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

(11) EP 0 985 790 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
15.03.2000 Bulletin 2000/11

(51) Int. Cl.[7]: **E05B 49/00**, H04L 9/32

(21) Numéro de dépôt: **99117014.3**

(22) Date de dépôt: **30.08.1999**

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Etats d'extension désignés:
AL LT LV MK RO SI

(30) Priorité: **10.09.1998 FR 9811397**

(71) Demandeur: **MR Electronic SA**
2300 La Chaux-de-Fonds (CH)

(72) Inventeur: **Monnier, Jean-Luc**
2300 La Chaux-de-Fonds (CH)

(74) Mandataire: **Gresset, Jean**
Gresset - Laesser - Nithardt,
Cabinet de Conseils en propriété industrielle,
8A, Puits-Godet
2000 Neuchâtel (CH)

(54) Serrure electronique a commande dynamique et systeme de commande muni d'une telle serrure

(57) L'invention se rapporte à une serrure électronique à commande dynamique. Selon l'invention, la serrure comporte un instrument (10) pour entrer des données dans la serrure, un circuit électronique de traitement des informations (12) et un système de commande (14) du verrouillage et du déverrouillage. L'électronique de la serrure comporte, de manière particulièrement avantageuse, des registres à décalage à récurrence pour traiter les valeurs permettant d'assurer l'accès à un espace protégé.

Application à des systèmes de protection d'espaces confinés dont l'accès doit être contrôlé.

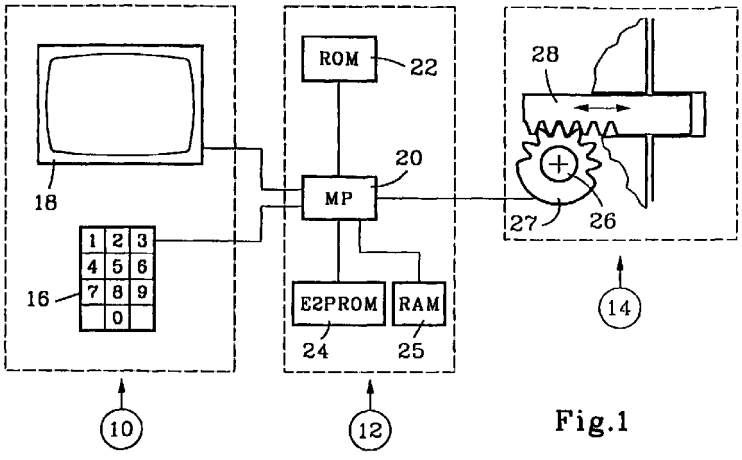

Fig.1

EP 0 985 790 A1

Description

[0001] La présente invention concerne les serrures électroniques à commande dynamique. Elle se rapporte plus particulièrement à une serrure du type comportant un instrument pour entrer des données, un dispositif électromagnétique d'actionnement pour actionner un verrou et un circuit électronique.

[0002] Une telle serrure est, par exemple, décrite dans le brevet US 5'488'660. Son ouverture est commandée par une combinaison, donnée par une unité centrale et modifiée à chaque fois que la serrure est ouverte. Comme la serrure et l'unité centrale ne sont pas reliées directement l'une à l'autre, il est nécessaire qu'elles puissent travailler en synchronisme, de manière que le code émis par l'unité centrale puisse être vérifié comme correct par la serrure.

[0003] Ces serrures sont particulièrement destinées à permettre un accès unique à un espace protégé, par exemple à l'intérieur d'un distributeur de billets de banque, pour en assurer son entretien et son chargement. Elles permettent notamment d'éviter que des personnes chargées une fois d'une opération de maintenance puissent utiliser le code qui leur a été transmis pour ouvrir ultérieurement la serrure. De la sorte, il n'est pas possible d'accéder à l'espace protégé sans obtenir préalablement un code d'accès auprès de la centrale gérant le système. De ce fait, on augmente considérablement la sécurité d'accès.

[0004] De manière plus précise, la serrure décrite dans le brevet mentionné plus haut comporte un clavier pour entrer les combinaisons dans la serrure, un affichage pour afficher les informations relatives à l'entrée de données, et un circuit électronique pour recevoir la combinaison et pour la comparer avec une combinaison autorisée. Le circuit électronique comprend:

- un dispositif activé lors de l'introduction d'une combinaison d'entrée, pour générer une combinaison à partir d'informations précédemment mémorisées,
- un comparateur, pour comparer la combinaison d'entrée avec la combinaison générée et, en cas d'égalité, pour adresser des signaux de commande du verrou et de mémorisation des nouvelles informations.

[0005] Dans cette serrure, la combinaison est obtenue à partir d'opérations mathématiques dans lesquelles interviennent entre autres:

- la dernière combinaison acceptée,
- un paramètre spécifique à la serrure,
- une combinaison maîtresse, et
- une valeur variable selon une loi prédéfinie, par exemple le nombre d'ouvertures.

[0006] La combinaison d'entrée est définie par un ordinateur de la centrale gérant le système, qui comporte les mêmes moyens de calcul et conserve en mémoire les mêmes informations que la serrure. Les combinaisons sont calculées, tant dans la serrure qu'à la centrale, sur la base de nombres en mémoires et en appliquant des formules mathématiques préétablies. La serrure comporte, en outre, des moyens de comparaison pour comparer la combinaison entrée avec la combinaison générée, le verrou étant libéré si les combinaisons sont égales.

[0007] On entend par combinaison un nombre introduit dans la serrure pour être comparé avec un nombre généré dans la serrure, ces deux nombres devant être égaux.

[0008] En développant une approche différente, dans laquelle les informations en mémoires sont traitées au moyen de fonctions logiques, il est possible de réaliser des serrures permettant d'améliorer encore la sécurité d'accès.

[0009] A cet effet, la serrure selon l'invention comporte un instrument pour entrer des données, un dispositif électromagnétique d'actionnement pour commander un verrou et un circuit électronique. Elle est caractérisée en ce que le circuit électronique comporte:

- une première mémoire pour mémoriser une valeur de référence,
- une deuxième mémoire pour mémoriser une valeur courante,
- une unité de traitement comprenant un premier registre pour appliquer une fonction sur la valeur de référence, un deuxième registre pour traiter la valeur courante, un troisième registre pour traiter une valeur d'entrée, des moyens pour transférer la valeur de référence et la valeur courante de sa mémoire dans son registre respectif et réciproquement, et des moyens logiques pour:
  - traiter la valeur de référence contenue dans le premier registre pour définir une nouvelle valeur de référence remplaçant la valeur antérieure dans le premier registre,
  - combiner la valeur courante contenue dans le deuxième registre et la valeur d'entrée contenue dans le troisième registre, pour définir une nouvelle valeur courante remplaçant l'ancienne dans le deuxième registre,
  - comparer le contenu des premier et deuxième registres et,
  - en cas de concordance uniquement, adresser un ordre au dispositif électromagnétique d'actionnement pour commander le verrou, remplacer dans la première mémoire la valeur de référence qui s'y trouve par la nouvelle valeur de référence contenue dans le premier registre, et remplacer dans la deuxième mémoire la valeur courante qui s'y trouve par la nouvelle valeur courante contenue dans le deuxième registre.

[0010] Une telle serrure nécessite un nouveau code d'accès à chaque manipulation correcte, ce qui réduit les risques d'accès non autorisés, comme évoqué ci-dessus, et cela de manière remarquablement performante.

[0011] On entend par code un nombre ou un mot introduit dans la serrure et traité par le circuit électronique pour donner une valeur qui, comparée à une autre valeur définie également par le circuit, permet ou non l'ouverture de la serrure.

