CH 627 570 A5

(19) CONFÉDÉRATION SUISSE
OFFICE FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE

(51) Int. Cl.³: G 06 K 9/62
G 06 K 7/00

Brevet d'invention délivré pour la Suisse et le Liechtenstein
Traité sur les brevets, du 22 décembre 1978, entre la Suisse et le Liechtenstein

(12) FASCICULE DU BREVET A5

(11) 627 570

(21) Numéro de la demande: 9089/78

(22) Date de dépôt: 29.08.1978

(30) Priorité(s): 16.09.1977 FR 77 28049

(24) Brevet délivré le: 15.01.1982

(45) Fascicule du brevet publié le: 15.01.1982

(73) Titulaire(s):
Compagnie Internationale pour l'Informatique
CII-Honeywell Bull, Paris (FR)

(72) Inventeur(s):
Georges Giraud, Le Vésinet (FR)
Jean Henri Mollier, Bougival (FR)

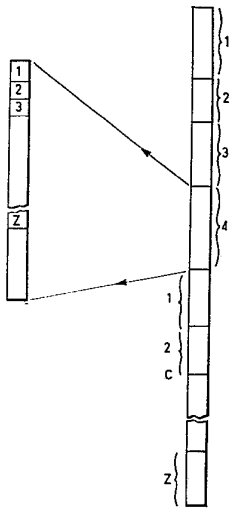
(74) Mandataire:
Dr. A.R. Egli & Co., Patentanwälte, Zürich

(54) Dispositif de comptabilisation d'unités homogènes prédéterminées.

(57) Le dispositif comprend un objet porteur d'informations et des moyens externes d'inscription et/ou d'exploitation desdites informations.

La mémoire de l'objet porteur d'informations comprend une première zone (1) permettant d'inscrire le code d'identification dudit objet permettant son utilisation dans les appareils d'exploitation appropriés, une zone (2) permettant d'identifier la valeur attachée à l'unité de crédit pour un usage déterminé, une zone (3) permettant d'inscrire un numéro d'ordre et une zone (4) permettant la validation des zones numérotées de 1 à Z.

Application : Cartes de crédit.



REVENDICATIONS

1. Dispositif de comptabilisation d'unités homogènes prédéterminées à l'aide d'un objet porteur d'informations et de moyens externes d'inscription et/ou d'exploitation desdites informations, ledit objet comportant une mémoire, des circuits de commande de la mémoire et des moyens pour effectuer l'accouplement temporaire de l'objet avec lesdits moyens d'inscription et/ou d'exploitation constitués par des moyens de lecture et d'écriture de données dans ladite mémoire, la mémoire de l'objet comportant, sous forme codée, des informations sur l'usage auquel l'objet est destiné, sur l'unité dans laquelle sont comptabilisées les opérations réalisées et sur le nombre d'unités disponibles cependant que lesdits moyens d'écriture et de lecture comprennent des moyens pour écrire dans la mémoire de l'objet le nombre d'unités désirées ou reçues par le détenteur, ce dispositif étant caractérisé en ce que la mémoire est divisée en trois parties, à savoir une partie où sont emmagasinées les informations sur les unités et le numéro d'ordre de l'objet, une partie dite champ de validation à laquelle on a accès par une clé prédéterminée incorporée dans l'objet et accessible seulement par les moyens d'écriture et de lecture de la mémoire de l'objet et une troisième partie affectée au stockage des unités, fractionnée en zones individuellement validables.

2. Dispositif selon la revendication 1, caractérisé en ce qu'au moins une des zones où sont emmagasinées les informations sur les unités est sub-divisée en plusieurs sous zones affectées l'une à des unités élémentaires et les autres à des multiples, ou sous-multiples de ces unités élémentaires, à chacune de ces zones correspondant une zone de validation à l'intérieur dudit champ de validation.

3. Dispositif selon la revendication 1 ou 2 caractérisé en ce que ledit objet comporte un générateur d'adresse relié à la mémoire de l'objet et à un générateur de signaux de contrôle, le générateur d'adresse recevant des informations, d'une part, desdits moyens d'écriture et de lecture de la mémoire, et d'autre part, d'un générateur de clé incorporé à l'objet, lesdits moyens d'écriture et de lecture comportant également un générateur de clé susceptible de reconstituer ladite clé de l'objet et chargé de coder les informations à destination de l'objet.

4. Dispositif selon la revendication 3, caractérisé en ce que le générateur d'adresse comprend un registre d'adresse incidente relié au générateur de clé de l'objet et à l'entrée de la mémoire, un registre d'adresse effective relié à la sortie de la mémoire, un comparateur relié aux deux registres susnommés et un sélecteur relié au comparateur et susceptible d'établir la connexion entre la sortie du registre d'adresse incidente avec les entrées d'adressage de la mémoire.

5. Dispositif selon la revendication 3 ou 4, caractérisé en ce que dans le cas de non-concordance entre l'adresse effective et l'adresse reçue desdits moyens d'écriture de la mémoire, le générateur d'adresse adresse la dernière cellule de la mémoire.

6. Dispositif selon l'une des revendications 1 à 5, caractérisé en ce que les moyens d'inscription comportent une mémoire destinée à emmagasiner les clés des objets.

7. Dispositif selon la revendication 1, caractérisé en ce que l'objet porteur d'informations est constitué par une carte.

La présente invention concerne un dispositif de comptabilisation d'unité homogènes prédéterminées à l'aide d'un objet porteur d'informations et de moyens externes d'inscription et/ou d'exploitation desdites informations et plus particulièrement aux systèmes du type décrit dans le brevet FR 77 09822 (2386080) déposé au nom de la titulaire et intitulé: «Dispositif de comptabilisation d'unités homogènes prédéterminées».

Les dispositifs de ce type sont formés d'un objet porteur d'un quantum initial et chargé d'enregistrer des quantités correspondant à des prestations reçues ou accomplies, d'un appareil capable d'inscrire dans l'objet ledit quantum initial, d'un appareil susceptible de modifier dans l'objet le quantum disponible d'une quantité correspondant à la prestation désirée ou reçue dont la délivrance est validée par ledit appareil et d'un système de liaison entre l'objet et lesdits appareils.

Le but de ces dispositifs est de permettre de créer des supports de transaction ou d'enregistrement capables d'enregistrer des valeurs entières d'unités et de servir de saisie et de comptabilisation des données de la transaction ou de l'enregistrement effectué.

Le dispositif décrit dans le brevet précité comprend notamment un objet porteur d'informations constitué par une carte, par exemple, sur laquelle est inscrit, en langage codé, sous forme d'un certain nombre d'unités égales distinctes, un certain quantum de prestations désirées.

Au moment où l'utilisateur se procure une carte, celle-ci contient donc dans sa mémoire un crédit déterminé qui pourra être incrémenté au gré de l'utilisation et passera ainsi de la valeur initiale à la valeur zéro.

La mémoire de la carte n'étant pas réutilisable une fois incrémentée, la carte, une fois vide, ne peut plus servir à nouveau et doit être rendue par l'utilisateur lorsqu'il veut se procurer une nouvelle carte.

Si la carte doit satisfaire une quantité importante de prestations la valeur initiale inscrite dans la carte peut être très grande, ce qui aboutit à une mise de fond importante au moment de l'achat de la carte.

Il est donc apparu souhaitable, afin de rendre la carte plus rentable et plus abordable, de prévoir la possibilité de la valider par fraction.

Le but de l'invention est de permettre cette possibilité de «recharge» tout en conservant au système une très grande résistance à la fraude éventuelle.

