

①9 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

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

2 635 893

②1 N° d'enregistrement national :

89 11249

⑤1 Int Cl⁵ : G 06 K 19/073.

⑫

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 25 août 1989.

③0 Priorité : JP, 26 août 1988, n° 63-211834.

④3 Date de la mise à disposition du public de la
demande : BOPI « Brevets » n° 9 du 2 mars 1990.

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

⑦1 Demandeur(s) : Société dite : KABUSHIKI KAISHA TOS-
HIBA. — JP.

⑦2 Inventeur(s) : Yasuo Iijima.

⑦3 Titulaire(s) :

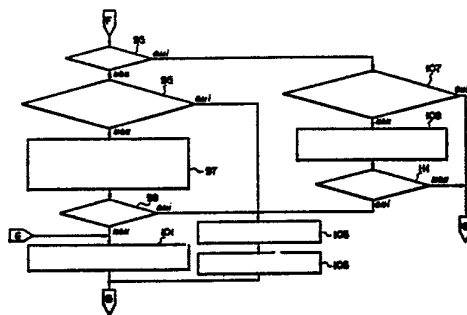
⑦4 Mandataire(s) : Cabinet Beau de Loménie.

⑤4 Dispositif électronique portable.

⑤7 L'invention concerne les techniques d'accès conditionnel à
une zone de mémoire.

Une mémoire interne contient un ensemble de données de
clé d'accès qui sont comparées avec un ensemble de se-
condes données de clé, appliquées sélectivement par un dis-
positif externe. Les résultats de comparaison sont enregistrés
pour chacune des données de clé. L'accès à une zone de la
mémoire est autorisé lorsque l'un des résultats de comparaison
qui sont enregistrés est affirmatif, ou lorsque tous les résultats
de comparaison sont affirmatifs. Un ensemble de données de
décision d'autorisation/interdiction d'accès sont enregistrées
en correspondance avec les zones et l'une correspondante de
ces données est sélectionnée conformément à des données
d'instruction appliquées de l'extérieur.

Application aux cartes à puce.



FR 2 635 893 - A1

D

La présente invention concerne un dispositif électronique portable, connu sous le nom de carte à circuit intégré, ou carte à puce, qui contient une puce de circuit intégré comprenant par exemple une mémoire non volatile et un élément de commande tel qu'une unité centrale, et elle porte plus particulièrement sur un dispositif électronique portable qui utilise un procédé de commande d'accès amélioré pour une zone de la mémoire.

On a développé à titre de support de mémorisation portable un dispositif appelé carte à puce qui contient une puce de circuit intégré comportant par exemple une mémoire non volatile et un élément de commande tel qu'une unité centrale. Une carte à puce de ce type mémorise dans sa mémoire interne un numéro d'identification qui remplit la fonction de données de clé d'accès. Lorsqu'un numéro d'identification est introduit à partir de l'extérieur, il est comparé avec le numéro d'identification attribué qui est enregistré dans la mémoire interne, et l'accès ultérieur à la mémoire est autorisé ou interdit en fonction du résultat de la comparaison.

Une carte à puce classique est décrite dans la publication de brevet du Japon (Kokai) n° 60-160491, Tamada et col., 22 août 1985 (demande de brevet des E.U.A. n° 699 099).

A titre de procédé pour déterminer si l'accès à une zone de mémoire est autorisé, on enregistre un ensemble de numéros d'identification dans une mémoire, et on enregistre en correspondance avec des zones des données d'identification qui indiquent un numéro d'identification à comparer lorsqu'on désire accéder à une zone correspondante. Le résultat de la comparaison des numéros d'identification est alors comparé avec les données d'identification pour chaque

accès, pour déterminer si un accès est autorisé ou non.

5 Cependant, si les données d'identification sont utilisées en commun pour toutes les données d'instruction d'accès, les conditions d'accès pour toutes les données d'instruction deviennent les mêmes, et on ne peut pas établir de façon fine une condition d'accès pour une zone, ce qui fait qu'on ne peut pas utiliser de façon souple le système de carte à puce.

10 Un but de l'invention est de procurer un dispositif électronique portable qui puisse fixer arbitrairement une combinaison de données de clé qui sont nécessaires pour accéder à une zone parmi un ensemble de zones, et qui puisse fixer plus précisément
15 une combinaison logique ET ou OU conjointement à la combinaison, de façon qu'il soit possible d'établir de façon fine une condition d'accès pour chaque zone, et d'obtenir une grande souplesse dans l'utilisation d'un système.

20 Un autre but de l'invention est de procurer un dispositif électronique portable qui permette de faire varier une condition d'accès pour chacune des données d'instruction qu'on utilise pour accéder à chaque zone, et qui puisse fixer arbitrairement une
25 correspondance entre des données d'instruction et une condition d'accès.

30 Un autre but encore de l'invention est de procurer un dispositif électronique portable qui puisse fixer une condition d'accès spécifique, par exemple une condition d'interdiction d'accès et une condition de libre accès, dans des données d'instruction qui sont utilisées pour accéder à chaque zone, et qui permette une commande fine de l'accès.

35 Un autre but encore de l'invention est de procurer un dispositif électronique portable qui puisse

se fixer l'une des conditions de commande d'accès, d'interdiction d'accès et de libre accès, sur la base d'une combinaison de données de clé qui sont nécessaires pour un accès, et d'une logique combinatoire, à titre de condition d'accès pour chaque zone, avec un faible volume de données.

Conformément à l'invention, un ensemble de données de clé sont enregistrées dans une mémoire interne, et elles sont comparées avec un ensemble de secondes données de clé qui sont introduites sélectivement à partir d'un dispositif externe. Les résultats de comparaison sont enregistrés pour chacune des données de clé. Au moment de la demande d'accès à une zone déterminée, un accès est autorisé si l'un des résultats de comparaison enregistrés est affirmatif, ou si tous les résultats de comparaison enregistrés sont affirmatifs.

On peut ainsi fixer zone par zone une combinaison de données de clé qui sont nécessaires pour accéder à une zone, et on peut établir une condition logique ET ou OU en association avec la combinaison. Une condition d'accès pour chaque zone peut donc être fixée de façon fine, ce qui permet d'obtenir une grande souplesse dans la configuration d'un système.

Selon un second aspect de l'invention, un ensemble de données de clé sont enregistrées dans une mémoire interne, et elles sont comparées avec un second ensemble de données de clé qui sont introduites sélectivement à partir d'un dispositif externe. Un ensemble de données de décision d'autorisation/interdiction d'accès sont enregistrées en correspondance avec des zones. Des données correspondantes de décision d'autorisation/interdiction d'accès sont sélectionnées conformément à des données d'instruction qui sont introduites de façon externe, et une décision d'autori-

sation/interdiction d'accès pour chaque zone est prise conformément aux données de décision d'autorisation/interdiction d'accès qui ont été sélectionnées, sur la base du résultat de comparaison.

5 D'autres caractéristiques et avantages de l'invention seront mieux compris à la lecture de la description qui va suivre d'un mode de réalisation, et en se référant aux dessins annexés sur lesquels :

10 La figure 1 est un schéma synoptique qui montre une structure comprenant un dispositif électronique portable conforme à l'invention, et un terminal d'utilisation;

15 La figure 2 est un schéma synoptique qui montre des fonctions de la carte à puce qui est représentée sur la figure 1;

La figure 3 est un schéma synoptique qui montre la structure de la carte à puce qui est représentée sur la figure 1;

20 La figure 4 montre une structure de fichier d'une mémoire de données qui est représentée sur la figure 3;

La figure 5 est une représentation qui est destinée à expliquer des données d'identification pour des données de clé;

25 La figure 6 est une représentation destinée à l'explication d'une section d'enregistrement d'état de comparaison et d'une section d'enregistrement de nom de fichier de données;

30 La figure 7 est une représentation destinée à l'explication de données d'identification pour une zone;

35 La figure 8 est une représentation destinée à l'explication d'une table de données qui enregistre des données de sélection pour la sélection de données de confirmation d'état de comparaison, en correspon-

dance avec divers codes d'instruction,

Les figures 9A à 9E sont des organigrammes qui sont destinés à l'explication d'opérations de traitement;

5 La figure 10 montre un format de données d'instruction de sélection de fichier de données;

La figure 11 montre un format de données d'instruction de comparaison de données de clé;

10 La figure 12A montre un format de données d'instruction de lecture dans une zone;

La figure 12B montre un format de données d'instruction d'écriture dans une zone; et

La figure 12C montre un format de données d'instruction d'effacement dans une zone.

15 La figure 1 montre une carte à puce à titre de dispositif électronique portable conforme à l'invention, et un terminal pour l'utilisation de la carte à puce. La carte à puce 1 peut être connectée par l'intermédiaire d'un lecteur/enregistreur de carte 2 à
20 une section de commande 3 qui comprend par exemple une unité centrale de traitement. La section de commande 3 est connectée à un clavier 4, à un dispositif de visualisation à tube cathodique 5, à une imprimante 6 et à une unité de disquette 7. La carte à puce est portée
25 par un utilisateur et elle est utilisée pour faire appel à des données de clé (numéro d'identification) qui sont connues de l'utilisateur, au moment de l'achat d'un article, et pour enregistrer des données nécessaires.

30 La figure 2 montre des blocs fonctionnels de la carte à puce. La carte à puce est constituée par des sections qui sont destinées à exécuter des fonctions de base, à savoir une section de lecture/écriture 11, une section de fixation/comparaison de numéro
35 d'identification personnel, 12, et une section de cryp-

tage/décryptage 13, ainsi que par un superviseur 14 destiné à la gestion de ces fonctions de base.