[0012] Dans un mode de réalisation particulier, l'unité de traitement comporte des registres à décalage, comprenant chacun une pluralité de cellules, numérotées de *0* à *n* et dans lesquelles la dernière information introduite occupe la cellule de rang le plus bas.

[0013] De manière plus précise, l'unité de traitement comporte, en outre, trois portes OU exclusif, munies chacune de deux entrées et d'une sortie et définissant avec les registres à décalage des registres à décalage à récurrence, généralement connu sous leur nom anglais: "Linear feed shift register" (LFSR).

[0014] Plus particulièrement, l'unité de traitement comporte:

- un registre à décalage à récurrence de traitement de valeur, comprenant un premier registre à décalage et une porte OU exclusif, pour traiter l'ancienne valeur de référence en vue d'obtenir une nouvelle valeur de référence, et
- un registre à décalage à récurrence, de combinaison, comprenant un deuxième registre à décalage, dans lequel est introduite la valeur courante, et un troisième registre à décalage, dans lequel est introduite la valeur d'entrée et deux portes OU exclusif pour combiner la valeur courante et la valeur d'entrée et pour définir la nouvelle valeur courante.

[0015] L'unité de traitement comporte, en outre, une unité de traitement logique agencée pour vérifier que les cellules de même rang d'une partie au moins des premier et deuxième registres à décalage, ont un contenu identique.

[0016] On relèvera que le système objet du brevet mentionné plus haut conduit à des combinaisons qui sont parfaitement déterminées. En d'autres termes, en connaissant l'algorithme, ce qui peut se faire facilement en disposant d'un système de ce type, et en analysant quelques combinaisons successives, il est possible de définir les combinaisons suivantes. Certes, l'accès à la serrure est rendu plus difficile que lorsque le code ne change pas, mais il est encore possible, avec des moyens relativement modestes, de générer les combinaisons d'ouverture subséquentes sur la base d'informations relativement faciles à obtenir et accéder ainsi de manière non autorisée à l'espace protégé.

[0017] Un but important de la présente invention est de pallier cet inconvénient. A cet effet, la serrure est, en outre, caractérisée en ce que l'unité de traitement est agencée de manière qu'elle ne compare qu'une partie seulement des éléments de la valeur courante et de la valeur de référence. De manière plus précise, l'unité de traitement logique ne prend en compte qu'une partie seulement des cellules des premier et deuxième registres à décalage.

[0018] La présente invention concerne également un système de commande comportant un dispositif central agencé pour générer des codes de commande successifs différents et une serrure à commande dynamique.

[0019] Ce système de commande est caractérisé en ce que le dispositif central comprend:

- une première mémoire pour mémoriser une valeur de référence, égale à la valeur de référence contenue dans la première mémoire de la serrure,
- une deuxième mémoire pour mémoriser une valeur courante, égale à la valeur courante contenue dans la deuxième mémoire de la serrure,
- une unité de traitement comprenant :
  - un premier registre pour traiter la valeur de référence,
  - un deuxième registre pour traiter la valeur courante,
  - des moyens pour transférer la valeur de référence et la valeur courante de sa mémoire dans son registre respectif et réciproquement,
  - des moyens pour traiter la valeur de référence contenue dans le premier registre, pour définir une nouvelle valeur de référence remplaçant la valeur contenue antérieurement dans le premier registre,
  - des moyens pour combiner la valeur courante contenue dans le deuxième registre et la nouvelle valeur de référence, pour définir une valeur d'entrée contenue dans un troisième registre et une nouvelle valeur courante contenue dans le deuxième registre.

[0020] Afin d'utiliser des moyens aussi simples que possible pour la création des codes d'accès, le système de commande est caractérisé en ce que le dispositif central et la serrure comportent des registres à décalage comprenant chacun des cellules, numérotées de *0* à *n*, et dans lesquelles la dernière information introduite occupe la cellule de rang le plus bas.

[0021] Dans un mode particulièrement avantageux de réalisation de l'invention, le système de commande est caractérisé en ce que l'unité de traitement de la serrure comporte, en outre, trois portes OU exclusif munies chacune de deux entrées et d'une sortie, définissant avec lesdits registres:

- un registre à décalage à récurrence de traitement de valeur, comprenant un premier registre à décalage dans lequel est introduite la valeur de référence et une porte OU exclusif pour traiter

l'ancienne valeur de référence en vue d'obtenir une nouvelle valeur de référence, et

- un registre à décalage à récurrence, de combinaison, comprenant un deuxième registre à décalage dans lequel est introduite la valeur courante, et un troisième registre à décalage dans lequel est introduite la valeur d'entrée et deux portes OU exclusif, pour combiner la valeur courante et la valeur d'entrée et pour définir la nouvelle valeur courante,

et en ce que l'unité de traitement du dispositif comporte, en outre, trois portes OU exclusif et un commutateur, définissant ensemble:

- un registre à décalage à récurrence de traitement de valeur, comprenant un premier registre à décalage dans lequel est introduite la valeur de référence, et une porte OU exclusif pour traiter l'ancienne valeur de référence en vue d'obtenir une nouvelle valeur de référence, et
- un registre à décalage à récurrence de combinaison et mixage, comprenant un deuxième registre à décalage dans lequel la valeur courante est introduite, un troisième registre à décalage dans lequel la valeur d'entrée est introduite, et un quatrième registre à décalage dans lequel une valeur provenant au moins médiatement du premier registre à décalage est introduite, et deux portes OU exclusif, pour traiter la valeur contenue dans le quatrième registre et l'ancienne valeur courante, en vue d'obtenir la valeur d'entrée et une nouvelle valeur courante.

[0022] Pour assurer le traitement des informations, l'unité de traitement de la serrure comporte, en outre, une unité de traitement logique pour vérifier que les cellules de même rang d'une partie au moins du premier et du deuxième registre ont un contenu identique.

[0023] Comme cela a été expliqué plus haut, l'analyse de codes successifs et la connaissance de l'algorithme les générant peut permettre de définir les codes à venir. Dès lors que la serrure est agencée de manière qu'une partie seulement des informations contenues dans le code est lue par le comparateur, il est possible d'introduire des valeurs aléatoires, rendant ainsi illusoire la détermination des codes à venir. A cet effet, le système de commande est caractérisé en ce que l'unité de traitement logique de la serrure est agencée de manière qu'elle ne compare qu'une partie seulement des éléments de la valeur courante et de la valeur de référence et en ce que l'unité de traitement du dispositif central comporte, en outre, une unité de traitement logique pour traiter la valeur de référence contenue dans le premier registre à décalage et pour introduire la valeur après traitement dans le quatrième registre à décalage, un cinquième registre à décalage et un sixième registre à décalage coopérant avec l'unité de traitement logique pour respectivement masquer un certain nombre de cellules du premier registre et pour introduire une valeur aléatoire dans des cellules dont les éléments ne font pas l'objet de la comparaison.

[0024] D'autres avantages et caractéristiques de l'invention ressortiront de la description qui va suivre, faite en regard du dessin annexé, dans lequel:

- La figure 1 montre un schéma général d'une serrure à commande dynamique selon l'invention,
- Les figures 2 à 4 montrent respectivement des schémas de registres à décalage à récurrence, de traitement de valeur, de combinaison de valeurs et de combinaison et mixage, et
- Les figures 5a et 5b représentent la structure schématique du système selon l'invention, de l'unité centrale en a et de la serrure en b.

[0025] La serrure telle que schématiquement représentée à la figure 1 comporte un instrument 10 pour entrer des données dans la serrure, un circuit électronique de traitement des informations 12 et un système de commande 14 du verrouillage et du déverrouillage.