A cet effet, l'invention a pour objet un dispositif de comptabilisation d'unités homogènes prédéterminées à l'aide d'un objet porteur d'informations et de moyens externes d'inscription et/ou d'exploitation desdites informations ledit objet comportant une mémoire, des circuits de commande de la mémoire et des moyens pour effectuer l'accouplement temporaire de l'objet avec lesdits moyens d'inscription et/ou d'exploitation constitués par des moyens de lecture et d'écriture de données dans ladite mémoire, la mémoire de l'objet comportant, sous forme codée, des informations sur l'usage auquel l'objet est destiné, sur l'unité dans laquelle sont comptabilisées les opérations réalisées et sur le nombre d'unités disponibles, cependant que lesdits moyens d'écriture et de lecture comprennent des moyens pour écrire dans la mémoire de l'objet le nombre d'unités désirées ou reçues par le détenteur, ce dispositif étant caractérisé en ce que la mémoire est divisée en trois parties, à savoir une partie où sont emmagasinées les informations sur les unités et le numéro d'ordre de l'objet une partie dite champ de validation à laquelle on a accès par une clé prédéterminée incorporée dans l'objet et accessible seulement par les moyens d'écriture et de lecture de la mémoire de l'objet et une troisième partie affectée au stockage des unités, fractionnée en zones individuellement validables.

Avec un tel dispositif l'objet peut être validé pour une ou plusieurs zones et pourra par la suite, être validé pour de nouvelles zones jusqu'à épuisement de la capacité totale de la mémoire de l'objet.

Puisqu'il y a possibilité au cours de la vie d'un objet de va-

lider d'autres zones de la mémoire, il faut donc éviter les tentatives de fraude qui consisteraient à vouloir valider, en dehors des machines d'inscription prévue à cet effet, d'autres zones de la mémoire. C'est le but de la clé incorporée dans l'objet.

D'autres caractéristiques et avantages ressortiront de la description qui va suivre d'un mode de réalisation du dispositif de l'invention, description donnée à titre d'exemple, uniquement et en regard des dessins annexés sur lesquels:

Fig. 1 représente un schéma d'organisation du contenu informatique d'un objet selon l'invention.

Fig. 2 représente le schéma logique général des circuits portés par l'objet et d'une partie des circuits des moyens d'inscription et/ou d'utilisation de l'objet.

Fig. 3 représente un schéma logique plus détaillé du générateur d'adresse du dispositif de la figure 2.

Fig. 4 représente un schéma logique plus détaillé des circuits de l'objet.

Fig. 5 représente un schéma logique détaillé du générateur de clé du dispositif de la figure 2.

Fig. 6 représente un schéma logique détaillé du générateur d'adresse du dispositif de la figure 4.

Fig. 7 et 8 représentent respectivement les diagrammes des signaux de cycles et des signaux de phases pour l'écriture ou la lecture du contenu informatique de l'objet.

Fig. 9 représente le formatage d'une zone permettant d'attribuer à chaque bit des valeurs différentes.

La fig. 1 représente le schéma de l'organisation du contenu informatique d'un objet, tel qu'une carte par exemple, selon l'invention. Ce contenu informatique est sous forme binaire.

En tête de la carte est inscrit en 1 le code d'identification de la carte permettant l'utilisation de celle-ci dans les appareils d'exploitation appropriés.

En 2, est inscrit le code permettant d'identifier dans un type d'utilisation donné la valeur attachée à l'unité de crédit.

En 3, est inscrit un numéro de service ou d'ordre permettant l'identification de la carte.

Ces trois codes 1, 2 et 3 sont irréversibles, c'est-à-dire qu'ils ne doivent pas pouvoir être manipulés de manière à transformer un code déterminé reconnu par un appareil d'exploitation en un autre code également reconnu par l'appareil, mais affecté à un autre type de prestation.

A cet effet, pour ces codes, on utilise des champs de n bits dans lesquels le passage d'un état de chaque bit dans l'autre état est irréversible.

Pour plus de détails sur un tel codage, on pourra se reporter à la demande de brevet précitée.

En 4 se trouve un champ de validation d'un certain nombre de zones numérotées de 1 à Z.

Ce champ de validation 4 groupe Z bits numérotés 1 à Z et correspondant chacun à l'une des zones 1 à Z.

Le passage à 1 irréversible de l'un des bits du champ 4 valide la zone correspondante. Afin de donner plus de souplesse à l'exploitation de la carte, les valeurs des bits de différentes zones 1 à Z ne sont pas les mêmes.

Par exemple, dans une zone le bit peut prendre différentes valeurs unitaires suivant sa fonction dans la zone, selon la fig. 9, un bit dans la sous zone suivant sa fonction dans la zone, selon la fig. 9, un bit dans la sous zone la valeur υ, un bit dans la sous zone 2 a la valeur 5 υ, un bit dans la sous zone 3 a la valeur 10 υ, un bit dans la sous zone 4 a la valeur 20 υ, un bit dans la sous zone 5 a la valeur 50 υ, un bit dans la sous zone 6 a la valeur 100 υ.

Le rôle du champ de validation 4 est de préciser à la machine d'exploitation de la carte, le ou les zones (1 à Z) à exploiter, l'expression «exploiter une zone» signifiant le passage sous la commande de la machine d'exploitation de 0 à 1, de un ou plusieurs bits de la zone en question.

Comme dans la demande de brevet précitée le passage des bits de la ou les zones incrémentables de la mémoire de la carte se fait de manière ittéversible de 0 à 1 lors de l'exploitation de la carte.

Lorsque la ou les zones incrémentables sont épuisées on peut réutiliser la carte en autorisant l'exploitation d'une ou de plusieurs autres zones restantes de la carte, cette opération s'effectuant en introduisant la carte dans une machine d'inscription ou machine à créditer appropriée.

Afin d'éviter toutes possibilité de fraude, l'adresse du bit de validation dans la carte est envoyée brouillée à la carte, à partir de la machine à créditer par une clé, identique à celle résidant dans la carte. Ladite clé étant au niveau de la machine à créditer, retrouvée dans une mémoire protégée grâce au numéro de service ou d'ordre 3.

La fig. 2 représente le schéma logique général du dispositif selon l'invention. Au niveau de la carte, le dispositif comprend une mémoire 10 programmable du type PROM adressée par un générateur cyclique d'adresse 11 recevant des signaux de synchronisation d'une horloge (signal H) située dans la machine d'inscription ou d'exploitation de la carte.

La mémoire 10 peut communiquer avec l'extérieur par une borne d'entrée EM et une borne de sortie SM.

L'entrée EM reçoit le signal S en provenance de la machine, ce signal étant également appliqué à une porte OU EXCLUSIF 12 dont une seconde entrée est reliée à la sortie d'un registre à décalage circulaire 13 chargé de fournir une clé C de codage.

La sortie de la porte OU EXCLUSIF 12 est reliée au générateur d'adresse 11.

La sortie SM de la mémoire 10 est reliée au générateur d'adresse 11 et à travers l'élément 24 à la ligne reliant la carte à la machine et véhiculant les signaux E et S, E étant le signal émis par la carte à destination de la machine d'inscription ou d'exploitation.

Au générateur d'adresse 11 est connecté un générateur 14 de signaux de cycles et de phases (signaux de contrôle) qui sera exploité par la suite.