La section de lecture/écriture 11 a pour fonctions de lire, d'écrire ou d'effacer des données dans une mémoire de données 16, ou autre.

La section de fixation/comparaison de numéro d'identification personnel 12 a pour fonctions d'accomplir des opérations de traitement d'enregistrement et d'interdiction de lecture pour un numéro d'identification qui est fixé par l'utilisateur, ainsi que de comparer le numéro d'identification, après qu'il a été fixé, pour permettre l'accomplissement de la suite du traitement.

La section de cryptage/décryptage 13 a pour fonction de crypter des données afin d'empêcher la divulgation ou la reproduction frauduleuse de données de communication, lorsque ces données sont transmises de la section de commande 3 vers un autre terminal par l'intermédiaire d'une ligne de communication, ainsi que de décrypter les données cryptées. A titre d'exemple, la section 13 a pour fonction d'accomplir un traitement de données conformément à un algorithme de cryptage ayant une sécurité de cryptage suffisante, comme par exemple l'algorithme DES (Data Encryption Standard).

Le superviseur 14 a pour fonction de décoder un code de fonction qui est introduit par le lecteur/enregistreur de carte 2, ou un code de fonction qui est ajouté aux données, et de sélectionner et d'exécuter l'une nécessaire des fonctions de base.

Pour mettre en oeuvre ces fonctions, la carte à puce 1 comprend un élément de commande (section de commande) 15, tel qu'une unité centrale, une mémoire de données (section de mémoire) 16, une mémoire de programme 17 et une partie de contact 18, pour établir

un contact électrique avec le lecteur/enregistreur de carte 2, comme le montre la figure 3. Parmi ces composants, l'élément de commande 15, la mémoire de données 16 et la mémoire de programme 17 sont constitués par une seule puce de circuit intégré (ou par plusieurs puces de circuit intégré), et ils sont noyés dans le corps de la carte à puce.

La mémoire de programme 17 consiste par exemple en une mémoire morte à masque, et elle conserve un programme de commande ou un programme similaire de l'élément de commande 15, qui comprend des sous-programmes destinés à la mise en oeuvre des fonctions de base précitées.

Comme le montre la figure 4, la mémoire de données 16 comprend par exemple une mémoire non volatile programmable, telle qu'une mémoire morte programmable et effaçable par des moyens électriques, ou EEPROM, qu'on utilise pour enregistrer diverses données.

La mémoire de données 16 est constituée par un fichier de données commun (première région) 21 auquel on accède dans toutes les applications, et par un ensemble de fichiers de données d'application (secondes régions) 22₁ et 22₂ auxquels on accède uniquement pour l'application concernée, comme le montre la figure 4. Chacun des fichiers de données 21, 22₁ et 22₂ conserve un ensemble de données de clé (numéro d'identification), et il comprend un ensemble de zones.

Un nom de fichier de données (DFN) est donné à chacun des fichiers de données d'application 22₁ et 22₂. A la désignation d'un nom de fichier de données par l'utilisation de données d'instruction de sélection de fichier de données (qu'on décrira ultérieurement), le dispositif reconnaît un fichier de données qui doit faire l'objet d'un accès.

Des données d'identification (KID) pour désigner des données de clé sont affectées à chacune des données de clé, comme le montre la figure 5. Lorsqu'on désigne des données d'identification en utilisant des données d'instruction de comparaison de données de clé (qu'on décrira ultérieurement), le dispositif reconnaît des données de clé qui doivent faire l'objet d'un traitement de comparaison.

Sur la figure 3, des données d'identification KID01, KID02 et KID03 sont affectées à des données de clé 1, 2 et 3 qui appartiennent au fichier de données commun 21. Des données d'identification KID04, KID05 et KID06 sont affectées aux données de clé X4, X5 et X6 qui appartiennent au fichier de données d'application 22₁. Des données d'identification KID04, KID05 et KID06 sont également affectées aux données de clé Y4, Y5 et Y6 qui appartiennent au fichier de données d'application 22₂. Des données de désignation d'état de comparaison sont affectées à chacune des données de clé, comme le montre la figure 5. On utilise les données de désignation d'état de comparaison pour déterminer si des données de clé nécessaires pour un accès suivant ont déjà été comparées.

Des données indiquant si des données de clé ont déjà été comparées sont enregistrées dans des sections d'enregistrement d'état de comparaison 23₁ et 23₂ qui sont représentées sur la figure 6. Les sections d'enregistrement d'état de comparaison 23₁ et 23₂ sont établies dans une mémoire vive qui est incorporée par exemple dans l'élément de commande 15. Des données de clé appartenant au fichier de données commun 21 sont enregistrées dans la section d'enregistrement d'état de comparaison 23₁, et des données de clé appartenant aux fichiers de données d'application 22₁ et 22₂ sont enregistrées dans la section d'enregistre-

ment d'état de comparaison 23₂.

Comme le montre la figure 6, une section d'enregistrement de nom de fichier de données 24 est établie conjointement aux sections d'enregistrement d'état de comparaison 23₁ et 23₂. La section d'enregistrement de nom de fichier de données 24 conserve un nom de fichier de données relatif au fichier de données sélectionné à titre d'objet auquel on doit accéder par des données d'instruction de sélection de fichier de données (qu'on décrira ultérieurement). Comme le montre la figure 7, des données d'identification (AID) qui sont destinées à désigner une zone sont attribuées à chaque zone. Par conséquent, lorsque les données d'identification sont désignées en utilisant des données d'instruction de traitement de zone (qu'on décrira ultérieurement), le dispositif peut reconnaître une zone qui est l'objet d'un traitement de zone.

Sur la figure 4, des données d'identification AIDgg et AIDhh sont affectées à des zones G et H qui appartiennent au fichier de données commun 21. Des données d'identification AIDaa, AIDbb et AIDcc sont affectées à des zones A, B et C qui appartiennent au fichier de données d'application 22₁. Des données d'identification AIDdd, AIDee et AIDff sont affectées à des zones D, E et F qui appartiennent au fichier de données d'application 22₂.

Comme le montre la figure 7, des premières et secondes données de confirmation d'état de vérification sont ajoutées à chaque zone. Des données logiques (A ou O) sont affectées à ces premières et secondes données de confirmation d'état de comparaison. Les premières et secondes données de confirmation d'état de comparaison demandent des états de comparaison de données de clé qui sont nécessaires dans un accès à une zone. Les données logiques indiquent si

une combinaison des données de confirmation d'état de comparaison correspond à une fonction logique ET ou OU. Dans le cas de la fonction logique ET, les données logiques sont fixées à "A", et dans le cas de la fonction logique OU, elles sont fixées à "O".

La figure 8 montre une table de données qu'on utilise pour sélectionner les deux données de confirmation d'état de comparaison qui sont affectées à chaque zone, avec des codes d'instruction respectifs. La table de données contient des données de sélection pour sélectionner l'information de confirmation d'état de comparaison, en correspondance avec divers codes d'instruction, et cette table de données est établie par exemple dans la mémoire de données 16.

On décrira ci-après le mode de réalisation de l'appareil électronique portable conforme à l'invention, en se référant aux organigrammes qui sont représentés sur les figures 9A à 9F. Sur les organigrammes, le fichier de données commun 21 est désigné par l'abréviation CDF, et le fichier de données d'application 22₁ ou 22₂ est désigné par l'abréviation ADF.

On décrira ci-après le traitement de sélection de fichier de données en se référant à l'organigramme qui est représenté sur la figure 9A. Dans l'état de repos, l'élément de commande attend des données d'instruction. Si des données d'instruction sont introduites à l'étape 31, l'élément de commande 15 détermine à l'étape 33 si les données d'instruction qui sont introduites correspondent à une instruction de sélection de fichier de données, représentée sur la figure 10. Si la réponse est NON, à l'étape 33, la séquence passe à l'étape 47 et l'élément de commande 15 effectue un autre traitement.

Si la réponse est OUI à l'étape 33, l'élément de commande 15 cherche dans la mémoire de données

16, à l'étape 35, un fichier de données d'application ayant un nom de fichier de données identique à celui qui figure dans ces données d'instruction. Si aucun fichier de ce type n'est trouvé à l'étape 37, l'élé-
5 ment de commande 15 émet à l'étape 41 des données de réponse qui indiquent que le fichier de données n'est pas défini, et la séquence retourne à l'état d'attente de données d'instruction à l'étape 31.

Si à l'étape 37 la réponse est OUI, l'élé-
10 ment de commande 15 enregistre dans la section d'enregistrement de nom de fichier 24 de la figure 6, à l'étape 39, le nom de fichier de données qui figure dans ces données d'instruction, et il fixe dans un état de non-comparaison le contenu de la section d'en-
15 registrement d'état de comparaison 23₂, c'est-à-dire qu'il fixe tous les bits à "0" à l'étape 43. L'élément de commande émet des données de réponse qui indiquent que la sélection du fichier de données est terminée, à l'étape 45, et la séquence retourne ensuite à l'état
20 d'attente de données d'instruction à l'étape 31.

Au moment de la mise en service de la carte à puce, les sections d'enregistrement 23₁ et 23₂ de la figure 6 ne contiennent que des "0". Dans ce cas, si
25 on introduit des données d'instruction de sélection de fichier de données ayant un nom de fichier de données "xxx", une valeur "xxx" est enregistrée dans la section d'enregistrement de nom de fichier de données 24.