[0026] L'instrument 10 comporte un clavier 16 et un écran 18, permettant respectivement à l'utilisateur d'introduire et d'obtenir des informations relatives aux opérations en cours.

[0027] Le circuit électronique comprend un microprocesseur 20, une mémoire 22 de type ROM, contenant les programmes de commande, un ensemble de mémoires reprogrammables 24, de type E2PROM, permettant de mémoriser les valeurs successives destinées à la gestion de l'ouverture du verrou et un ensemble de mémoires volatiles 25, de type RAM, dans lequel sont définis des registres qui seront décrit de manière plus détaillée en référence aux figures 2, 3 et 4.

[0028] Le système de commande 14 comporte un moteur 26 et un verrou 28, entraîné par une roue 27 solidaire de l'axe du moteur 26. On relèvera incidemment que le verrou pourrait également être commandé par un électroaimant.

[0029] La serrure telle que décrite permet, par exemple, de commander l'ouverture d'un distributeur de billets de banque. Lorsque la personne responsable d'en assurer le chargement doit intervenir, elle demande un code d'accès à la société gérant ce distributeur. Le code est défini par une unité centrale, qui fera l'objet d'une description plus détaillée en référence à la figure 5a.

[0030] L'entrée du code se fait au moyen du clavier 16. Le microprocesseur 20 traite les valeurs contenues dans les mémoires reprogrammables 24 correspondant au dernier code reconnu ainsi que le nouveau code entré, pour obtenir une valeur de référence REF, fonction uniquement des valeurs de références antérieures, et une valeur courante CRT. S'il y a concordance entre REF et CRT, il permet l'ouverture du verrou 28 et mémorise les nouvelles valeurs obtenues par combinaison des anciennes valeurs et du code entré.

[0031] Si, au contraire, il n'y a pas concordance, le verrou reste bloqué et le contenu des mémoires 24 n'est pas modifié. Après avoir terminé le travail qu'il avait à effectuer, l'utilisateur donne quittance à la société gérant le distributeur, qui introduit l'information dans l'unité centrale.

[0032] Pour bien saisir la manière dont la fonction de traitement des informations est assurée, il est nécessaire de comprendre ce qu'est un registre à décalage à récurrence, plus connu sous son appellation anglaise de "Linear feed shift register" (LFSR) et décrit par exemple dans EDN ACCESS, 4 janvier 1996, sous le titre "The Ouroboros of the digital consciousness: Linear feedback-shift registers". L'un d'entre eux est représenté à la figure 2. Il comporte, sur cette figure, un registre à décalage 30, comprenant quarante cellules numérotées de *0* à *39* et contenant chacune un élément d'une valeur binaire enregistrée, et une porte OU exclusif 32, dont l'une des entrées, portant la référence 32a, est reliée à la cellule de rang *1* et l'autre 32b à la cellule de rang *32*. La sortie 32c est reliée à l'entrée du registre à décalage 30, soit à la cellule de rang *0*.

[0033] Selon le principe des registres à décalage, on introduit à chaque signal d'horloge CLK un nouvel élément dans la cellule de rang *0* et le contenu des cellules est décalé de un rang. Dans le registre à décalage à récurrence de la figure 2, la valeur entrée est définie par le contenu du registre à décalage lui-même. A chaque fois qu'on fait avancer le registre de un pas, la nouvelle valeur introduite est définie par les valeurs contenues dans les cellules de rang *1* et *32* qui sont reliées respectivement aux entrées 32a et 32b de la porte 32.

[0034] Lorsque les contenus de ces cellules sont égaux (0-0 ou 1-1), le signal de sortie de la porte 32 vaut 0. Si, au contraire, les contenus sont différents (0-1 ou 1-0), le signal de sortie est égal à 1. On peut ainsi générer, de manière simple, une succession de nombres binaires ayant un caractère quasi aléatoire, et pourtant évoluant de manière prévisible. La période de répétition dépend des cellules auxquelles les entrées 32a et 32b de la porte 32 sont reliées. Avec la solution décrite ci-dessus, cette période représente plusieurs milliards de rotations.

[0035] La figure 3 montre un registre à décalage à récurrence de combinaison de valeurs, destiné à définir une nouvelle valeur courante CRT, à partir de l'ancienne valeur courante et d'une valeur d'entrée INT dont les caractéristiques seront précisées plus tard. Il comporte deux registres à décalages 36 et 38 et deux portes OU exclusif 40 et 42, chacune ayant deux entrées définies par les lettres a et b et une sortie définie par la lettre c. Le code d'accès, en code décimal, est entré dans la serrure au moyen du clavier 16. Un circuit électronique 43 le transforme en code binaire, définissant une valeur d'entrée INT, introduite dans le registre 38 par chargement parallèle.

[0036] Les deux registres à décalage 36 et 38 comprennent chacun quarante cellules, numérotées de *0* à *39*. Les entrées 40a et 40b de la porte 40 sont respectivement reliées aux cellules de rangs *1* et *32* du registre 36. Les entrées 42a et 42b de la porte 42 sont respectivement reliées à la sortie 40c de la porte 40 et à la cellule de rang *39* du registre 38.

[0037] Le registre 36 contient donc initialement la valeur CRT provenant de la transaction antérieure et le registre 38 la valeur INT nouvellement introduite. Comme la cellule de rang *39* du registre 38 est reliée à l'entrée 42b de la porte 42, alors que l'autre entrée 42a est reliée à la sortie 40c de la porte 40, les états logiques de ces deux entrées définissent une information binaire introduite dans la cellule de rang *0* du registre 36. De la sorte, à chaque fois qu'un signal d'horloge est appliqué au registre 38, son contenu est décalé d'un rang et un bit est introduit dans le registre 36, fonction de son propre contenu et de celui du registre 38.

[0038] Un registre à décalage à récurrence de combinaison de valeurs permet d'obtenir une valeur prédictible, à partir de deux valeurs connues. Il est toutefois extrêmement difficile de déterminer cette valeur si l'on ne connaît pas la structure des registres à décalage.

[0039] Pour améliorer encore la sécurité d'accès, il est possible d'introduire des paramètres aléatoires dans la valeur d'entrée et de ne comparer que la part des paramètres prédictibles. A cet effet, on utilise une structure telle que représentée à la figure 4, sur laquelle on peut voir trois registres à décalage portant respectivement les références 44, 46 et 48, deux portes OU exclusif 50 et 52 et un commutateur à deux entrées et deux sorties, schématiquement représenté en 54. L'ensemble forme un registre à décalage à récurrence de combinaison et de mixage. Il permet d'introduire dans les registres 44 et 46 une partie des informations contenues dans les cellules du registre 48, ces parties étant complémentaires, les autres cellules étant chargées d'informations obtenues par combinaison des informations initialement contenues dans les registres 44 et 48.

[0040] De manière plus précise, il permet d'obtenir, dans le registre 46, la valeur d'entrée INT comportant des informations permettant d'assurer la commande du verrou. A cet effet, la porte 50 comporte deux entrées 50a et 50b respectivement reliées aux cellules de rangs *32* et *1* du registre 44. La porte 52 comprend des entrées 52a et 52b respectivement reliées à la sortie 50c de la porte 50 et à la cellule de rang *39* du registre 48. Le commutateur 54 comprend deux entrées 54a et 54b et deux sorties 54c et 54d. La cellule de rang *39* du registre 48 est également reliée à la première entrée 54a du commutateur 54. La deuxième entrée 54b est reliée à la sortie 52c de la porte 52. Enfin, les sorties 54c et 54d sont respectivement reliées aux cellules de rang *0* des registres 44 et 46.

