(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
16 octobre 2003 (16.10.2003)

PCT

(10) Numéro de publication internationale
WO 03/085496 A1

(51) Classification internationale des brevets[7] : G06F 1/00

(21) Numéro de la demande internationale :
PCT/FR03/01024

(22) Date de dépôt international : 2 avril 2003 (02.04.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/04321 8 avril 2002 (08.04.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **CANAL + TECHNOLOGIES** [FR/FR]; 34, place Raoul Dautry, F-75015 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **DAUVOIS, Jean Luc** [FR/FR]; 19, rue Eugène Manuel, F-75116 Paris (FR).

(74) Mandataire : **DU BOISBAUDRY, Dominique**; c/o Brevalex, 3, rue du Docteur Lancereaux, F-75008 Paris (FR).

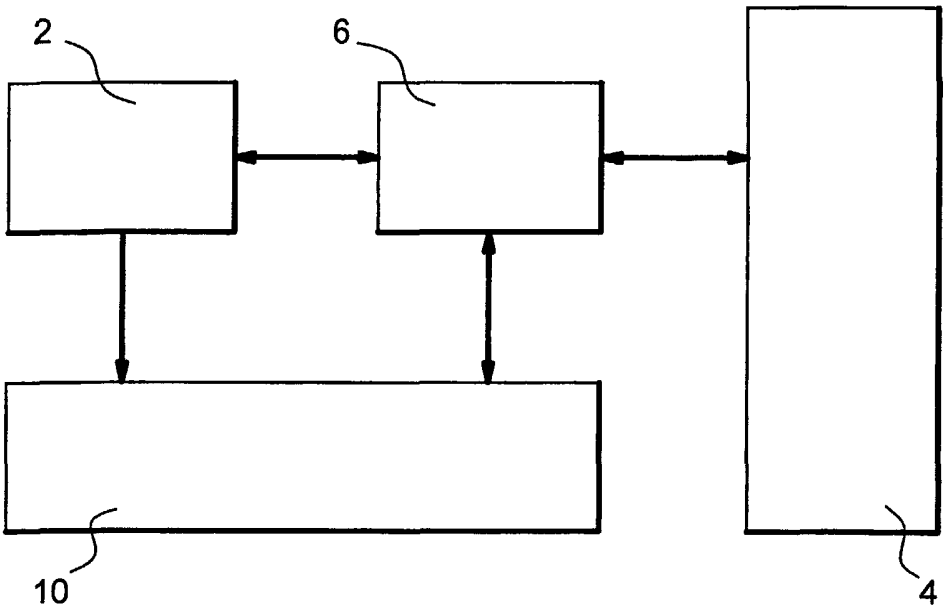
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR PROTECTING DIGITAL DATA STORED IN A MEMORY

(54) Titre : PROCEDE ET DISPOSITIF DE PROTECTION DE DONNEES NUMERIQUES STOCKEES DANS UNE MEMOIRE



(57) Abstract: The invention concerns a method for protecting digital data stored in a memory (4) and previously encrypted with an encryption key. The inventive method is characterized in that said encryption key is dynamically defined on the basis of at least one operating parameter intrinsic to said smart card.

[Suite sur la page suivante]

WO 03/085496 A1

TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de protection de données numériques stockées dans une mémoire (4) et préalablement cryptées par une clé de chiffrement. Le procédé selon l'invention est caractérisé par le fait que ladite clé de chiffrement est définie dynamiquement en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite carte à puce.

PROCEDE ET DISPOSITIF DE PROTECTION DE DONNEES NUMERIQUES STOCKEES DANS UNE MEMOIRE

Domaine technique

L'invention se situe dans le domaine de la lutte contre le piratage du contenu des mémoires de stockage de données et concerne plus particulièrement un procédé de protection de données numériques stockées dans une mémoire d'une carte à puce et préalablement cryptées par une clé de chiffrement.

L'invention concerne également une carte à puce et un dispositif de protection de la mémoire de cette carte à puce.