On décrira ci-après le traitement de comparaison de données de clé en se référant aux organi-
30 grammes qui sont représentés sur les figures 9B et 9C. Si la détermination qui est faite à l'étape 33 indique que les données d'instruction d'entrée ne sont pas les données d'instruction de sélection de fichier de données, l'élément de commande 15 détermine à l'étape 47
35 si les données d'instruction d'entrée sont une ins-

truction de comparaison de données de clé, qui est représentée sur la figure 11. Si la réponse à l'étape 47 est NON, la séquence passe à l'étape 79, et l'élément de commande 15 exécute un autre traitement.

5 Si la réponse à l'étape 47 est OUI, l'élément de commande 15 détermine à l'étape 49 si le contenu de la section d'enregistrement de nom de fichier de données 24 ne comprend que des "0" (c'est-à-dire si le fichier de données est sélectionné ou non). Si la
10 détermination qui est faite à l'étape 49 indique que la section précitée ne contient que des "0", ceci signifie qu'aucun fichier de données n'est sélectionné, et l'élément de commande 15 accède au fichier de données commun à l'étape 53 pour trouver des données de clé
15 ayant des données d'identification (KID) identiques à celles qui figurent dans les données d'instruction d'entrée, à l'étape 55. Si la détermination qui est faite à l'étape 49 indique que la section 24 ne contient pas que des "0", ceci signifie qu'un fichier de
20 données est sélectionné. Par conséquent, l'élément de commande 15 accède au fichier de données commun 21 et au fichier sélectionné parmi les fichiers de données d'application 22₁ et 22₂, à l'étape 51, pour chercher des données de clé ayant des données d'identification
25 identiques à celles qui figurent dans les données d'instruction d'entrée, à l'étape 55. Si la réponse à l'étape 55 est NON, l'élément de commande 15 émet des données de réponse qui indiquent que les données de clé ne sont pas définies, à l'étape 57, et la séquence
30 retourne à l'état d'attente de données d'instruction, à l'étape 31.

 Si la réponse à l'étape 55 est OUI, l'élément de commande 15 compare les données de clé qui ont été trouvées et les données de clé qui figurent dans
35 les données d'instruction d'entrée, à l'étape 59.

Si la comparaison qui est faite à l'étape 61 permet de trouver une coïncidence entre les deux types de données de clé, l'élément de commande 15 détermine à l'étape 63 si les données de clé appartiennent au
5 fichier de données commun 21 ou au fichier de données d'application 22₁ ou 22₂. Si la détermination qui est faite à l'étape 63 indique que les données de clé appartiennent au fichier de données commun 21, l'élément de commande 15 accède aux données de désignation
10 d'état de comparaison qui ont été affectées aux données de clé, et il fixe à "1" à l'étape 67 un bit de la section d'enregistrement d'état de comparaison 23₁ qui correspond à un bit "1" des données de désignation. Si la détermination qui est faite à l'étape 63 indique
15 que les données de clé appartiennent au fichier de données d'application, l'élément de commande 15 fixe de façon similaire à "1" un bit de la section d'enregistrement d'état de comparaison 23₂ qui correspond à un bit "1" des données de désignation. A l'étape 69,
20 l'élément de commande 15 émet des données de réponse qui indiquent la coïncidence des données de clé, et la séquence retourne à l'état d'attente de données d'instruction.

Si la comparaison de l'étape 61 conduit à
25 trouver une absence de coïncidence entre les données de clé, l'élément de commande 15 fixe de façon similaire à "0", à l'étape 65, un bit correspondant de la section d'enregistrement d'état de comparaison 23₁ ou 23₂. A l'étape 69, l'élément de commande 15 émet des
30 données de réponse qui indiquent une absence de coïncidence des données de clé, et la séquence retourne à l'état d'attente de données d'instruction.

A titre d'exemple, lorsque des données de clé 1 et des données de clé Y5 et Y6 sont comparées
35 après que le fichier de données d'application 22₂ a

été sélectionné par les données d'instruction de sélection de fichier de données, le contenu de la section d'enregistrement d'état de comparaison 23₁ est fixé à "10000000", le contenu de la section d'enregistrement d'état de comparaison 23₂ est fixé à "00001100", et le contenu de la section d'enregistrement de nom de fichier de données 24 est fixé à "YYY". Ensuite, lorsque le fichier de données d'application 22₁ est sélectionné, le contenu de la section d'enregistrement d'état de comparaison 23₁ est laissé inchangé, le contenu de la section d'enregistrement d'état de comparaison 23₂ est fixé à "00000000", et le contenu de la section d'enregistrement de nom de fichier de données 24 est fixé à "xxx".

On décrira ensuite un traitement de zone (traitement de lecture, d'écriture et d'effacement de données dans une zone), en se référant aux organigrammes qui sont représentés sur les figures 9D et 9E. Si la détermination qui est faite à l'étape 47 indique que les données d'instruction d'entrée ne sont pas les données d'instruction de comparaison de données de clé, l'élément de commande 15 détermine à l'étape 79 si les données d'instruction d'entrée sont des données d'instruction de lecture, représentées sur la figure 12A, des données d'instruction d'écriture représentées sur la figure 12B, ou des données d'instruction d'effacement représentées sur la figure 12C. Si la réponse à l'étape 79 est NON, l'élément de commande 15 exécute un autre traitement.

Si la réponse à l'étape 79 est OUI, l'élément de commande 15 détermine à l'étape 81 si la section d'enregistrement de nom de fichier de données 24 ne contient que des "0" (c'est-à-dire si le fichier de données est sélectionné ou non). Si la détermination qui est faite à l'étape 81 indique que la section

précitée ne contient que des "0", ceci signifie qu'aucun fichier de données n'est sélectionné, et l'élément de commande 15 adresse le fichier de données commun 21 et le fichier sélectionné parmi les fichiers de données d'application 22₁ et 22₂, pour trouver une zone ayant des données d'identification (AID) identiques à celles qui figurent dans les données d'instruction d'entrée, à l'étape 85.

Si la détermination qui est faite à l'étape 81 indique que la section d'enregistrement de nom de fichier de données 24 ne contient pas que des "0", ceci signifie qu'un fichier de données est sélectionné. Par conséquent, l'élément de commande 15 adresse le fichier de données commun 21 et le fichier sélectionné parmi les fichiers de données d'application 22₁ et 22₂, pour trouver une zone ayant des données d'identification (AID) identiques à celles qui figurent dans les données d'instruction d'entrée, à l'étape 83. Si ces données ne sont pas trouvées à l'étape 87, l'élément de commande 15 émet à l'étape 91 des données de réponse qui indiquent qu'une zone n'est pas définie, et la séquence retourne à l'état d'attente de données d'instruction.

Si la réponse à l'étape 87 est OUI, l'élément de commande 15 combine par une fonction logique OU les contenus des sections d'enregistrement d'état de comparaison 23₁ et 23₂, à l'étape 89, et il donne l'appellation "résultat 1" au résultat de la fonction OU.

L'élément de commande 15 recherche dans la table de données qui est représentée sur la figure 8 un code d'instruction identique à celui qui figure dans les données d'instruction d'entrée, pour sélectionner deux données de confirmation d'état de comparaison qui sont affectées à chaque zone. Si les don-

nées d'instruction de traitement de zone sont des données d'instruction de lecture, du fait que leur code d'instruction est "zz", les premières données de confirmation d'état de comparaison sont sélectionnées par
5 des données de sélection "1" correspondantes; s'il s'agit de données d'instruction d'écriture, du fait que leur code d'instruction est "ww", les secondes données de confirmation d'état de comparaison sont sélectionnées par des données de sélection "2" corres-
10 pondantes; et s'il s'agit de données d'instruction d'effacement, du fait que leur code d'instruction est "vv", les secondes données de confirmation d'état de comparaison sont sélectionnées par des données de sélection "2" correspondantes.

15 Lorsque les premières ou les secondes données de confirmation d'état de comparaison sont sélectionnées de cette manière, l'élément de commande 15 adresse les données de confirmation d'état de comparaison sélectionnées, à l'étape 93, pour déterminer si
20 les données logiques qui leur sont ajoutées consistent en une fonction logique ET. Si la réponse à l'étape 93 est NON (c'est-à-dire si une fonction logique OU est sélectionnée), l'élément de commande 15 détermine à l'étape 95 si les bits des données de confirmation
25 d'état de comparaison sont tous à "0". Si la réponse à l'étape 95 est OUI, l'élément de commande 15 ne confirme pas l'état de comparaison, et il effectue le traitement pour la zone, à l'étape 103.

Si la détermination qui est faite à l'étape
30 95 indique qu'un bit quelconque est un "1", l'élément de commande 15 détermine à l'étape 97 si un bit dans le résultat 1, correspondant au bit "1", est fixé à "1". Il résulte de l'étape 97 que si aucun des bits n'est un "1", l'élément de commande 15 émet des don-
35 nées de réponse qui indiquent l'interdiction d'accès,

à l'étape 101, et la séquence retourne à l'état d'attente de données d'instruction. Il résulte également de l'étape 97 que si un bit quelconque est un "1", l'élément de commande effectue le traitement pour la zone, à l'étape 103.

Si la réponse à l'étape 93 est OUI, l'élément de commande 15 détermine de façon similaire à l'étape 107 si les données de confirmation d'état de comparaison ne contiennent que des "0". Si la réponse à l'étape 107 est OUI, l'élément de commande 15 détermine qu'un accès à la zone correspondante est interdit, et il émet à l'étape 101 des données de réponse qui indiquent l'interdiction d'accès. La séquence retourne ensuite à l'état d'attente de données d'instruction.