[0041] Lorsque le commutateur 54 est en position telle que représentée au dessin, c'est-à-dire que l'entrée 54a est reliée à la sortie 54d, les informations contenues dans le registre 48 sont transférées sans modification dans le registre 46. En d'autres termes, elles sont trans-

férées sans cryptage. Cette position correspond aux transfert d'éléments aléatoires de la valeur d'entrée INT. Dans le registre 44, au contraire, les informations introduites sont obtenues par traitement du contenu du registre 44 et du contenu du registre 48, par la fonction OU exclusif appliquée par la porte 52. La situation est inversée lorsque le commutateur bascule. De la sorte, le contenu du registre 48 est transféré en clair dans le registre 44 alors que le registre 46 reçoit une information obtenue par traitement du contenu des registres 44 et 48, au moyen de la porte 52.

[0042] Le contenu du registre 46 est ensuite transformé en code décimal par des moyens non représentés au dessin, le nombre obtenu tenant lieu de code d'accès.

[0043] La figure 5a montre, de manière schématique, le dispositif de l'unité centrale destiné à définir les codes d'accès successifs d'une serrure à commande dynamique, dont le dispositif logique est représenté à la figure 5b.

[0044] Le dispositif de l'unité central comporte deux mémoires reprogrammables 58 et 60, un registre à décalage à récurrence de traitement de valeurs 62, tel que défini en référence à la figure 2 et un registre à décalage à récurrence de combinaison et mixage 63, tel que défini en référence à la figure 4. Les parties constitutives de ces registres portent les mêmes références que celles utilisées dans ces figures. Il comporte en outre deux registres à décalage 64 et 68, et une unité de traitement logique 70 comprenant des moyens schématiquement représentés en 72 et 76, et destinés à assurer respectivement une fonction logique ET et une fonction logique OU.

[0045] Les mémoires 58 et 60 contiennent respectivement des valeurs REF et CRT dont les caractéristiques seront précisées plus tard.

[0046] Les registres 64 et 68 comportent un même nombre de cellules. Le registre 64 contient une valeur MAS constante, définissant les cellules dont le contenu est crypté, identifiées par 1, alors que les cellules dont le contenu est en clair contiennent un 0. Le registre 68 est destiné à recevoir une valeur aléatoire ALE. Elle est obtenue à partir d'un nombre binaire aléatoire, comportant autant de chiffres que les registres comptent de cellules, généré par l'unité centrale par des moyens connus de l'homme de l'art et non représentés au dessin, et traité par comparaison avec le contenu du registre 64 de manière que pour toutes les cellules du registre 64 contenant un 1, la cellule de même rang du registre 68 est amené à 0. De la sorte, les cellules occupées par les éléments variables de la valeur ALE correspondent aux cellules du registre 64 dont le contenu est égal à 0. Les autres cellules contiennent la valeur 0.

[0047] Lorsque le dispositif de l'unité centrale reçoit une demande de code, le contenu des mémoires 58 et 60 sont respectivement introduits, par chargement parallèle, dans les registres 30 du registre à décalage à récurrence de traitement de valeur 62, et 44 du registre à décalage à récurrence de combinaison et mixage 63. Un signal d'horloge CLK REF est appliqué au registre 30, pour définir une nouvelle valeur REF.

[0048] Après quoi, les contenus des registres 30, 64 et 68 sont ensuite traités en parallèle, au moyen de l'unité de traitement logique 70. De manière plus précise, les contenus des registres 30 et 64 sont traités au moyen de la fonction ET représentée en 72. La valeur ainsi obtenue est égale au contenu du registre 30 lorsque le contenu du registre 64 est égal à 1, et à 0 dans les autres cas. On libère ainsi des cellules pour introduire une partie aléatoire ALE, entrée au moyen de la fonction OU, de manière que la valeur obtenue à la sortie de l'unité 70 soit formée de deux parties comportant respectivement, une partie aléatoire et une information de référence. La valeur ainsi obtenue est introduite en parallèle dans le registre 48 dont le contenu est ensuite traité par le registre 63.

[0049] On applique ensuite un signal d'horloge CLK sur les registres 44, 46, 48 et 64. Les informations contenues dans le registre 64 commandent le commutateur 54 de manière que les signaux issus du registre 48 soient directement introduits dans le registre 46 lorsque le contenu de la cellule correspondante du registre 64 est égal à 0 et dans le registre 44 lorsqu'il est égal à 1. A la fin de cette opération, le registre 46 contient la valeur, appelée INT, comprenant une partie aléatoire et une partie destinée à commander l'ouverture de la serrure. La valeur INT est ensuite transformée on code décimal, par des moyens non représentés, pour on rendre la lecture et le traitement plus aisé. Le code est transmis ainsi à la personne devant ouvrir la serrure.

[0050] On relèvera que tous les composants nécessaires pour assurer les fonctions du dispositif de l'unité centrale se trouvent dans n'importe quel ordinateur personnel et que la programmation des fonctions devant être assurées sont à la portée de l'homme du métier.

[0051] Le code d'accès, ainsi obtenu, est traité, après introduction au moyen du clavier et transformation en valeur binaire, par le dispositif logique de la serrure tel que représenté à la figure 5b. Ce dispositif comporte, à cet effet, deux mémoires reprogrammables 80 et 82, un registre à décalage à récurrence de traitement de valeurs 84, tel que défini en référence à la figure 2 et un registre à décalage à récurrence de combinaison de valeurs 86, tel que défini en référence à la figure 3. Les parties constitutives de ces registres portent les mêmes références que celles utilisées dans ces figures. Ce dispositif comporte, en outre, un registre à décalage 88, et une unité de traitement logique 90 comprenant des moyens schématiquement représentés an 92, 94 et 96, et destinés à assurer respectivement des fonctions logiques OU exclusif, ET et SI.

[0052] Les mémoires 80 et 82 contiennent respectivement des valeurs REF et CRT, égales aux valeurs contenues dans l'unité centrale. Pour qu'il en soit ainsi, il suffit qu'au départ, des valeurs égales soient introduites dans les mémoires correspondantes de la serrure et de

l'unité centrale. Ces valeurs s'ajustent ensuite automatiquement.

[0053] Le registre 88 contient une valeur constante MAS égale à la valeur contenue dans le registre 64.

[0054] Pour assurer l'ouverture de la serrure, la mise en marche du système provoque le transfert respectif du contenu des mémoires 80 et 82 dans les registres 30 et 36. Comme représenté sur la figure 3, le code d'accès, décimal, est transformée en binaire et donne la valeur INT introduite en parallèle dans le registre 38. Le contenu de ce registre est ensuite traité par le registre à décalage à récurrence de combinaison de valeurs 86. Simultanément, le contenu du registre 30 est traité comme expliqué on référence à la figure 2.

[0055] Les éléments des cellules de même rang des registres 30, 36 et 88 sont ensuite traités on parallèle au moyen de l'unité logique 90. A chaque fois que les éléments de même rang des registres 30 et 36 sont égaux, l'élément résultant issu de la fonction OU exclusif est égal à 0, alors que s'ils diffèrent, il est égal à 1. En traitant les éléments résultants avec les éléments de même rang de la valeur MAS contenue dans le registre 88, au moyen de la fonction ET 94, les éléments variables de la valeur ALE sont toujours égaux à 0. En d'autres termes, si tous les éléments cryptés de même rang des registres 30 et 36 sont égaux , le signal issu de la porte ET est toujours égal à 0. Si tel est le cas, la fonction SI répond OUI et le verrou est ouvert ou libéré. Si, au contraire, l'un, au moins, des éléments cryptés diffère, la fonction SI répond NON et le verrou reste bloqué.