Au niveau de la machine, outre les circuits destinés à l'inscription et à la lecture de la carte qui ne sont pas représentés mais qui sont identiques à ceux décrits et représentés dans la demande de brevet précitée, il est prévu un registre à décalage circulaire 15 destiné à engendrer une clé M selon les indications fournies à partir du numéro de service ou d'ordre 3 de la carte. Ce registre 15 est relié à une porte OU EXCLUSIF 16 dont une seconde entrée reçoit les adresses élaborées par la machine et dont la sortie est connectée à la ligne véhiculant les signaux E et S. La machine comprend en outre une mémoire 67 reliée à la ligne E/S et destinée à la mémorisation des informations lues dans la carte à chaque transaction. Le signal d'horloge H nécessaire à la synchronisation des échanges entre la carte et la machine est fourni par une horloge 6B.

La fig. 3 représente un schéma plus détaillé de générateur d'adresse 11 de la fig. 2.

Ce générateur comprend un comparateur 17 recevant les signaux de sorties d'un registre d'adresse effective 18 et d'un registre d'adresse incidente 19.

Le registre 18 est relié à la sortie SM de la mémoire 10 et le registre 19 est relié à la porte OU EXCLUSIF 12.

La sortie du comparateur 17 est reliée à un sélecteur 20 recevant également le signal de sortie du registre 19 et générant les adresses A0 à A10.

La fig. 4 représente un schéma logique plus détaillé des circuits de la carte de la fig. 2.

On a représenté en 10 la mémoire, en 11 le générateur

d'adresse, en 21 le générateur de clé, en 14 le générateur de signaux de cycles et de phases, et en 22, un élément fournissant les tensions V1 d'alimentation des circuits logiques de la carte et V2 de programmation de la mémoire 10, ainsi que le signal de remise à zéro RAZ transformé en signal $\overline{RAZ}$ par un inverseur 23.

Le générateur 14 est constitué par un registre à décalage fournissant les signaux de cycles C1 à C5 (figure 7) et les signaux de phases φ 1, φ 2, φ 3, φ 4, φ 7, (figures 7 et 8) les signaux de phases φ 5 et φ 6, étant générés par le générateur d'adresse 11 (voir figure 6).

La sortie SM de la mémoire 10 est relié à la ligne de liaison véhiculant les signaux E et S par l'intermédiaire d'une porte logique ET 24 validée par les signaux de cycles C1, C3 et C5.

La mémoire 10 comporte une entrée de commande d'écriture CE, reliée à un élément 25 comprenant une porte logique ET 26 et deux portes logiques NON ET 27 - et 28 recevant respectivement les signaux C4, φ 7 et C2 φ 5.

Le générateur de clé 21 reçoit les signaux φ 1, φ 3, C2, H et RAZ et 1r générateur d'adresse 11 reçoit les signaux φ 1, φ 2, φ 3, φ 4, C2 RAZ et $\overline{RAZ}$ ainsi que le signal S provenant de la machine (inscription et exploitation), il émet outre les bits d'adresse A0 à A10 le signal φ 5.

La fig. 5 représente un schéma logique détaillé du générateur de clé 21 de la figure 4. Le générateur comprend un élément 30 qui fixe l'état logique des broches A, B, C et D de deux registres à décalage 31 et 32 définissant la clé C.

La commande du générateur s'effectue par une porte logique NON ET 33 recevant les signaux C2 et φ 1, et par une porte logique OU 34 recevant les signaux C2, φ 3 et H par l'intermédiaire d'une porte logique ET 35 et le signal de la porte 33, par l'intermédiaire d'un inverseur 36 et d'une porte logique ET 37 validée par le signal H.

La fig. 6 représente un schéma logique détaillé du générateur d'adresse 11 de la figure 4.

Ce générateur comprend un compteur formé par les registres 41, 42 et 43 et qui est chargé de générer les adresses A0 à A10.

Les éléments 44, 45 et 46 sont des registres chargés de recevoir d'une part l'adresse effective du bit à valider, d'autre part l'adresse incidente élaborée par le comparateur 51. Au comparateur 17 de la figure 3 correspondent les deux bascules bistables 47 et 48 commandant le compteur (41, 42, 43) par l'intermédiaire d'une porte logique ET 49 validée par le signal C2. La bascule 47 est commandée par une porte logique OU EXCLUSIF 50 reliée d'une part à la sortie du registre et à la sortie d'une autre porte logique OU EXCLUSIF 51 recevant le signal appliqué à l'entrée EM de la mémoire 10 et validé par le signal de clé C.

Le signal de sortie de la porte 51 commande également les registres 44 à 46.

La bascule 48 est commandée par une porte ET 52 validée par les signaux H, C2 et φ 4. Les bascules 47 et 48 sont remises à zéro par une porte logique ET 53 validée par le signal $\overline{RAZ}$ et le signal de sortie d'une porte logique ET 54 validée par les signaux φ 1 et C2.

Les registres 44 à 46 sont remis à zéro par un signal RAZ et les registres de compteur 41 à 43 sont remis à zéro par une porte logique ET 55 validée par le signal RAZ et le signal de sortie d'une porte logique ET 56 validée par les signaux H et φ 6.

La commande du transfert du contenu des registres 44 à 46 dans les registres de compteur 41 à 43 s'effectue par une série de portes logiques OU 57 validées par la porte 49 et sous la commande d'une porte logique NON-ET 58 validée par les signaux C2 et φ 5.

La progression des bits dans les registres 44 à 46 est commandée par une porte logique OU 59 validée, d'une part, à partir des signaux C2, φ 3 et H par l'intermédiaire d'une porte ET 60 et, d'autre part par le signal de sortie d'une porte logique ET 61 validée par le signal H et par le signal de sortie (inversé) d'une porte logique NON-ET 62 validée par les signaux C2, φ 2 et SM (sortie de mémoire inversée).

La sortie de la porte 62 charge également les registres 44 à 46.

Enfin, le générateur 11 génère les signaux de phase φ 5 et φ 6 par l'intermédiaire de deux bascules bistables 63 et 64 sous la commande des signaux C2 et φ 4.

La figure 8 représente les signaux de phase φ 1 à φ 6, le signal d'horloge H étant celui fourni par la machine (d'écriture ou d'exploitation) conformément à la demande de brevet précitée.

La figure 7 illustre les signaux de cycles C1 à C5 ainsi que le signal de phase φ 7.

Le fonctionnement des dispositifs représentés et décrits ci-dessus est le suivant, qu'il s'agisse d'une écriture de la carte (crédit inscrit dans la mémoire de la carte) ou d'une exploitation de cette carte, (débit porté dans la mémoire) les opérations se déroulent suivant cinq cycles C1 à C5.

Le cycle C1 est un cyle de lecture de la mémoire 10 de la carte durant lequel toute la mémoire est lue, y compris les zones non validées.

Le cycle C2 est un cycle d'écriture dans la zone de validation (champ de validation des zones 1 à Z).

Lorsque l'on veut créditer une ou plusieurs zones de la mémoire de la carte, on fait passer un ou plusieurs bits du champ de validation 4 de l'état 0 à l'état 1.

Si l'on veut utiliser, par exemple les zones 1, 2, 3 et 4 la machine d'inscription fera passer à 1 les quatre premiers bits du champ 4.

Si au contraire, la carte est à débiter, la machine d'exploitation fera passer à 1 les bits correspondants à la valeur à débiter dans la ou les zones disponibles (incrémentables).

L'adresse du bit à écrire est émise par la machine (d'inscription ou d'exploitation). Cette adresse n'est pas émise en clair, mais brouillée par le générateur de clé 15 (fig. 2).