Si la détermination qui est faite à l'étape 107 indique qu'un bit quelconque est un "1", l'élément de commande 15 compare ces données de confirmation d'état de comparaison avec le résultat 1. Si la détermination qui est faite à l'étape 111 indique une discordance entre ces données, l'élément de commande 15 émet à l'étape 101 des données de réponse qui indiquent l'interdiction d'accès, et la séquence retourne à l'état d'attente de données d'instruction, à l'étape 31. Si la détermination qui est faite à l'étape 111 indique la découverte d'une coïncidence entre les deux données, l'élément de commande 15 effectue le traitement pour la zone, à l'étape 103. Après le traitement, l'élément de commande 15 émet le résultat du traitement à titre de données de réponse, à l'étape 105, et la séquence retourne ensuite vers l'état d'attente de données d'instruction, à l'étape 31.

Plus précisément, sur la figure 4, pour une zone B, les données logiques des premières données de confirmation d'état de comparaison qui sont ajoutées à

la zone B indiquent une fonction logique ET, "A", et les premières données de confirmation d'état de comparaison sont "10000000". Par conséquent, un accès de lecture à la zone B ne peut être autorisé qu'après une
5 comparaison affirmative pour les données de clé 1. Les secondes données de confirmation d'état de comparaison sont "00000000", et les données logiques associées indiquent une fonction logique OU, "O". Il en résulte que des accès d'écriture et de lecture dirigés vers la
10 zone B peuvent être effectués sans comparaison de données de clé.

Pour une zone C, les premières données de confirmation d'état de comparaison sont "00000000", et les données logiques associées indiquent une fonction
15 logique ET, "A". Un accès de lecture dirigé vers la zone C est donc interdit. Les secondes données de confirmation d'état de comparaison sont "00001100", et les données logiques associées indiquent une fonction logique OU, "O". Il en résulte qu'après une comparaison affirmative pour l'une des données de clé X5 ou
20 X6, des accès d'écriture et d'effacement dirigés vers la zone C sont autorisés.

Après la comparaison des données de clé Y5 et Y6, lorsque le fichier de données d'application 22₁
25 est sélectionné pour effectuer un accès d'écriture dirigé vers la zone C, les états de comparaison des données de clé Y5 et Y6 sont effacés au moment de la sélection du fichier de données, et l'accès à la zone C est interdit.

30 Les états de comparaison de données de clé dans les fichiers de données d'application 22₁ et 22₂ ne sont valides que pour un accès à une zone dans un fichier de données d'application identique.

35 Des données d'identification identiques (KID) sont ajoutées aux données de clé X4 du fichier

de données d'application 22₁ et aux données de clé Y4
du fichier de données d'application 22₂. Lorsque les
données d'identification sont désignées, du fait que
l'un de ces fichiers de données d'application consti-
5 tue un objet sur lequel doit porter l'accès, il n'y
aura pas de confusion entre ces données de clé. On
n'utilise cependant pas des données d'identification
(KID) identiques entre le fichier de données commun et
les autres fichiers de données d'application. Il faut
10 noter que ceci s'applique également aux données
d'identification (AID) qui sont affectées à une zone.

Dans le fichier de données d'application
identique, on peut employer une valeur identique du
fait que les données d'identification (AID) et les
15 données d'identification (KID) peuvent être détermi-
nées sans ambiguïté en fonction des données d'instruc-
tion.

Le nombre de données de confirmation d'état
de comparaison qui est affecté à chaque zone peut
20 être changé en correspondance avec les nombres d'ins-
tructions et d'opérations de traitement pour la zone.

De cette manière, un ensemble de données de
clé (numéros d'identification) sont enregistrées dans
la mémoire de données et sont comparées avec des don-
25 nées d'entrée. Les résultats des comparaisons sont en-
registrés pour chacune des données de clé. Au moment
de l'accès à une zone déterminée de la mémoire de don-
nées, l'accès à la zone est autorisé si l'un des ré-
sultats de comparaison enregistrés est affirmatif, ou
30 si tous les résultats de comparaison enregistrés sont
affirmatifs. On peut fixer l'une ou l'autre de ces
conditions pour chacune des données d'instruction qui
sont utilisées pour accéder à chaque zone de la mé-
moire de données.

35 On peut ainsi fixer arbitrairement, pour

chacune des zones de la mémoire de données, une combinaison de données de clé qui est nécessaire pour accéder à une zone, et on peut fixer une fonction logique ET ou OU conjointement à la combinaison. On peut fixer
5 la combinaison pour chacune des données d'instruction qui sont utilisées pour accéder à chaque zone de la mémoire de données. Une condition d'accès pour chaque zone de la mémoire de données peut donc être fixée de façon fine, ce qui permet d'obtenir une configuration
10 souple pour un système de carte à puce.

Un ensemble de données de décision d'autorisation/interdiction d'accès sont enregistrées en correspondance avec des zones de la mémoire de données. Des données correspondantes de décision d'autorisation/interdiction d'accès sont sélectionnées conformé-
15 ment à des données d'instruction qui sont introduites de façon externe, et une décision d'autorisation/interdiction d'accès pour chaque zone de la mémoire de données est prise conformément aux données de décision
20 d'autorisation/interdiction d'accès qui sont sélectionnées, sur la base du résultat de comparaison des données de clé.

Plus précisément, les différentes données de décision d'autorisation/interdiction d'accès sont établies en correspondance avec des zones de la mémoire
25 de données, et des données de décision d'autorisation/interdiction d'accès sont sélectionnées pour chacune des données d'instruction qu'on utilise pour accéder à chaque zone, pour prendre ainsi la décision d'autorisation/interdiction d'accès.
30

On peut changer une condition d'accès pour chacune des données d'instruction qui sont utilisées pour accéder à chaque zone de la mémoire de données, et des données qui indiquent une correspondance entre
35 les données d'instruction et la condition d'accès sont

enregistrées dans la mémoire de données. On peut donc fixer la correspondance de façon arbitraire, par exemple au moment de la fabrication de la carte à puce.

5 On peut déterminer les points suivants pour chacune des zones de la mémoire de données : si une décision d'autorisation/interdiction d'accès doit être prise pour chaque zone de la mémoire de données, sur la base du résultat de comparaison de données de
10 clé; si un accès à chaque zone de la mémoire de données est autorisé indépendamment du résultat de comparaison des données de clé; ou si un accès à chaque zone de la mémoire de données est interdit indépendamment du résultat de la comparaison des données de
15 clé.

 On utilise des conditions d'interdiction d'accès et de libre accès, dans le cadre des conditions d'accès pour chaque zone de la mémoire de données, et on peut fixer ces conditions d'accès pour
20 chacune des données d'instruction qui sont utilisées pour accéder à chaque zone de la mémoire de données.

 Les conditions d'accès, c'est-à-dire les conditions d'interdiction d'accès et de libre accès, peuvent donc être fixées pour chacune des données
25 d'instruction qui sont utilisées pour accéder à chaque zone de la mémoire de données. On peut donc parvenir à une commande d'accès fine pour la carte à puce.

 Des données de combinaison des résultats de
30 comparaison de données de clé, et des données d'identification (données logiques) destinées à indiquer qu'un accès est autorisé si tous les résultats de comparaison de données de clé qui sont indiqués par la combinaison sont affirmatifs, ou si l'un de ces
35 résultats est affirmatif, sont enregistrées en cor-

5 respondance avec les zones de la mémoire de données.
Des données d'identification (données logiques) qui
sont destinées à indiquer si une décision d'autorisa-
tion/interdiction d'accès est prise pour chaque zone
de la mémoire de données, conformément aux données
de combinaison et aux données d'identification précé-
dentes, sur la base du résultat de comparaison de
données de clé, ou des données d'identification desti-
nées à indiquer si un accès est autorisé sur la base
10 du résultat de comparaison de données de clé, sont en-
registrées en correspondance avec les zones de la mé-
moire de données. On détermine les points suivants
pour chacune des zones de la mémoire de données : si
une décision d'autorisation/interdiction d'accès est
15 prise pour chaque zone de la mémoire de données con-
formément aux données de combinaison et aux données
d'identification, sur la base du résultat de comparai-
son de données de clé; si l'accès à une zone de la mé-
moire de données est interdit sur la base des données
20 de combinaison et des données d'identification, indé-
pendamment du résultat de comparaison de données de
clé; ou si l'accès à chaque zone de la mémoire de don-
nées est autorisé sur la base des données de combinai-
son et des données d'identification indépendamment du
25 résultat de comparaison de données de clé.

On établit ainsi les données de combinaison
de données de clé et des données d'identification qui
indiquent que la combinaison correspond à une fonction
logique ET ou OU, ce qui permet de fixer une condition
30 d'interdiction d'accès ou de libre accès. On peut donc
fixer l'une des conditions suivantes : commande d'ac-
cès, interdiction d'accès et libre accès, sur la base
de la combinaison des données de clé qui sont néces-
saires pour un accès, une fonction logique de com-
35 binaison, à titre de condition d'accès pour chaque

zone de la mémoire de données, avec un faible volume de données.

5 Il va de soi que de nombreuses modifications peuvent être apportées au dispositif et au procédé décrits et représentés, sans sortir du cadre de l'invention.