[0056] Lorsque la valeur introduite est refusée, le contenu des mémoires n'est pas modifié. Si la valeur introduite est acceptée, les contenus des registres 30 et 36 sont respectivement transférés dans les mémoires 80 et 82, comme nouvelles valeurs de référence REF et courante CRT.

[0057] La personne ayant demandé le code donne quittance à l'unité centrale qui transfert dans les mémoires 58 et 60 les contenus respectifs des registres 30 et 44, comme nouvelles valeurs de référence REF et courante CRT, dans le dispositif tel que décrit en référence à la figure 5a.

[0058] On relèvera que dans le système tel que décrit, le code décimal donné à la personne devant ouvrir la serrure est défini par la combinaison d'éléments obtenus à partir du traitement des valeurs mémorisées REF et CRT et d'éléments aléatoires. De la sorte, il est impossible, sur la base du code ainsi donné, de déterminer avec précision quelle sera la valeur du prochain code à introduire. De plus, même on connaissant les rangs qu'occupent les cellules contenant des éléments relatifs à la partie aléatoire, il est impossible de définir un code à venir sans connaître, à la fois, le contenu des valeurs REF et CRT et la structure des registres à décalage à récurrence.

[0059] A cause de cette approche particulière, les moyens mis en oeuvre dans l'unité centrale différent de ceux associés à la serrure et la connaissance de cette dernière ne permet pas de réaliser un programme susceptible de générer des codes à venir. La sécurité d'accès en est, de la sorte, considérablement améliorée.

[0060] Il est bien entendu que le concept défini ci-dessus peut comporter de nombreuses variantes. Le système à commande dynamique peut être associé avec un système classique à code constant.

[0061] Il est fréquent que de telles serrures comportent une double commande, avec une clé électronique et un code d'accès. La partie masquée de la valeur d'entrée INT pourrait être agrandie, de manière à introduire, dans le code, une indication relative à la clé qui doit conjointement être utilisée. Une telle solution augmente encore la sécurité d'accès.

[0062] On relèvera qu'avec le système selon l'invention, la divulgation de la totalité de l'algorithme utilisé ne diminue en rien le niveau de sécurité de la serrure, ce qui n'est pas le cas de celle décrite dans le brevet US 5'488'660.

Revendications

1. Serrure électronique à commande dynamique comportant un instrument (10) pour entrer de données, un dispositif électromagnétique d'actionnement (26) pour commander un verrou (28) et un circuit électronique (12), caractérisée en ce que ledit circuit comprend:

- une première mémoire (80) pour mémoriser une valeur de référence (REF),
- une deuxième mémoire (82) pour mémoriser une valeur courante (CRT),
- une unité de traitement comprenant, un premier registre (30) pour appliquer une fonction sur la valeur de référence (REF), un deuxième registre (36) pour traiter la valeur courante (CRT), un troisième registre (38) pour traiter une valeur d'entrée (INT), des moyens pour transférer la valeur de référence (REF) et la valeur courante (CRT) de sa mémoire dans son registre respectif et réciproquement, et des moyens logiques (32, 40, 42, 90) pour:
  - traiter la valeur de référence (REF) contenue dans le premier registre pour définir une nouvelle valeur de référence remplaçant, dans le premier registre (30), la valeur (REF) antérieure,
  - combiner la valeur courante (CRT) contenue dans le deuxième registre (36) et la valeur d'entrée (INT) contenue dans le troisième registre (38), pour définir une nouvelle valeur courante contenue dans le deuxième registre (36),
  - comparer le contenu des premier (30) et deuxième (36) registres et,

- en cas de concordance uniquement, adresser un ordre au dispositif électromagnétique d'actionnement (26) pour commander le verrou (28), et remplacer dans la première mémoire (80) la valeur de référence qui s'y trouve par la nouvelle valeur de référence contenue dans le premier registre (30) et remplacer dans la deuxième mémoire (82) la valeur courante qui s'y trouve par la nouvelle valeur courante contenue dans le deuxième registre (36).

2. Serrure selon la revendication 1, caractérisée en ce que ladite unité de traitement comporte des registres à décalage, comprenant chacun des cellules, numérotées de *0* à *n*, et dans lesquelles la dernière information introduite occupe la cellule de rang le plus bas.

3. Serrure électronique à commande dynamique selon la revendication 2, caractérisée en ce que ladite unité de traitement comporte, en outre, trois portes OU exclusif (32, 40, 42) munies chacune de deux entrées et d'une sortie, définissant avec lesdits registres:

- un registre à décalage à récurrence (84) de traitement de valeur, comprenant un premier registre à décalage (30) et une porte OU exclusif (32), pour traiter l'ancienne valeur de référence en vue d'obtenir une nouvelle valeur de référence, et

- un registre à décalage à récurrence (86), de combinaison, comprenant un deuxième registre à décalage (36) dans lequel est introduite la valeur courante (CRT), et un troisième registre à décalage (38) dans lequel est introduite la valeur d'entrée (INT) et deux portes OU exclusif (40, 42) pour combiner la valeur courante et la valeur d'entrée et pour définir la nouvelle valeur courante.

4. Serrure selon la revendication 3, caractérisée en ce que l'unité de traitement comporte, en outre, une unité de traitement logique (90) pour vérifier que les cellules de même rang d'une partie au moins du premier et du deuxième registre à décalage (30, 36), ont un contenu identique.

5. Serrure selon l'une des revendications 1 à 3, caractérisée en ce que ladite unité de traitement est agencée de manière qu'elle ne compare qu'une partie seulement des éléments de la valeur courante (CRT) et de la valeur de référence (REF).

6. Serrure selon les revendications 4 et 5, caractérisée en ce que l'unité de traitement logique (90) ne compare qu'une partie seulement des cellules des premier et deuxième registres à décalage(30, 36).

7. Système de commande comportant un dispositif de commande central et au moins une serrure selon la revendication 1, caractérisé en ce que ledit dispositif comprend:

- une première mémoire (58) pour mémoriser une valeur de référence (REF), égale à la valeur de référence contenue dans la première mémoire (80) de la serrure,
- une deuxième mémoire (60) pour mémoriser une valeur courante (CRT), égale à la valeur courante contenue dans la deuxième mémoire (82) de la serrure,
- une unité de traitement comprenant:

  - un premier registre (30) pour traiter la valeur de référence (REF),
  - un deuxième registre (44) pour traiter la valeur courante (CRT),
  - des moyens pour transférer la valeur de référence (REF) et la valeur courante (CRT) de sa mémoire dans son registre respectif et réciproquement,
  - des moyens (62) pour traiter la valeur de référence contenue dans le premier registre (30) pour définir une nouvelle valeur de référence remplaçant la valeur contenue antérieurement dans le premier registre,
  - des moyens (63) pour combiner la valeur courante contenue dans le deuxième registre (44) et la nouvelle valeur de référence, pour définir une valeur d'entrée contenue dans un troisième registre et une nouvelle valeur courante contenue dans le deuxième registre.

8. Système de commande selon la revendication 7, caractérisé en ce que l'unité de traitement et la serrure comportent des registres à décalage (30, 36, 38, 44, 46, 48, 64, 66, 68, 88) comprenant chacun des cellules, numérotées de *0* à *n*, et dans lesquelles la dernière information introduite occupe la cellule de rang le plus bas.