Au niveau de la carte (fig. 3) l'adresse est décryptée (12) et comparée (comparateur 17) à l'adresse du bit à écrire (registre 18). Si ces deux adresses sont identiques, le bit est inscrit (sélecteur 20) et si elles sont différentes le dernier bit de la mémoire est inscrit. Cette anomalie sera ultérieurement détectée par la machine d'exploitation, ce qui provoquera le refus de la carte.

Le cycle C3 est un cycle de lecture identique au cycle C1.

Le cycle C4 est un cycle d'écriture, durant lequel les champs 1, 2, 3 et 4 sont protégés, les zones 1 à Z étant seules accessibles.

Enfin, le cycle C5 est un cycle de lecture identique au cycle C1.

On va maintenant décrire en détail une opération d'écriture d'un certain crédit dans la carte.

Une fois la carte mise en place et les connexions établies, le cycle C1 est déclenché par l'apparition du signal RAZ (figure 7). Il s'étend sur un cycle complet (2048 bits) d'adressage de la mémoire 10 de la carte (lecture de la carte).

Toute ces données de lecture (signal E) sont transmises à la machine de crédit. Si une anomalie quelconque est détectée, la carte est refusée.

On va supposer que la carte a déjà été utilisée, c'est-à-dire que ses champs 1, 2 et 3 sont déjà inscrits et qu'elle doit être «rechargée».

A la fin du cycle C1, apparaît le signal C2 (figure 7 et figure 8). C2 est un cycle court de 141 périodes d'horloge H d'écriture dans le champ de validation 4 de la mémoire de la carte.

Cette écriture est possible du fait que la machine connaît le

numéro d'ordre 3 que la carte lui a communiqué au cours du cycle C1. Ce numéro d'ordre donne la clé à utiliser.

Le signal incident a pour but de communiquer à la carte, après comparaison avec le signal du générateur de clé 21, l'adresse du prochain bit de validation à inscrire dans le champ de validation 4.

Quand apparaît le signal φ 2, le champ de validation 4 est lu. La détection dans ce champ 4 du premier bit à zéro provoque le chargement de l'adresse de ce bit dans les registres 44 à 46.

Pendant la phase φ 3 du cacle C2, la carte reçoit l'adresse du bit de validation à inscrire à 1, la réception se faisant poids fort en tête.

Si pendant la phase φ 3, aucune différence n'a été détectée, la bascule 47 reste à l'état 0. Si une différence a été détectée, la bascule 47 passe à l'état 1.

A la phase φ 4, si la bascule 47 est à 0 la bascule 48 reste à l'état 0 et si elle est à l'état 1, la bascule 48 passe aussi à l'état 1. Durant φ 3, le contenu des registres 31-32 est décalé circulairement 11 fois. Ce décalage circulaire génère la clé C qui sera envoyée au générateur d'adresse 11.

Pendant la phase φ 5, le contenu des registres 44 à 46 est recopié dans le compteur 41 à 43, si la bascule 48 est à l'état 0. Si cette bascule 48 est à l'état 1, le compteur 41 à 43 est chargé avec 11 bits à 1.

Pendant la phase φ 6, le compteur 41 à 43 est remis à zéro.

Si au cours de la phase φ 3, la comparaison entre l'adresse réelle du bit à inscrire et l'adresse fournie par la machine donne une différence, le dernier bit de la mémoire sera mis à 1 pendant la phase φ 5. C'est ce que l'on a représenté en haut de la figure 8 au niveau des signaux d'horloge H et des adresses de mémoire. Dans le cas d'un adressage correct, c'est (par exemple) le 67e bit du champ de validation de la mémoire qui sera dressé. Dans le cas d'un adressage incorrect, c'est le 2047 e bit qui sera adressé.

L'adressage du 2047 e bit traduit ainsi une tentative de fraude qui sera facilement détectée par la machine d'exploitation.

La probabilité pour un fraudeur (ne connaissant pas la clé C) de positionner correctement un bit de validation étant égale à

$$\frac{1}{2048},$$

le système présente donc une grande résistance à la fraude.

La fin du cycle C2 déclenche le cycle C3 qui est un cycle de lecture.

Au cours du cycle C4, les champs 1, 2, 3 et 4 de la carte sont protégés et seules les zones 1 à Z sont accessibles lorsqu'il apparaît la phase 7. A ce moment, les bits des zones concernées sont mis à 1.

Lorsque toute la mémoire de la carte adressée à la fin du cycle C4, apparaît le cycle C5 qui est un cycle de lecture.

Une fois la mémoire totalement lue, le cycle des opérations s'achève.

La machine de crédit peut enregistrer les numéros d'ordre 3 des cartes ainsi créditées, cette possibilité permettant de contrôler certaines cartes douteuses. A cet effet, elle comporte une mémoire non volatile 65 (figure 2) accessible par l'opérateur par le moyen d'un code d'identification synchronisé en 66 (figure 2). Adressée par le numéro d'ordre d'une carte cette mémoire délivre au registre de clé 15 de la machine de crédit la clé à utiliser.

La carte une fois dûment créditée peut être utilisée dans toute machine d'exploitation appropriée.

Après mis en place de la carte et établissement des connexions, les mêmes cycles C1 à C5 que ceux utilisés pour la machine de crédit se déroulent.

Cette machine est chargée de débiter la carte, c'est-à-dire de positionner à 1 les bits correspondant à la valeur à débiter dans la ou les zones à exploiter.

Durant le cycle C1, la mémoire de la carte est lue.

Durant le cycle C2, la machine demande l'inscription, dans le champ de validation de la mémoire, de la carte de 0 aux adresses de bit concernés et non plus de 1 comme dans le cas du crédit. Cette demande d'inscription n'a aucun effet sur la mémoire car les bits déjà à 1 irréversible et les bits déjà à 0 ne peuvent qu'y rester. Les adresses envoyées par la machine peuvent donc être quelconque.

Le cycle C3 est un cycle de lecture identique au cycle C1.

Au cours du cycle C4 qui est un cycle d'écriture les champs 1, 2, 3 et 4 sont protégés et seul la ou les zones et sous zones autorisées par le champ de validation 4 sont accessibles à la machine de débit qui inscrit alors des 1.

Enfin le cycle C5 est un cycle de lecture identique au cycle C1.

Dans le cas où il y a eu tentative de fraude on a vu que le dernier bit de la mémoire de la carte a été mis à 1. Lors de l'introduction dans une machine de débit d'une telle carte au premier cycle de lecture C1, le dernier bit à 1 de la mémoire est détecté dans la mémoire 67 et la carte est refusée.

Il est bien évident que l'exemple qui vient d'être donné d'une réalisation de l'invention n'est absolument pas limitatif et que l'homme de l'art pourra trouver d'autres variantes de réalisation sans pour autant sortir du cadre de l'invention.