REVENDEICATIONS

1. Dispositif électronique portable, caracté-
risé en ce qu'il comprend : une mémoire (16) divisée
en un ensemble de zones; des moyens de commande (15)
5 destinés à commander l'accès à la mémoire et à échan-
ger sélectivement des données avec un dispositif ex-
terne; des moyens d'enregistrement de données de clé
(21, 22₁, 22₂) destinés à enregistrer un ensemble de
données de clé; des moyens de comparaison (15, 17)
10 destinés à comparer l'une au moins des données de
l'ensemble de données de clé, avec un ensemble de se-
condes données de clé qui sont sélectivement introdui-
tes au moyen du dispositif externe; des moyens d'enre-
gistrement de résultat de comparaison (23₁, 23₂) des-
15 tinés à enregistrer des résultats de comparaison des
moyens de comparaison, pour chacune des données de
l'ensemble de données de clé; des premiers moyens de
commande d'accès (15, 17, figure 9E) qui sont destinés
à autoriser l'accès à une zone de la mémoire lorsque
20 l'un des résultats de comparaison qui sont enregistrés
dans les moyens d'enregistrement de résultat de compa-
raison est affirmatif; et des seconds moyens de com-
mande d'accès (15, 17, figure 9E) qui sont destinés à
autoriser l'accès à la zone lorsque tous les résultats
25 de comparaison qui sont enregistrés dans les moyens
d'enregistrement de résultat de comparaison sont af-
firmatifs.

2. Dispositif selon la revendication 1, ca-
ractérisé en ce que la mémoire (16) est divisée en un
30 ensemble de zones, et l'un des premiers et seconds
moyens de commande d'accès (15, 17) est utilisé avec
des données d'instruction qui sont appliquées de
l'extérieur, pour permettre ainsi d'accéder à la zone
correspondante dans la mémoire (16).

35 3. Dispositif électronique portable caracté-

risé en ce qu'il comprend : une mémoire (16) divisée en un ensemble de zones; des moyens de commande (15) destinés à commander l'accès à la mémoire et à échanger sélectivement des données avec un dispositif externe; des moyens d'enregistrement de données de clé (21, 22₁, 22₂) qui sont destinés à enregistrer un ensemble de données de clé; des moyens de comparaison (15, 17) qui sont destinés à comparer l'une au moins des données de l'ensemble de données de clé avec un ensemble de secondes données de clé qui sont appliquées sélectivement par le dispositif externe; des moyens d'enregistrement de données de décision d'autorisation/interdiction d'accès (21, 22₁, 22₂) qui sont destinés à enregistrer un ensemble de données de décision d'autorisation/interdiction d'accès, correspondant respectivement à l'ensemble de zones divisées; des moyens de sélection (figure 8) pour sélectionner une donnée correspondante parmi l'ensemble de données de décision d'autorisation/interdiction d'accès, conformément à des données d'instruction qui sont appliquées de l'extérieur; et des moyens de décision (15, 17) destinés à prendre une décision d'autorisation / interdiction d'accès pour une zone de l'ensemble de zones, conformément à des données de décision d'autorisation/interdiction d'accès qui sont sélectionnées par les moyens de sélection, sur la base du résultat de comparaison des moyens de comparaison (15, 17).

4. Dispositif électronique portable, caractérisé en ce qu'il comprend : une mémoire (16) divisée en un ensemble de zones; des moyens de commande (15) qui sont destinés à commander l'accès à la mémoire et à échanger sélectivement des données avec un dispositif externe; des moyens d'enregistrement de données de clé (21, 22₁, 22₂) qui sont destinés à enregistrer un ensemble de données de clé; des moyens

de comparaison (15, 17) qui sont destinés à comparer l'une au moins des données de l'ensemble de données de clé avec un ensemble de données de clé qui sont appliquées sélectivement par le dispositif externe; des
5 moyens de décision d'autorisation/interdiction d'accès (15, 17) qui sont destinés à prendre une décision d'autorisation/interdiction d'accès pour une zone de l'ensemble de zones, sur la base d'un résultat de comparaison des moyens de comparaison (15, 17); des
10 moyens d'autorisation d'accès (15, 17) qui sont destinés à autoriser l'accès à la zone précitée parmi l'ensemble de zones, indépendamment du résultat de comparaison des moyens de comparaison (15, 17); des
15 moyens d'interdiction d'accès (15, 17) qui sont destinés à interdire l'accès à la zone, indépendamment du résultat de comparaison des moyens de comparaison (15, 19); et des moyens de sélection (figure 8) destinés à sélectionner, pour chacune des zones, les moyens à
20 utiliser parmi les moyens de décision d'autorisation/interdiction d'accès, les moyens d'autorisation d'accès et les moyens d'interdiction d'accès.

5. Dispositif électronique portable, caractérisé en ce qu'il comprend : une mémoire (16) divisée en un ensemble de zones; des moyens de commande (15)
25 destinés à commander l'accès à la mémoire (16) et à échanger sélectivement des données avec un dispositif externe; des moyens d'enregistrement de données de clé (21, 22₁, 22₂) qui sont destinés à enregistrer un ensemble de données de clé; des moyens de comparaison
30 (15, 17) qui sont destinés à comparer l'une au moins des données de l'ensemble de données de clé avec un ensemble de secondes données de clé qui sont appliquées sélectivement par le dispositif externe; des
35 moyens d'enregistrement de données d'identification (21, 22₁, 22₂) qui sont destinés à enregistrer, en

correspondance avec les zones, des données de combinaison des résultats de comparaison de l'ensemble de données de clé par les moyens de comparaison, ces moyens d'enregistrement de données d'identification

5 enregistrant également des données d'identification pour indiquer qu'un accès est autorisé si tous les résultats de comparaison des données de clé qui sont indiquées par les données de combinaison sont affirmatifs, ou si l'un des résultats de comparaison est affirmatif;

10 des moyens de décision d'autorisation/interdiction d'accès (15, 17) destinés à prendre une décision d'autorisation/interdiction d'accès pour une zone de l'ensemble de zones, conformément aux données de combinaison et aux données d'identification, sur la

15 base du résultat de comparaison des moyens de comparaison (15, 17); des moyens d'autorisation d'accès (15, 17) qui sont destinés à autoriser l'accès à la zone conformément aux données de combinaison et aux données d'identification, indépendamment du résultat

20 de comparaison des moyens de comparaison; des moyens d'interdiction d'accès (15, 17) qui sont destinés à interdire l'accès à la zone conformément aux données de combinaison et aux données d'identification, indépendamment du résultat de comparaison des moyens de

25 comparaison; et des moyens de sélection (figure 8) destinés à sélectionner, pour chacune des zones, les moyens à utiliser parmi les moyens de décision d'autorisation/interdiction d'accès, les moyens d'autorisation d'accès et les moyens d'interdiction d'accès.