9. Système de commande selon la revendication 8, caractérisé en ce que l'unité de traitement de la serrure comporte, en outre, trois portes OU exclusif (32, 40, 42) munies chacune de deux entrées et d'une sortie, définissant avec lesdits registres:

- un registre à décalage à récurrence (84) de traitement de valeur, comprenant un premier registre à décalage (30) dans lequel est introduite la valeur de référence (REF), et une porte

OU exclusif (32) pour traiter l'ancienne valeur de référence en vue d'obtenir une nouvelle valeur de référence, et

- un registre à décalage à récurrence (86), de combinaison, comprenant un deuxième registre à décalage (36) dans lequel est introduite la valeur courante (CRT), et un troisième registre à décalage (38) dans lequel est introduite la valeur d'entrée (INT) et deux portes OU exclusif (40, 42), pour combiner la valeur courante et la valeur d'entrée et pour définir la nouvelle valeur courante,

et en ce que l'unité de traitement dudit dispositif comporte, en outre, trois portes OU exclusif (32, 50, 52) et un commutateur (54), définissant ensemble:

- un registre à décalage à récurrence (62) de traitement de valeur, comprenant un premier registre à décalage (30) dans lequel est introduite la valeur de référence (REF), et une porte OU exclusif (32) pour traiter l'ancienne valeur de référence en vue d'obtenir une nouvelle valeur de référence, et
- un registre à décalage à récurrence de combinaison et mixage (63), comprenant un deuxième registre à décalage (44) dans lequel la valeur courante (CRT) est introduite, un troisième registre à décalage (46) dans lequel la valeur d'entrée (INT) est introduite, et un quatrième registre à décalage (48) dans lequel est introduite une valeur provenant au moins médiatement du premier registre à décalage (30), et deux portes OU exclusif (40, 42), pour traiter la valeur contenue dans le quatrième registre et l'ancienne valeur courante, en vue d'obtenir la valeur d'entrée (INT) et une nouvelle valeur courante (CRT).

10. Système selon la revendication 9, caractérisé en ce que l'unité de traitement de la serrure comporte, on outre, une unité de traitement logique (90) pour vérifier que les cellules de même rang d'une partie au moins du premier (30) et du deuxième registre (36), ont un contenu identique.

11. Système selon la revendication 10, caractérisé en ce que ladite unité de traitement logique (90) de la serrure est agencée de manière qu'elle ne compare qu'une partie seulement des éléments de la valeur courante (CRT) et de la valeur de référence (REF) et on ce que l'unité de traitement dudit dispositif comporte, en outre, une unité de traitement logique (70) pour traiter la valeur de référence (REF) contenue dans le premier registre à décalage (30) et pour introduire la valeur après traitement dans ledit quatrième registre à décalage (48), un cinquième (64) et un sixième registre à décalage (68) coopérant avec l'unité de traitement logique (70) pour respectivement masquer un certain nombre de cellules du premier registre (30) et pour introduire une valeur aléatoire (ALE) dans des cellules dont les éléments ne font pas l'objet de ladite comparaison.

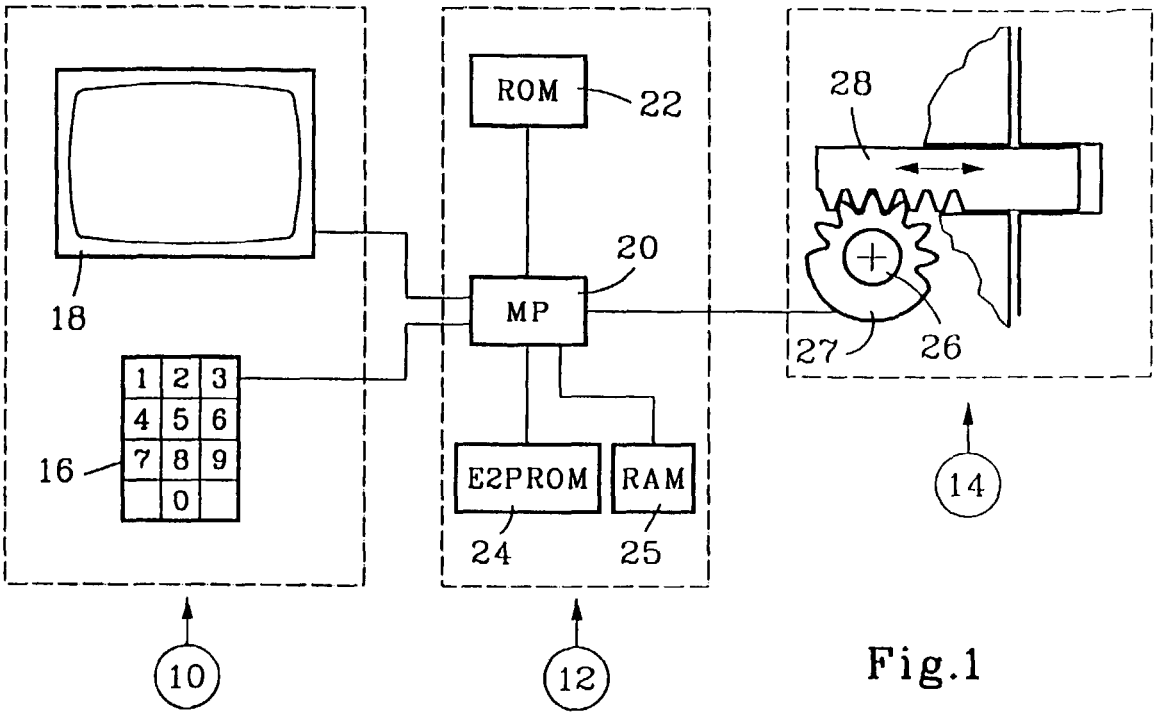
ROM
22
28
20
MP
18
1 2 3
4 5 6
7 8 9
0
16
27
26
E2PROM
RAM
24
25
14
10
12

Fig.1

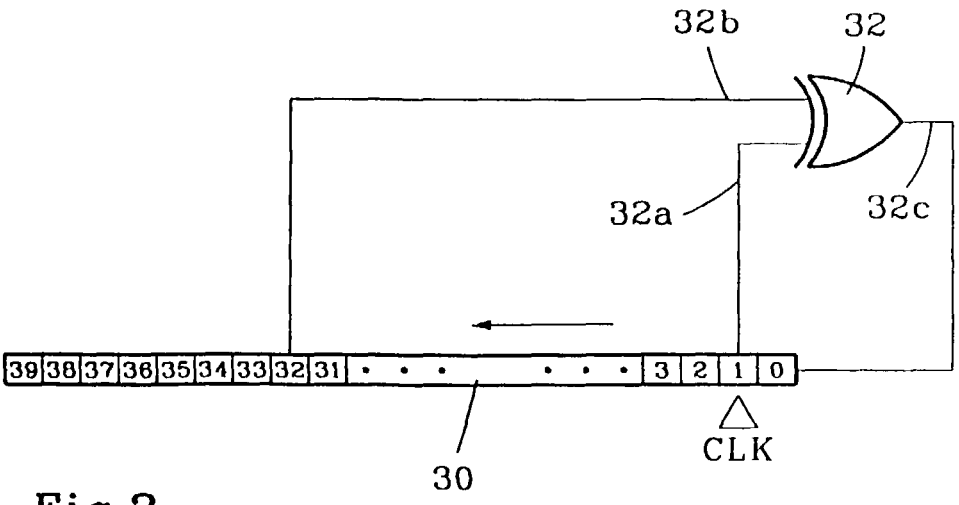
32b
32
32a
32c
39 38 37 36 35 34 33 32 31 . . . . . 3 2 1 0
CLK
30