FIG.1

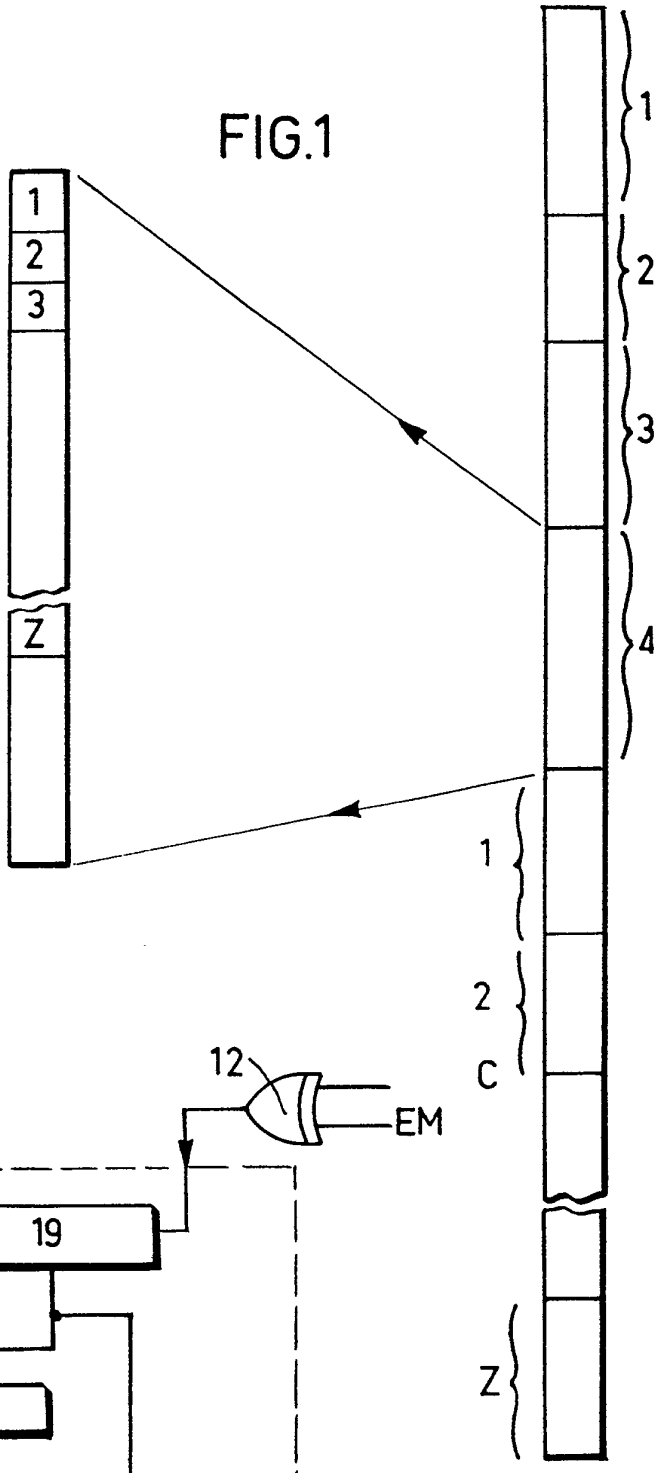
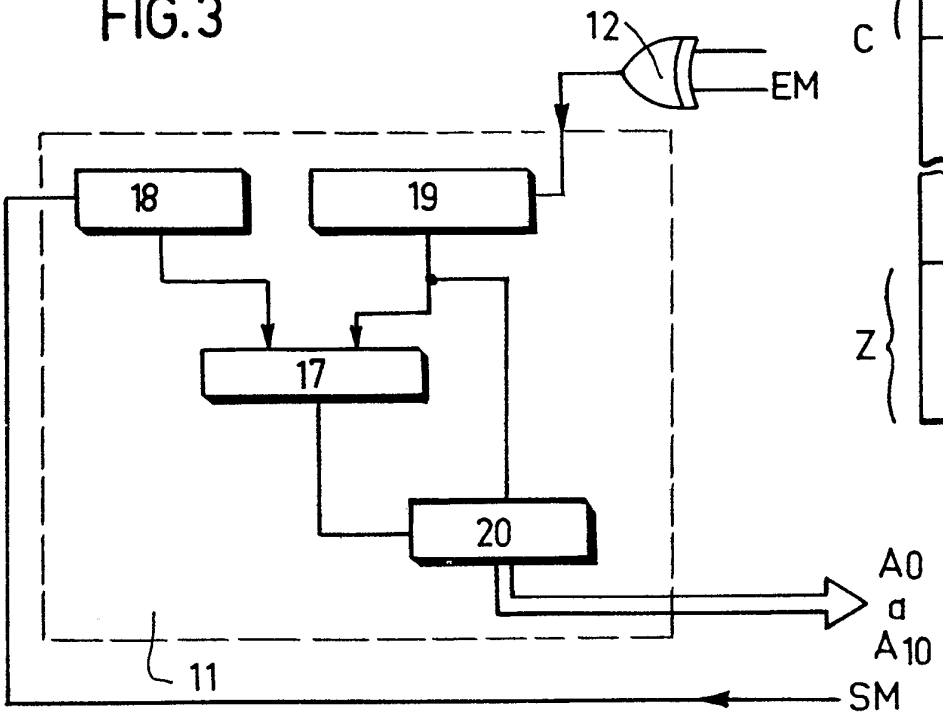