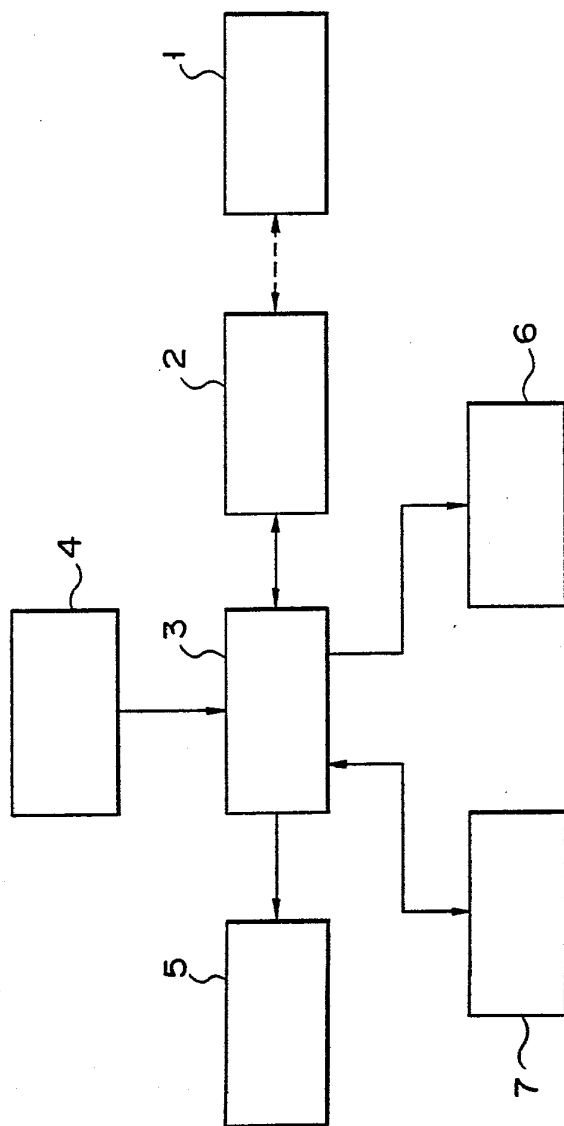


FIG. 1

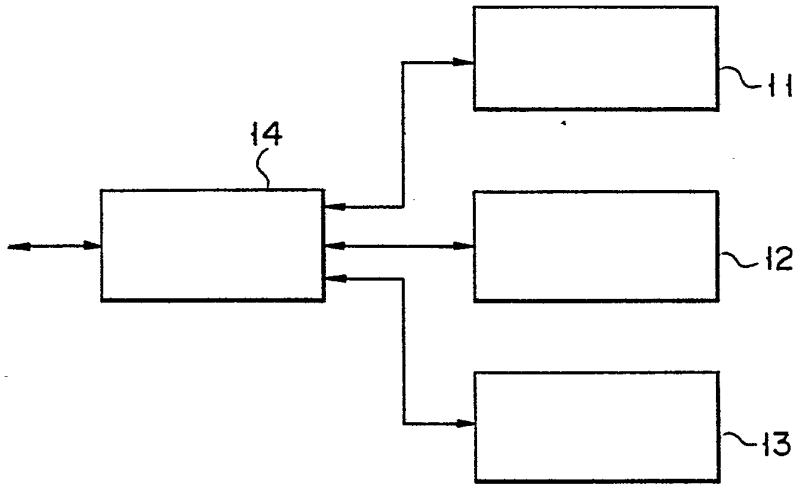


FIG. 2

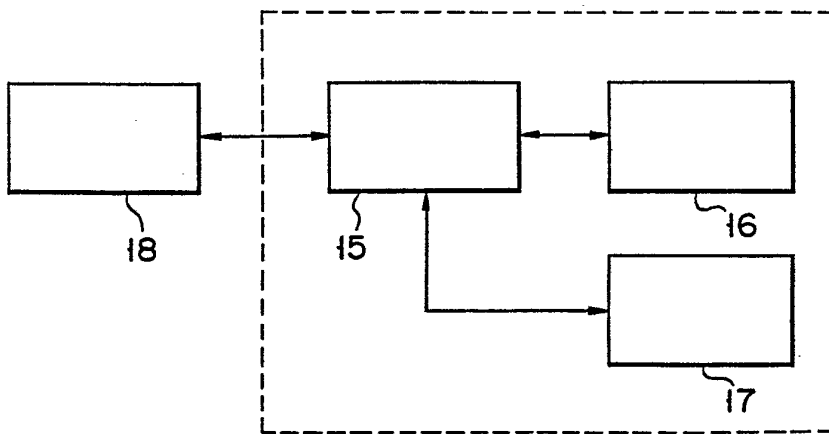


FIG. 3

KID01	<table border="1"> <tr><td>DONNÉES 1</td><td>10000000</td></tr> <tr><td>DE CLÉ</td><td></td></tr> </table>	DONNÉES 1	10000000	DE CLÉ		AIDgg	<table border="1"> <tr><td>ZONE G</td><td>10000000</td></tr> <tr><td></td><td>10000000</td></tr> </table>	ZONE G	10000000		10000000	A
DONNÉES 1	10000000											
DE CLÉ												
ZONE G	10000000											
	10000000											
KID02	<table border="1"> <tr><td>DONNÉES 2</td><td>01000000</td></tr> <tr><td>DE CLÉ</td><td></td></tr> </table>	DONNÉES 2	01000000	DE CLÉ		AIDhh	<table border="1"> <tr><td>ZONE H</td><td>10000000</td></tr> <tr><td></td><td>01000000</td></tr> </table>	ZONE H	10000000		01000000	A
DONNÉES 2	01000000											
DE CLÉ												
ZONE H	10000000											
	01000000											
KID03	<table border="1"> <tr><td>DONNÉES 3</td><td>00100000</td></tr> <tr><td>DE CLÉ</td><td></td></tr> </table>	DONNÉES 3	00100000	DE CLÉ								
DONNÉES 3	00100000											
DE CLÉ												
KID04	<table border="1"> <tr><td>DONNÉES X4</td><td>00010000</td></tr> <tr><td>DE CLÉ</td><td></td></tr> </table>	DONNÉES X4	00010000	DE CLÉ		AIDaa	<table border="1"> <tr><td>ZONE A</td><td>10000000</td></tr> <tr><td></td><td>10010000</td></tr> </table>	ZONE A	10000000		10010000	A
DONNÉES X4	00010000											
DE CLÉ												
ZONE A	10000000											
	10010000											
KID05	<table border="1"> <tr><td>DONNÉES X5</td><td>00001000</td></tr> <tr><td>DE CLÉ</td><td></td></tr> </table>	DONNÉES X5	00001000	DE CLÉ		AIDbb	<table border="1"> <tr><td>ZONE B</td><td>10000000</td></tr> <tr><td></td><td>00000000</td></tr> </table>	ZONE B	10000000		00000000	A
DONNÉES X5	00001000											
DE CLÉ												
ZONE B	10000000											
	00000000											
KID06	<table border="1"> <tr><td>DONNÉES X6</td><td>00000100</td></tr> <tr><td>DE CLÉ</td><td></td></tr> </table>	DONNÉES X6	00000100	DE CLÉ		AIDCC	<table border="1"> <tr><td>ZONE C</td><td>00000000</td></tr> <tr><td></td><td>00001100</td></tr> </table>	ZONE C	00000000		00001100	O
DONNÉES X6	00000100											
DE CLÉ												
ZONE C	00000000											
	00001100											
KID04	<table border="1"> <tr><td>DONNÉES Y4</td><td>00010000</td></tr> <tr><td>DE CLÉ</td><td></td></tr> </table>	DONNÉES Y4	00010000	DE CLÉ		AIDdd	<table border="1"> <tr><td>ZONE D</td><td>10000000</td></tr> <tr><td></td><td>10001000</td></tr> </table>	ZONE D	10000000		10001000	A
DONNÉES Y4	00010000											
DE CLÉ												
ZONE D	10000000											
	10001000											
KID05	<table border="1"> <tr><td>DONNÉES Y5</td><td>00001000</td></tr> <tr><td>DE CLÉ</td><td></td></tr> </table>	DONNÉES Y5	00001000	DE CLÉ		AIDee	<table border="1"> <tr><td>ZONE E</td><td>10000000</td></tr> <tr><td></td><td>00010000</td></tr> </table>	ZONE E	10000000		00010000	O
DONNÉES Y5	00001000											
DE CLÉ												
ZONE E	10000000											
	00010000											
KID06	<table border="1"> <tr><td>DONNÉES Y6</td><td>00000100</td></tr> <tr><td>DE CLÉ</td><td></td></tr> </table>	DONNÉES Y6	00000100	DE CLÉ		AIDff	<table border="1"> <tr><td>ZONE F</td><td>10000000</td></tr> <tr><td></td><td>00001000</td></tr> </table>	ZONE F	10000000		00001000	O
DONNÉES Y6	00000100											
DE CLÉ												
ZONE F	10000000											
	00001000											