Etat de la technique antérieure

Le piratage d'une carte à puce se fait en général par l'extraction du code ROM et des données secrètes contenues dans la mémoire de la carte. Une technique connue pour éviter que ces données sensibles ne soient utilisables après une extraction frauduleuse consiste à les chiffrer au moyen de clés secrètes avant de les stocker dans la mémoire de la carte. Les clés de chiffrement utilisées sont également stockées dans cette mémoire et sont de ce fait également exposées au risque d'une extraction frauduleuse au même titre que les données utiles mémorisées. Aussi, cette technique ne permet-elle pas de lutter efficacement contre le piratage.

Le but de l'invention est d'assurer une sécurité optimale des données mémorisées sous forme cryptée dans une mémoire.

Un autre but de l'invention est de lier intimement les clés de chiffrement à un ou plusieurs paramètres de fonctionnement intrinsèque à au moins un élément composant la carte. Ces paramètres de fonctionnement pouvant être des grandeurs physiques dépendant de la structure physique de la mémoire ou du microcontrôleur associé à cette mémoire ou encore des grandeurs reflétant un comportement déterminé de cette mémoire et du microcontrôleur dans des conditions particulières d'utilisation.

Exposé de l'invention

De façon plus précise, l'invention concerne un procédé et un dispositif de protection de données numériques stockées sous forme cryptée dans une mémoire qui peut être du type EEPROM ou du type flash par exemple.

Le procédé selon l'invention est caractérisé par le fait que ladite clé de chiffrement est définie dynamiquement en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite carte à puce.

Selon l'invention, ledit paramètre de fonctionnement intrinsèque à la carte à puce est généré par un générateur de fonction intégré à la carte à puce.

Selon l'invention, ledit paramètre de fonctionnement est intrinsèque à la mémoire de la carte à puce.

Selon un mode de réalisation, le procédé comporte les étapes suivantes :

•lors de la phase d'écriture des données dans la mémoire,

a- dériver un signal analogique d'une tension analogique d'écriture dans la mémoire,

b- convertir ce signal en une séquence numérique,

c- chiffrer les données à mémoriser au moyen de ladite séquence numérique,

d- stocker les données chiffrées dans la mémoire,

•et lors d'une phase ultérieure de lecture des données mémorisées,

- recalculer la clé de chiffrement définie aux étapes a et b de la phase d'écriture et

- décrypter les données au moyen de la clé recalculée.

Selon ce mode de réalisation, la tension analogique d'écriture est fournie par une pompe de charge.

Le dispositif selon l'invention est caractérisé par le fait qu'il comporte un module de calcul apte à définir une clé de chiffrement des données numériques à mémoriser en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite carte à puce.

Selon un mode de réalisation de l'invention, le module de calcul extrait un signal analogique d'une tension analogique d'écriture délivrée par une pompe de charge et convertit ce signal analogique en une séquence numérique pour constituer la clé de chiffrement.

L'invention concerne également une carte de contrôle d'accès comportant une unité centrale de traitement de données, au moins une mémoire de stockage de données, un module de chiffrement desdites données numériques et un module de calcul d'au moins une clé de chiffrement desdites données.

La carte de contrôle d'accès selon l'invention comporte des moyens pour définir la clé de chiffrement en fonction d'au moins un paramètre de fonctionnement intrinsèque à la mémoire de ladite carte, et des moyens pour recalculer dynamiquement la clé de chiffrement préalablement définie à chaque lecture des données mémorisées.

Selon une caractéristique de l'invention le module de calcul est fonctionnellement indépendant de l'unité centrale de sorte que le calcul de la clé de chiffrement est simplement initié et non supervisé par l'unité centrale de traitement.

Selon un mode particulier de réalisation de l'invention, le module de calcul comporte une pompe de charge destinée à fournir une tension analogique d'écriture des données dans la carte à puce, un convertisseur analogique/numérique destiné à convertir un signal analogique extrait de ladite tension analogique en une séquence numérique constituant la clé de chiffrement.