FIG.3



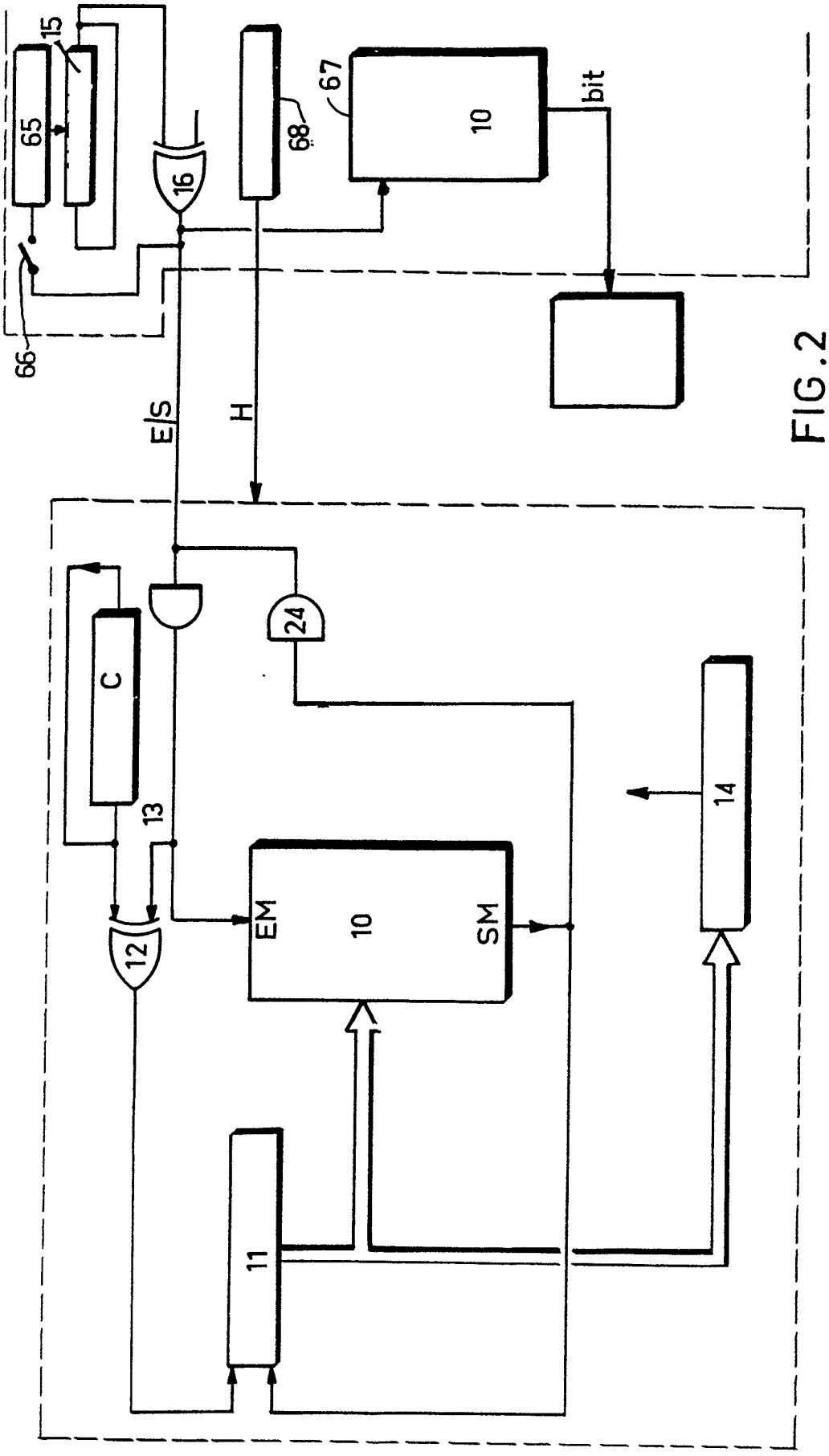


FIG.2

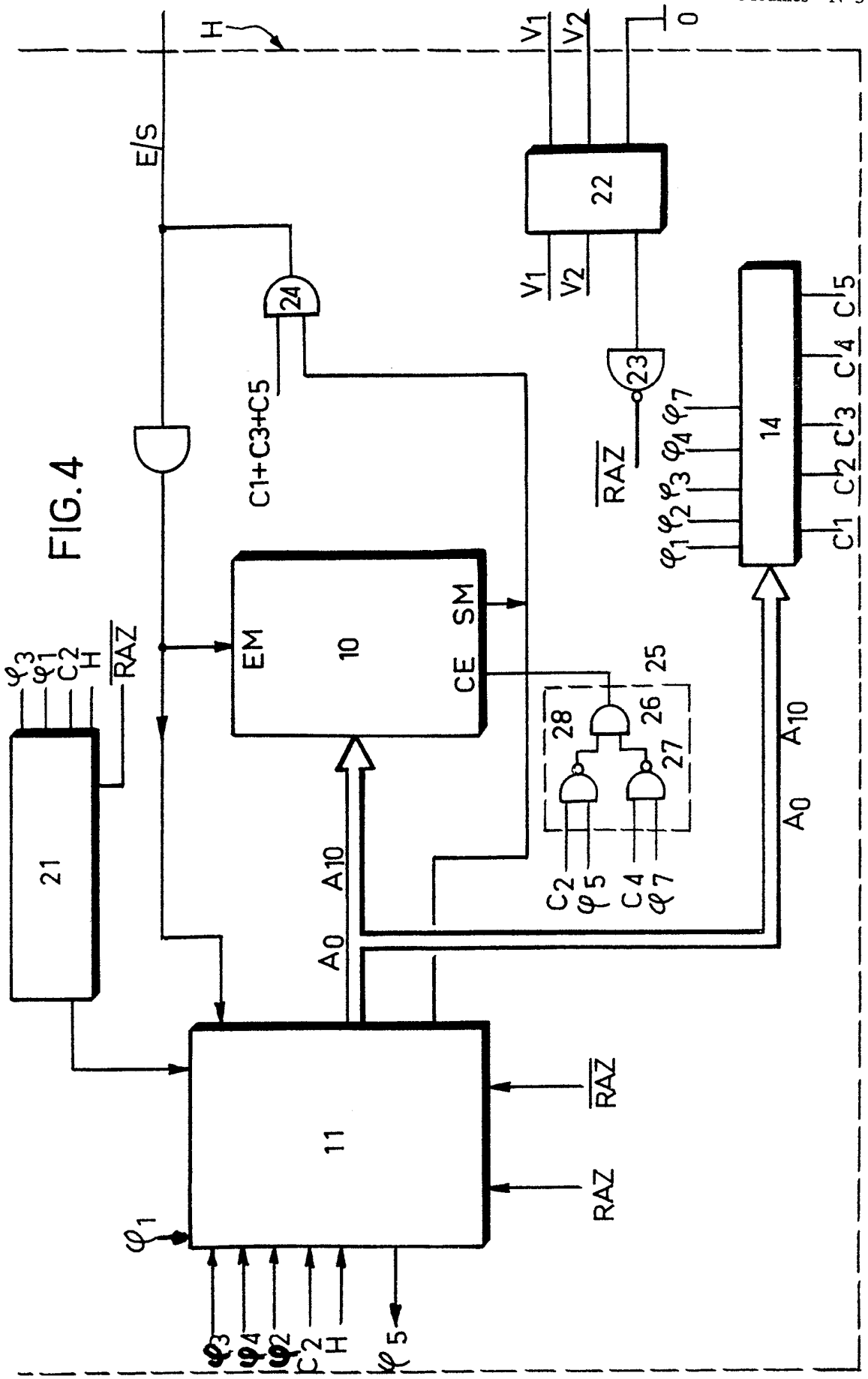

H
E/S
V1
V2
0
22
24
23
C1+C3+C5
RAZ
14
C'5
C'4
C'3
C'2
C'1
φ7
φ4
φ3
φ2
φ1
EM
10
CE
SM
25
28
26
27
A10
A0
21
φ3
φ1
C2
H
RAZ
C2
φ5
C4
φ7
11
RAZ
RAZ
φ1
φ3
φ4
φ2
C2
H
φ5