21

FIG. 4

DFN = XXX

221

DFN = YYY

222

4/10

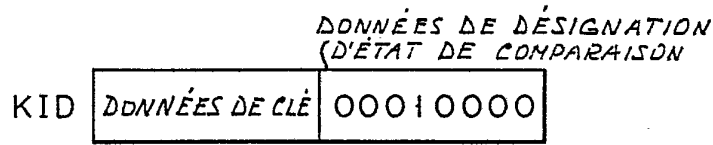


FIG. 5

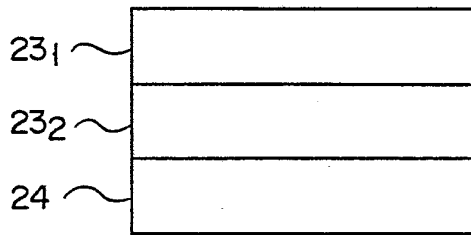


FIG. 6

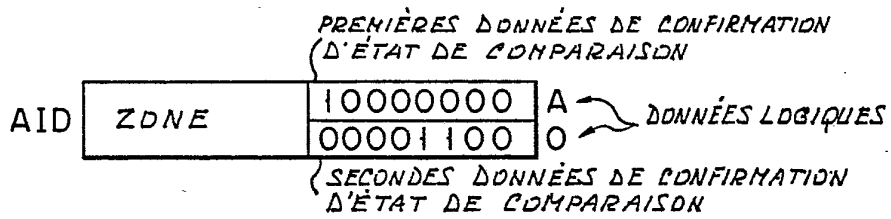


FIG. 7

CODE D'INSTRUCTION	DONNÉES DE SÉLECTION
X X	*
Y Y	*
Z Z	1
W W	2
V V	2

FIG. 8

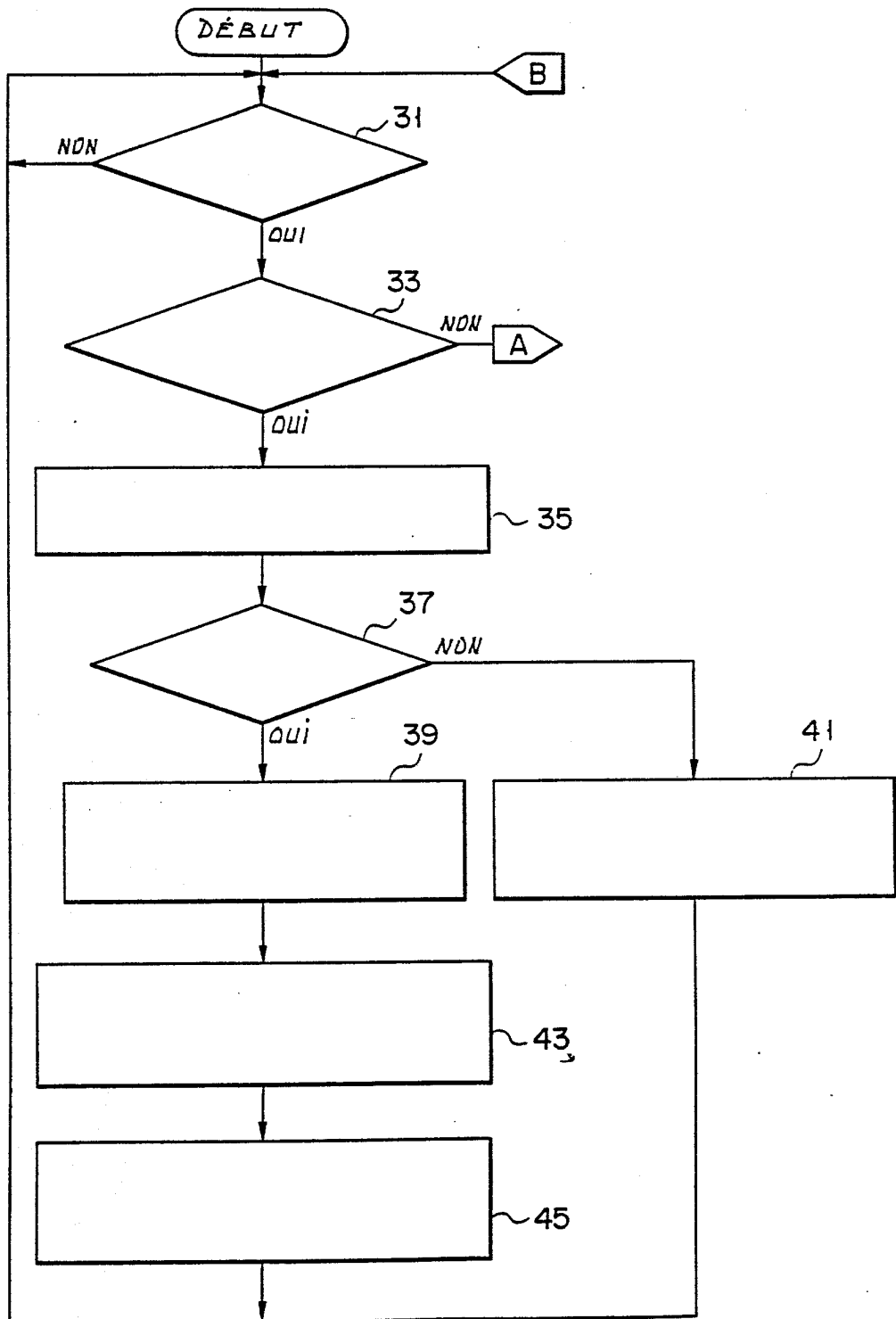


FIG. 9A

8/10

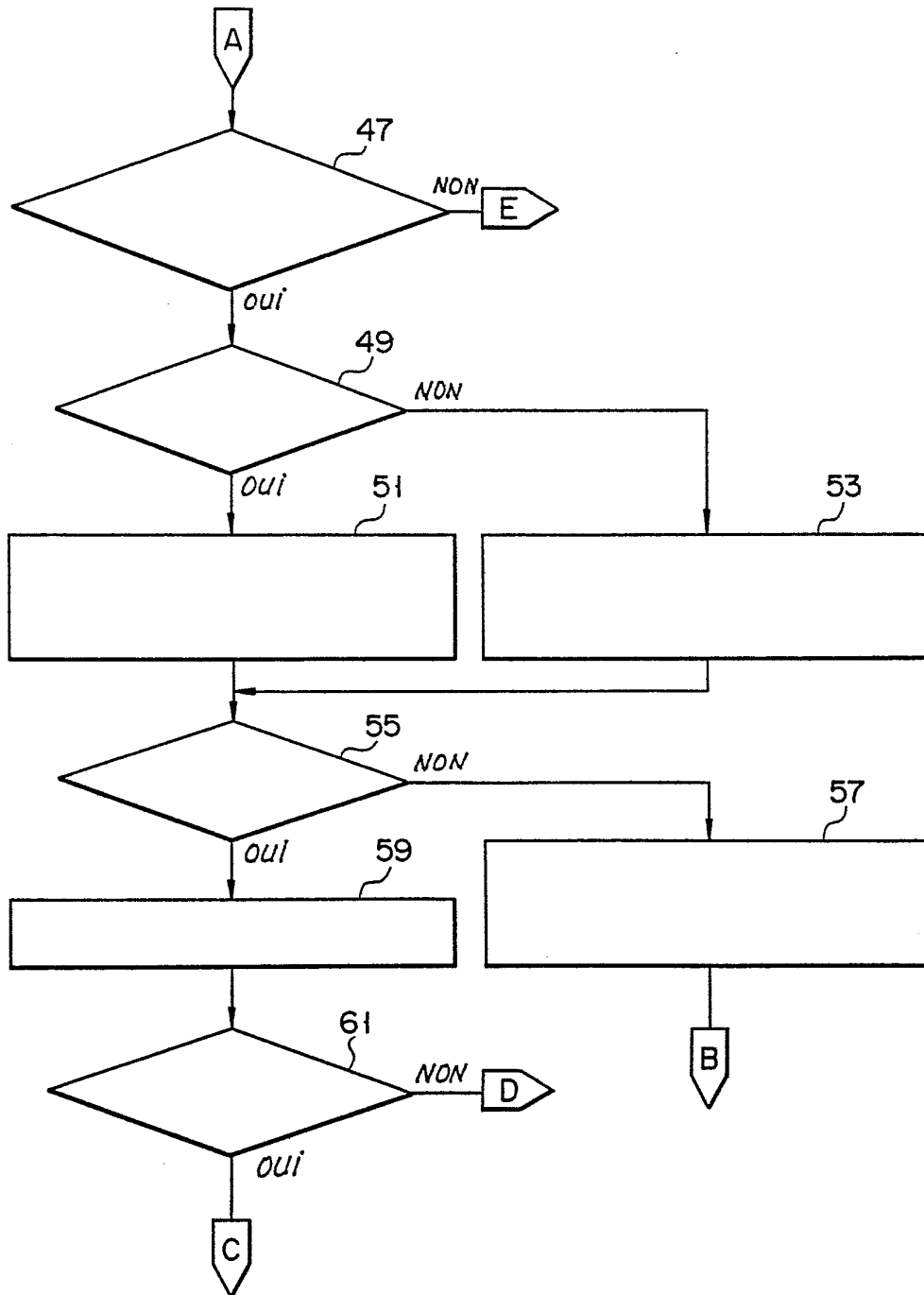


FIG. 9B

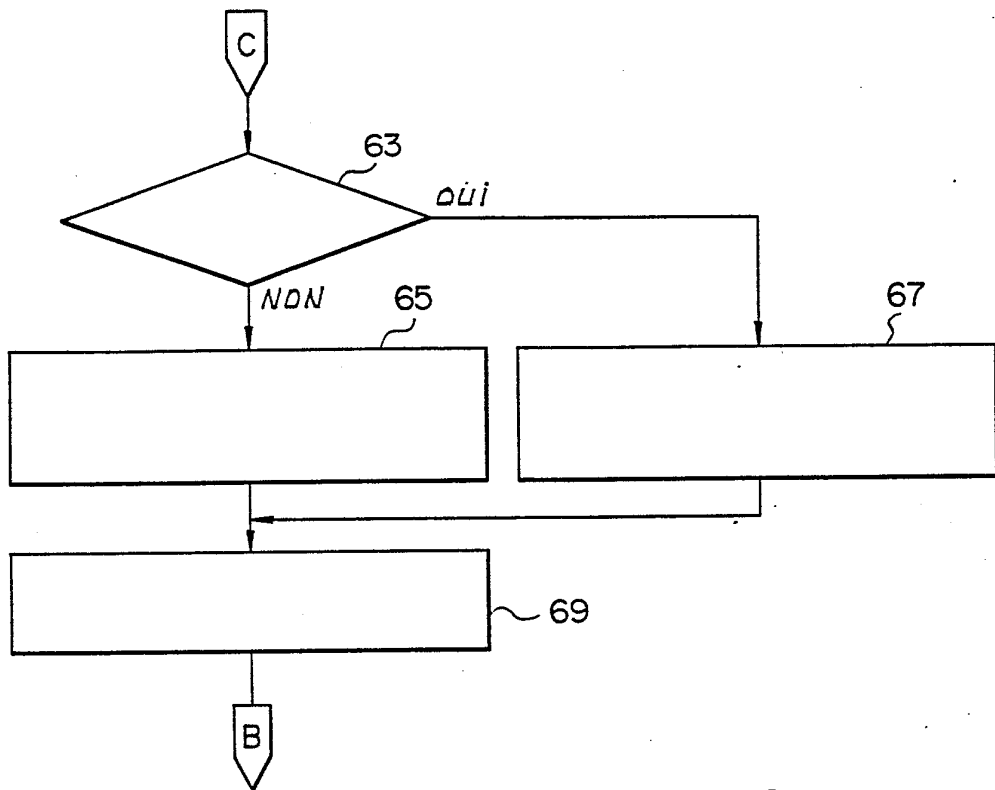
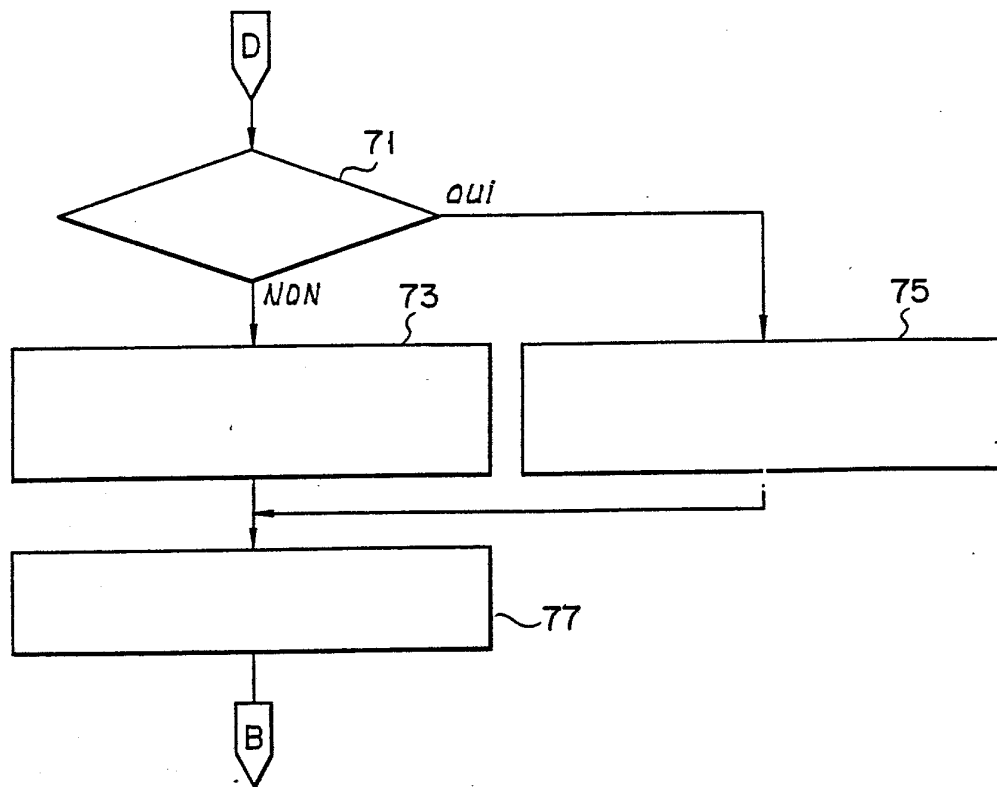