Fig.2

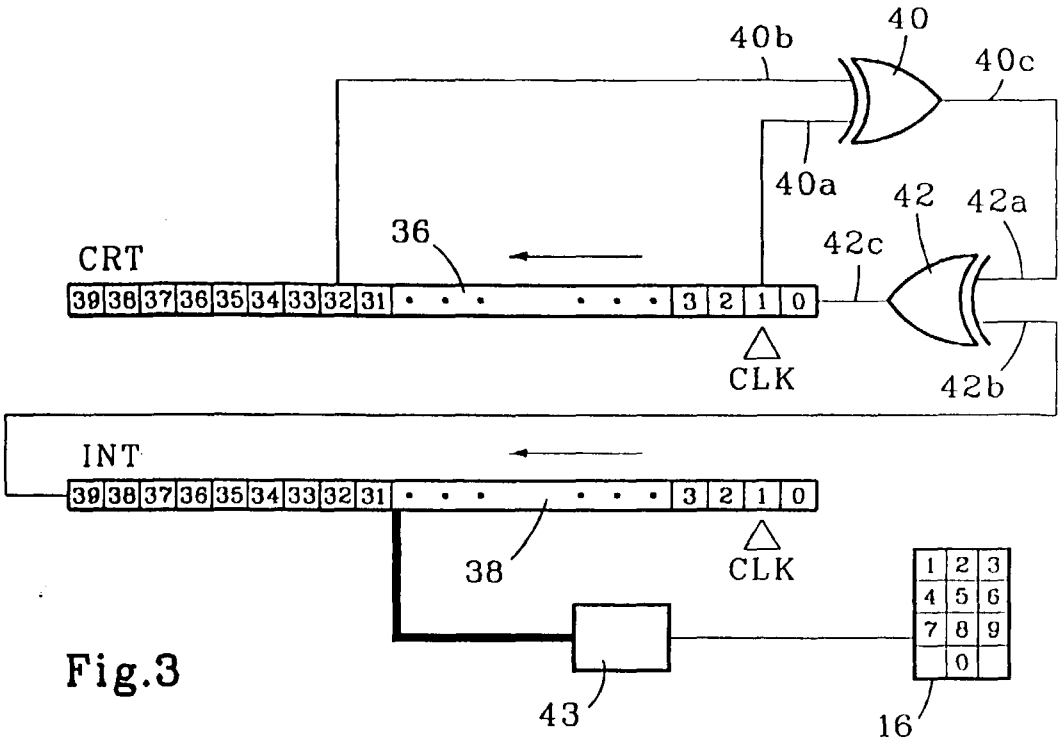
40b
40
40c
40a
42
42a
36
CRT
42c
39 38 37 36 35 34 33 32 31 . . . 3 2 1 0
CLK
42b
INT
39 38 37 36 35 34 33 32 31 . . . 3 2 1 0
38
CLK
1 2 3
4 5 6
7 8 9
0
43
16

Fig.3

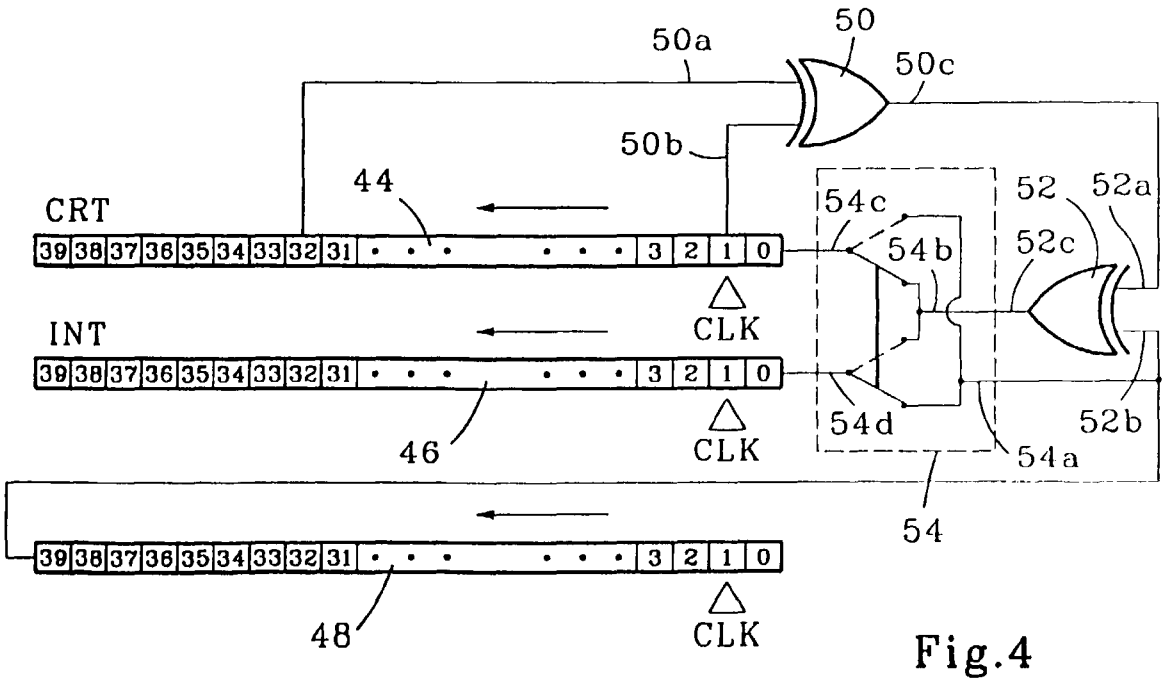
50a
50
50c
50b
44
52
52a
CRT
54c
54b
52c
39 38 37 36 35 34 33 32 31 . . . 3 2 1 0
CLK
INT
39 38 37 36 35 34 33 32 31 . . . 3 2 1 0
54d
52b
46
CLK
54a
54
39 38 37 36 35 34 33 32 31 . . . 3 2 1 0
48
CLK