FIG. 4

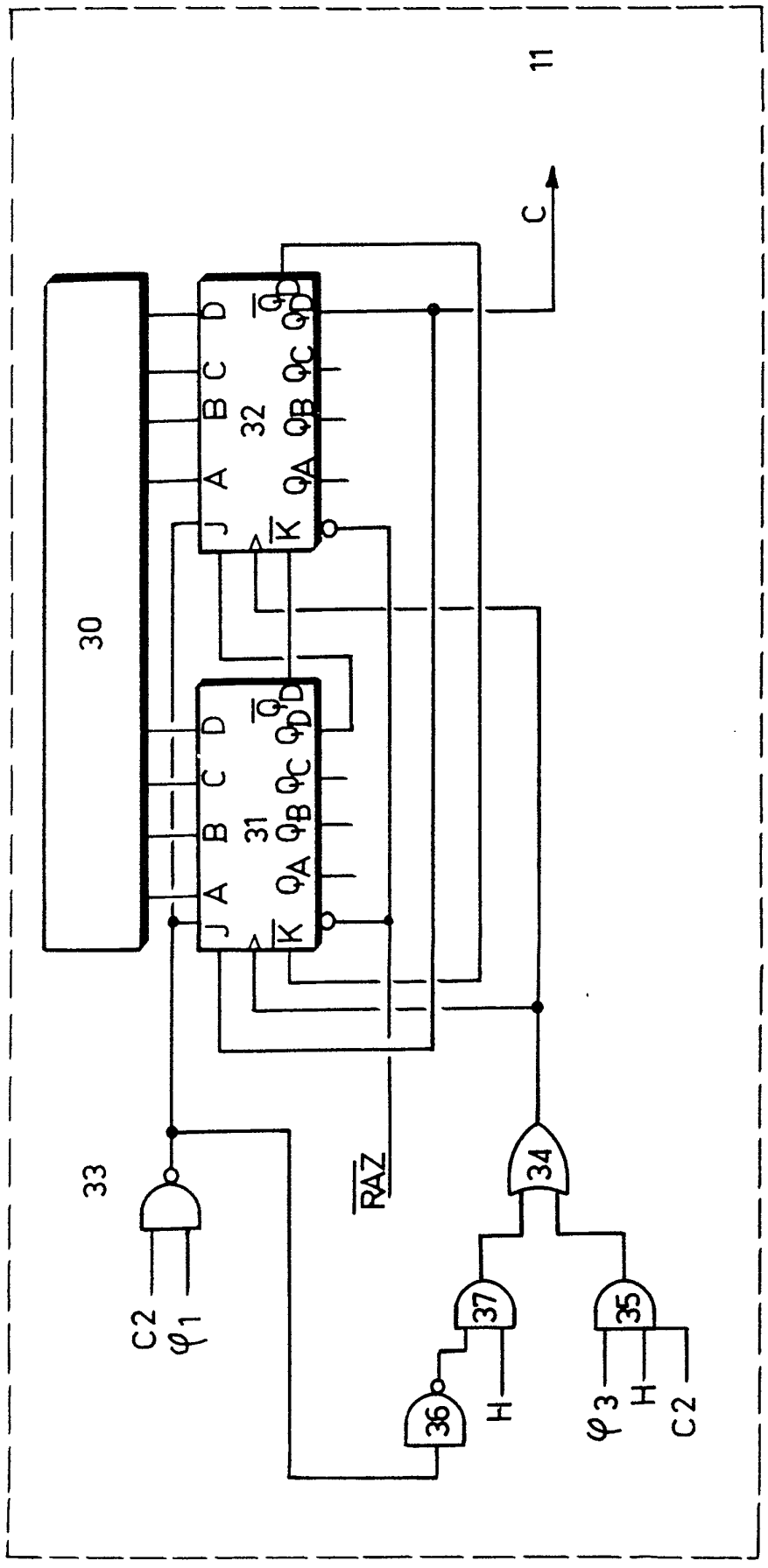


FIG.5

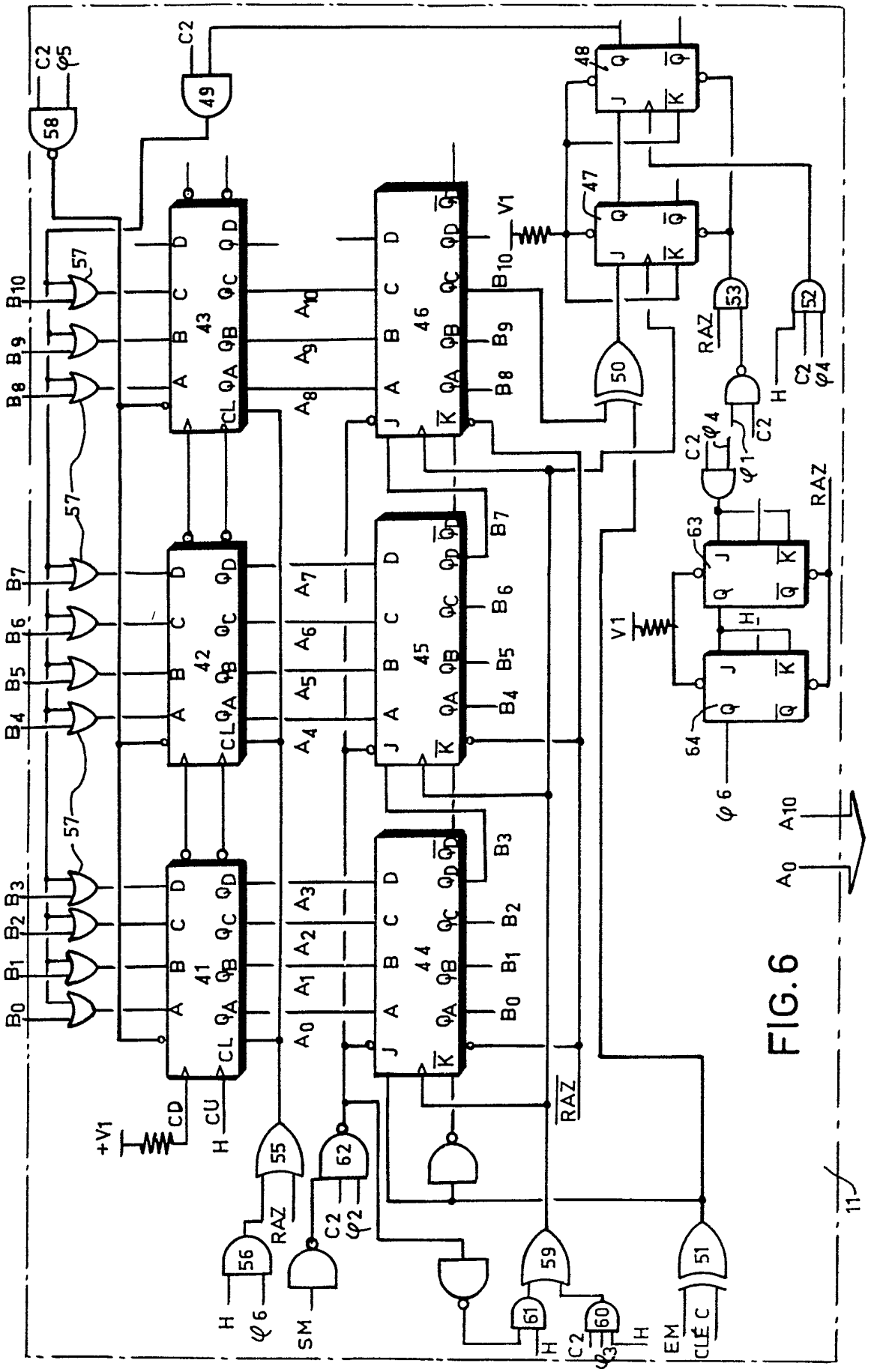

C2
φ5
58
49
48
47
V1
B10
B9
B8
B7
B6
B5
B4
B3
B2
B1
B0
57
43
42
41
46
45
44
A10
A9
A8
A7
A6
A5
A4
A3
A2
A1
A0
50
53
52
RAZ
H
C2
φ4
φ1
φ2
φ3
φ6
63
64
CD
CU
+V1
55
62
56
59
61
60
51
SM
EM
CLÉ C
RAZ
11