FIG. 9C



8/10

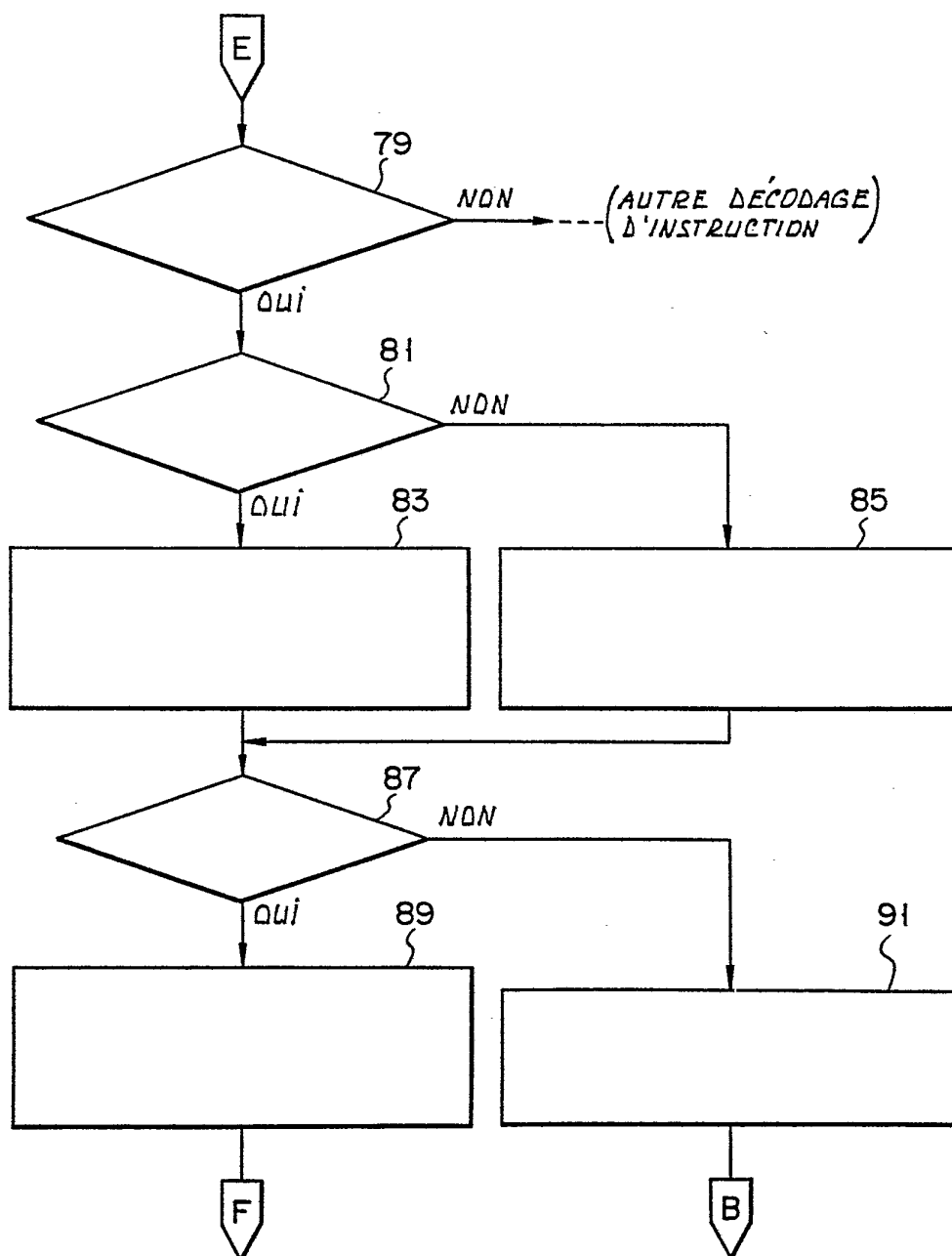


FIG. 9D

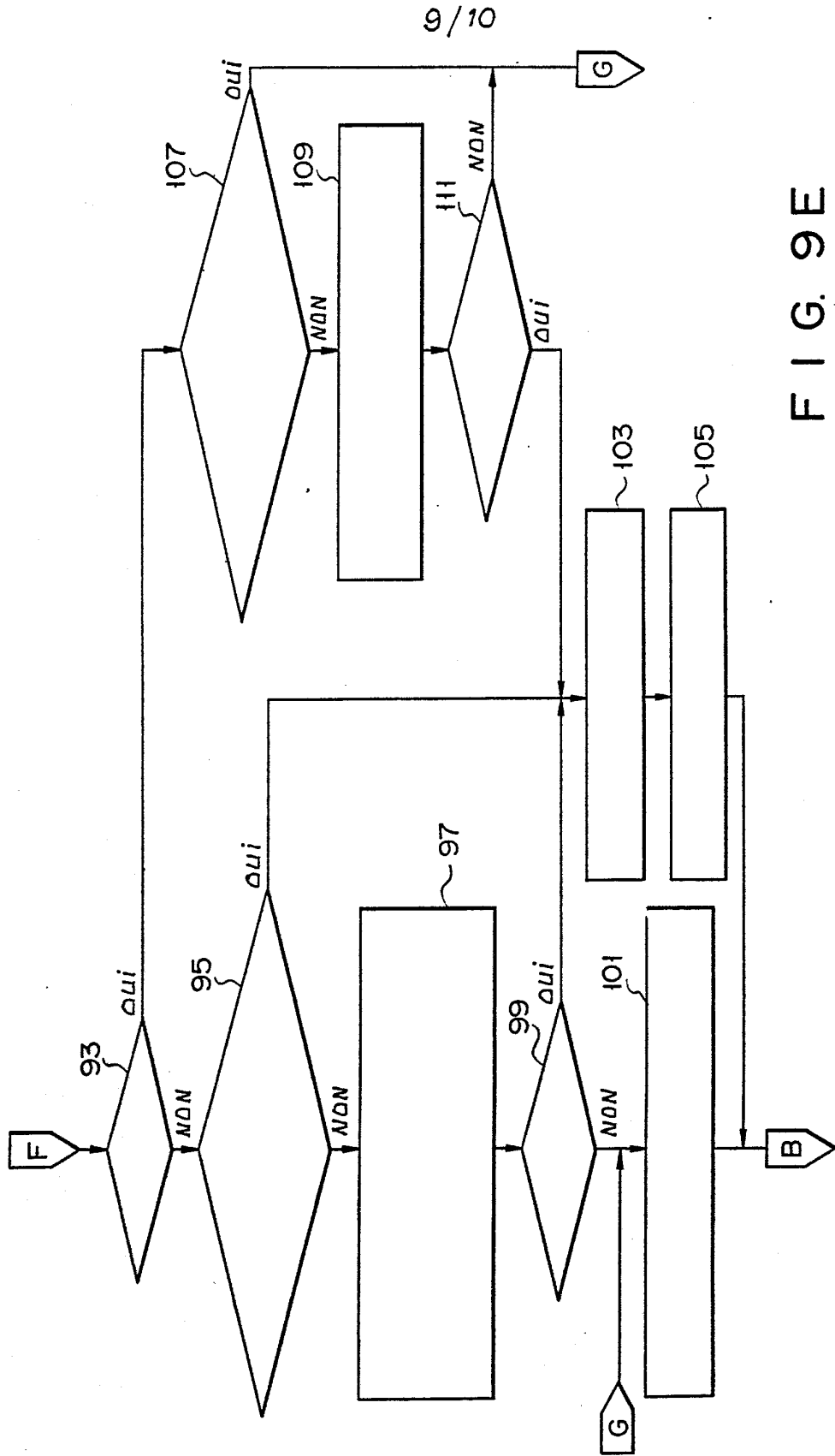


FIG. 9E

10/10

CODE D'INSTRUCTION DE
SÉLECTION DE FICHIER DE DONNÉES

XX	NOM DE FICHIER DE DONNÉES
----	------------------------------

FIG. 10

CODE D'INSTRUCTION DE COMPARAISON
DE DONNÉES DE CLÉ

YY	KID	DONNÉES DE CLÉ
----	-----	----------------

FIG. 11

CODE D'INSTRUCTION
DE LECTURE

ZZ	AID
----	-----

FIG. 12A

CODE D'INSTRUCTION
D'EFFACEMENT

VV	AID
----	-----

FIG. 12C

CODE D'INSTRUCTION D'ÉCRITURE

WW	AID	DONNÉES À ÉCRIRE
----	-----	------------------

FIG. 12B