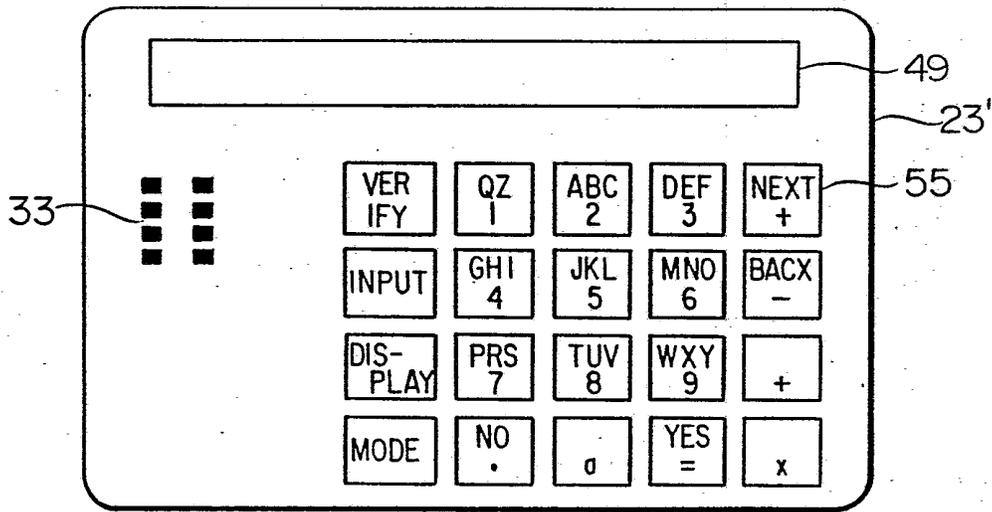


Fig. 5

Fig. 6