FIG.6

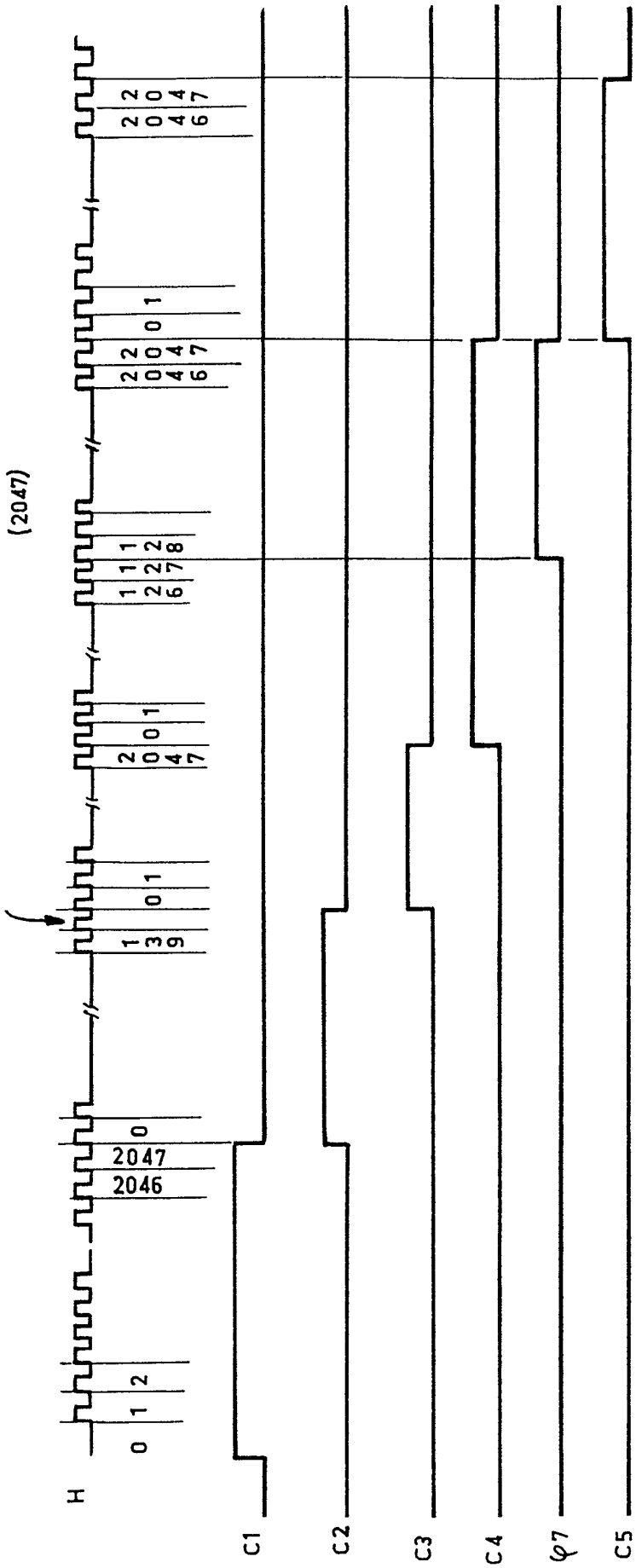

H
0
1
2
0
2047
2046
1
3
9
0
1
2
0
4
7
0
1
1
2
6
1
1
2
7
8
2
0
0
4
6
7
0
1
2
2
0
0
4
6
7
(2047)
C1
C2
C3
C4
φ7
C5

FIG.7

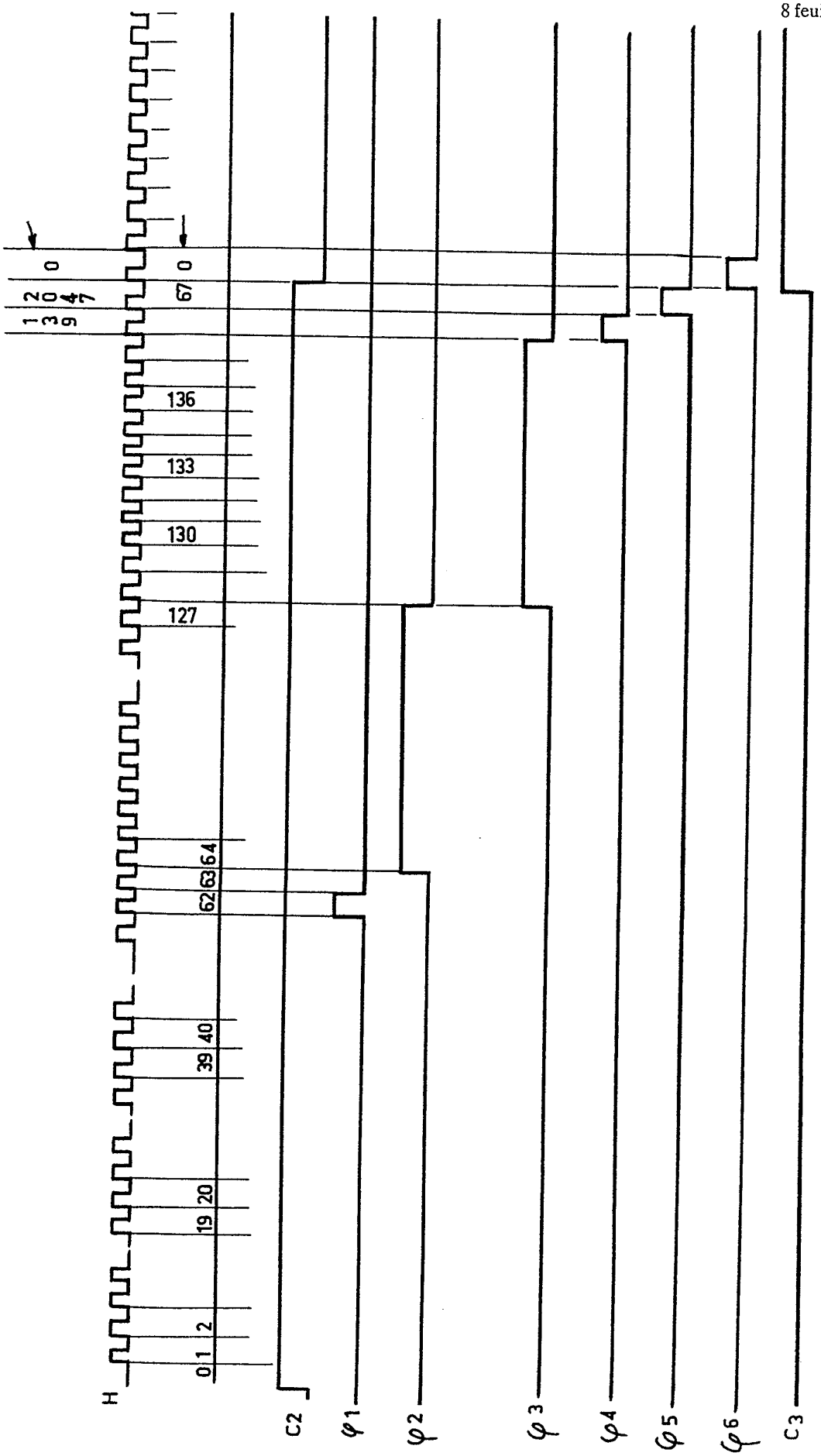

H
0
1
2
19
20
39
40
62
63
64
127
130
133
136
1
3
9
2
0
4
7
0
67
C2
φ1
φ2
φ3
φ4
φ5
φ6
C3

FIG.8

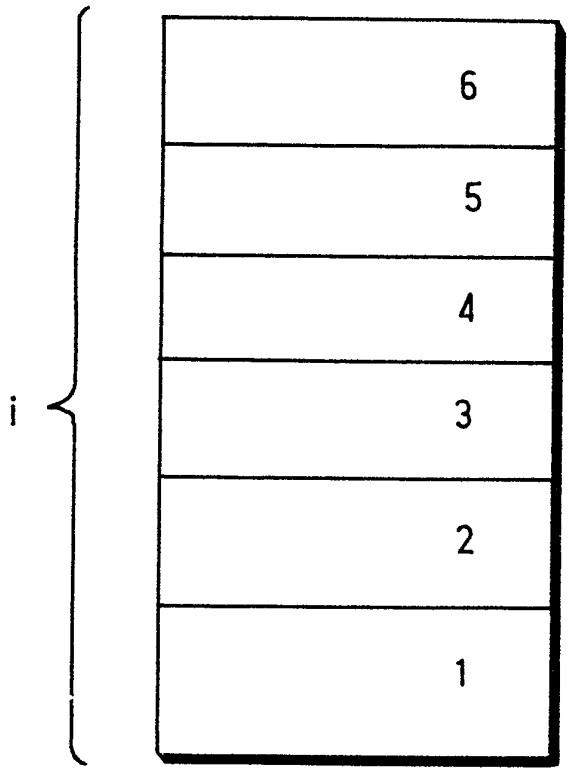


FIG.9