Fig.4

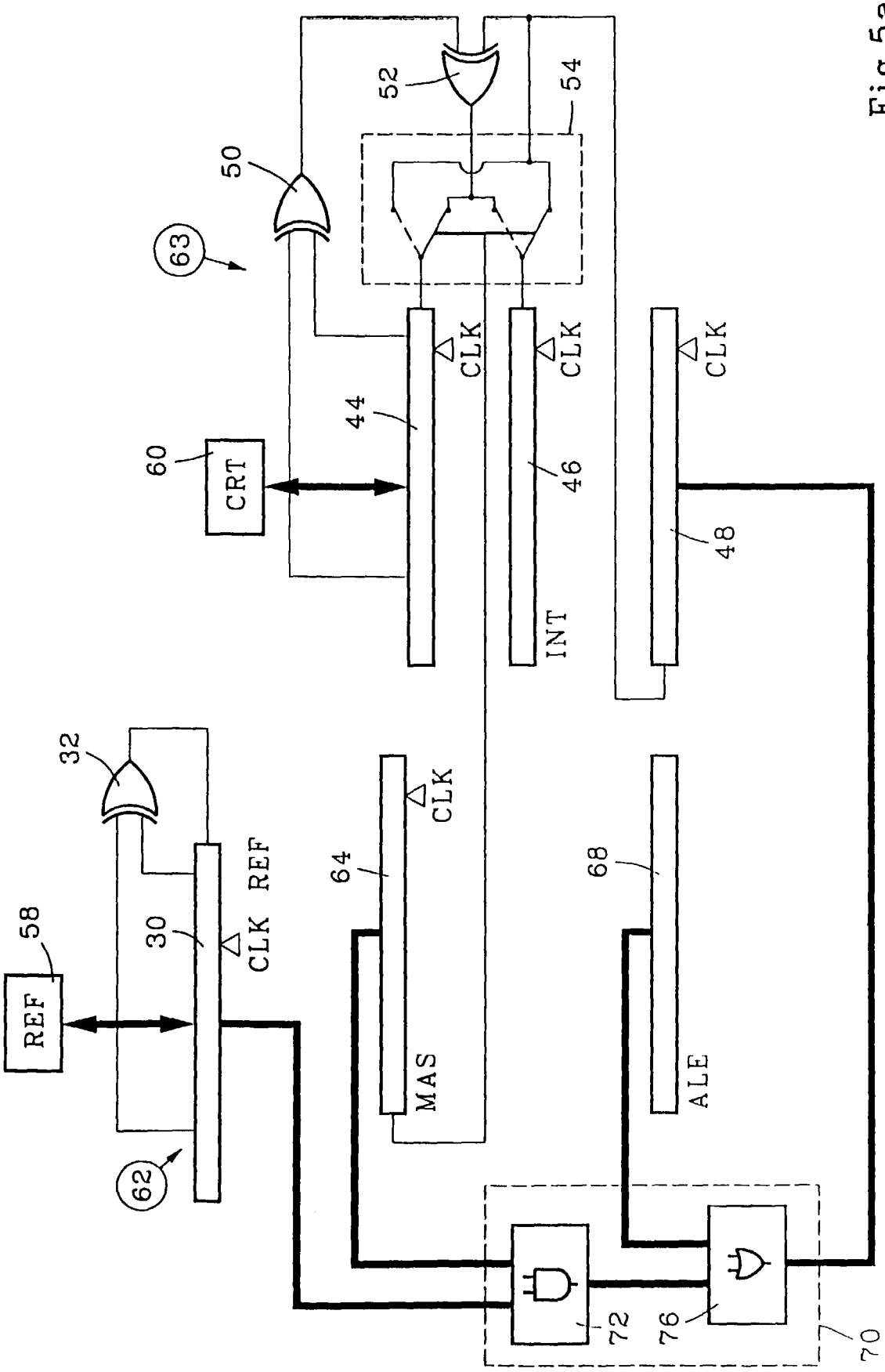
52
54
50
63
CLK
CLK
CLK
44
60
CRT
46
48
INT
32
64
CLK
68
58
30
CLK REF
REF
MAS
ALE
62
72
76
70

Fig.5a

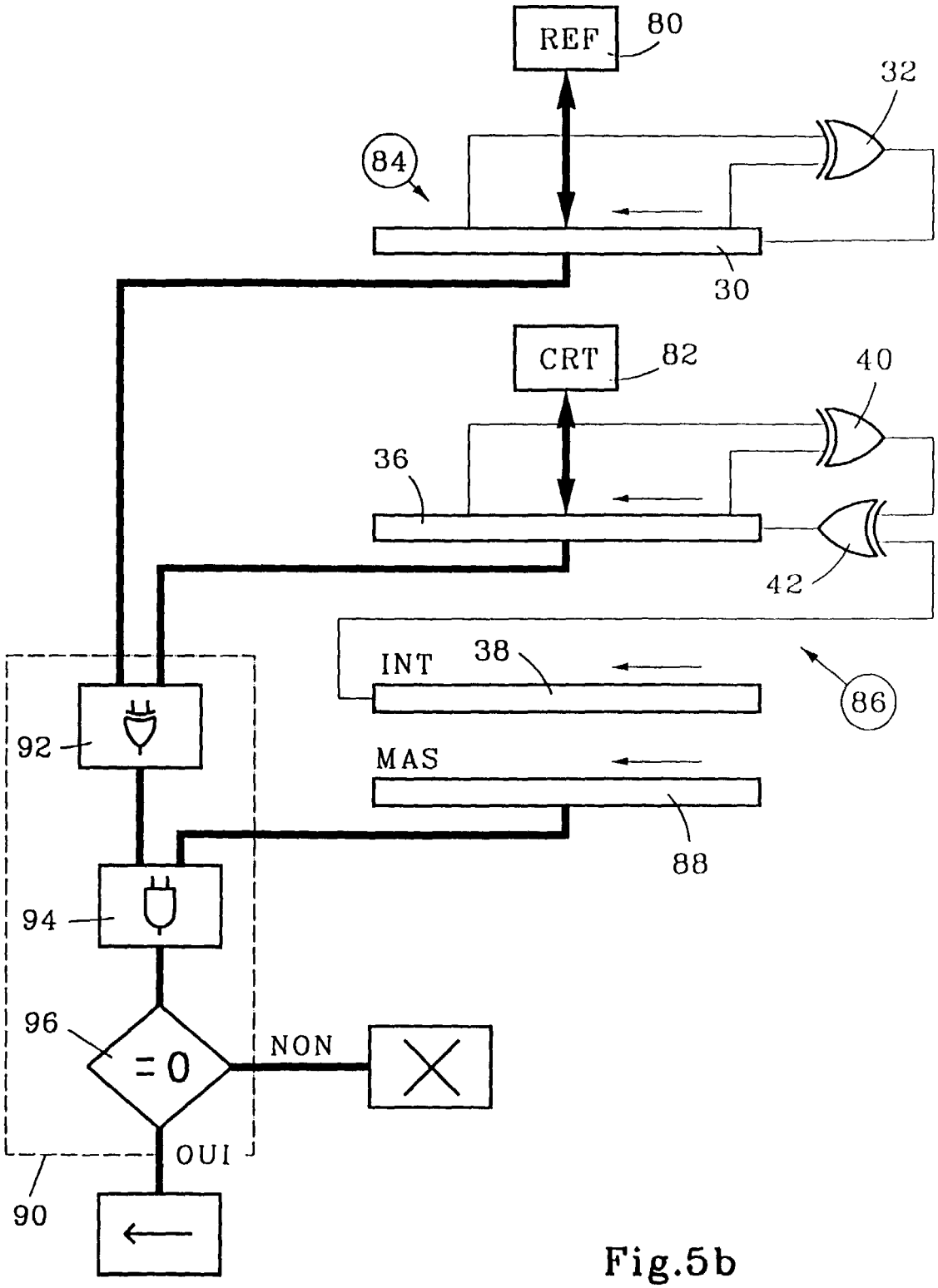

Fig.5b

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 99 11 7014

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
A	US 5 363 448 A (KOOPMAN,FINN) 8 novembre 1994 (1994-11-08) * colonne 4, ligne 47 - colonne 14, ligne 27; figures 1,2 *	1-3,7-9	E05B49/00 H04L9/32
A	US 5 420 925 A (MICHAELS) 30 mai 1995 (1995-05-30) * colonne 3, ligne 50 - colonne 8, ligne 5; figures 1,2 *	1-3,7-9	
A	GB 2 306 722 A (BURRI,RENARD) 7 mai 1997 (1997-05-07) * page 4, ligne 13 - page 9, ligne 22; figures 1-6 *	1-3,7-9	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)

E05B
H04L

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	1 novembre 1999	Herbelet, J.C.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

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

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 99 11 7014

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets citée dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnée à titre indicatif et n'engagent pas la reponsabilité de l'Office européen des brevets.

01-11-1999

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5363448 A	08-11-1994	CA 2159360 A	12-01-1995
		DE 69418714 D	01-07-1999
		EP 0706735 A	17-04-1996
		EP 0872976 A	21-10-1998
		JP 8512183 T	17-12-1996
		WO 9501685 A	12-01-1995
		US RE36181 E	06-04-1999
US 5420925 A	30-05-1995	CA 2139530 A	04-09-1995
		EP 0670402 A	06-09-1995
GB 2306722 A	07-05-1997	AUCUN	

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets. No.12/82