Brève description des dessins

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va

suivre, prise à titre d'exemple non limitatif, en référence aux figures annexées, dans lesquelles :

- la figure 1 représente un schéma général d'un dispositif selon l'invention.
- la figure 2 représente schématiquement un mode particulier de réalisation du dispositif de la figure 1.
- la figure 3 représente une courbe illustrant une mise en œuvre de l'invention dans le cas de l'exemple illustré par la figure 2.

Exposé détaillé de modes de réalisation particuliers

L'invention va maintenant être décrite dans le cadre de la protection des données stockées dans la mémoire d'une carte à puce.

Les carte à puces sont largement utilisées notamment pour mémoriser des paramètres de contrôle permettant l'accès à des données ou services tels que par exemple des programmes audiovisuels cryptés. Dans ce type d'application, les informations nécessaires au désembrouillage sont transmises dans des messages de contrôle d'accès, appelés ECM (Entitlement Control Message) et sont générés à partir des données d'entrées suivantes :

- un mot de contrôle (Control Word) destiné à initialiser la séquence de désembrouillage,
- une clé de service (Service Key) utilisée pour embrouiller le mot de contrôle, pour un groupe d'un ou de plusieurs utilisateurs,
- une clé utilisateur (user key) utilisée pour embrouiller la clé de service.

Préalablement, la clé de service est transmise, dans des messages appelés EMM générés à partir d'une clé utilisateur individuelle ou de groupe.

Les ECM sont notamment constitués du mot de contrôle et traités par la clé de service et sont transmis aux abonnés à intervalles réguliers.

Les EMM sont notamment constitués de la clé de service et traités par la ou les clés utilisateurs, et sont également transmis aux abonnés à intervalles réguliers.

A la réception, le principe de décryptage consiste à retrouver la clé de service à partir de la ou des clés utilisateurs contenue dans la mémoire d'une carte à puce (EMM). Cette clé de service est ensuite elle-même utilisée pour décrypter les ECM afin de retrouver le mot de contrôle permettant l'initialisation du système de désembrouillage.

Comme cela a été expliqué précédemment, le contenu de la mémoire de la carte à puce peut être extrait et réutilisé de façon frauduleuse pour retrouver les clés de traitement des EMM et des ECM qui, directement ou indirectement, permettent de calculer le mot de contrôle permettant l'initialisation du système de désembrouillage.

La figure 1 représente un schéma bloc général d'un dispositif à mémoire comportant une unité centrale de traitement 2 reliée à une mémoire 4 via un module de cryptage/décryptage 6. Un module de calcul 10, agencé extérieurement à l'unité centrale 2, est également relié au module de cryptage/décryptage 6.

Lorsque des données traitées dans l'unité centrale 2 doivent être stockées dans la mémoire 4, l'unité de traitement 2 envoie au module de calcul 10 un signal d'activation. A la réception de ce signal, le module de calcul 10 définit une clé de chiffrement des données à mémoriser et transmet cette clé au module de cryptage/décryptage 6.

Selon une caractéristique essentielle de l'invention, la clé de chiffrement est calculée au moment de la mémorisation des données dans la mémoire 4 en fonction d'au moins un paramètre de fonctionnement intrinsèque à la mémoire 4. La clé de chiffrement ainsi calculée n'est pas stockée dans la mémoire 4. Or le piratage des cartes à puces consiste généralement à extraire les programmes de calcul mis en œuvre dans l'unité centrale 2 et les données sensibles contenues dans la mémoire 4 associée à l'unité centrale 2. Aussi, en cas d'extraction frauduleuse de ces programmes et du contenu de la mémoire 4, les données extraites seront inutilisables sans la clé de chiffrement qui est calculée dynamiquement lors de la mémorisation desdites données et lors de la lecture de ces données.

Préférentiellement, cette clé est calculée en fonction d'un paramètre ou d'une combinaison de plusieurs paramètres de fonctionnement intrinsèque à ladite mémoire 4.

La clé de chiffrement définie est inaccessible de l'extérieur, du fait que le module de calcul 10 est indépendant de l'unité centrale 2.

En fonctionnement, au moment du transfert des données de l'unité centrale 2 vers le module de calcul

10, ce dernier reçoit de l'unité centrale 2 un premier signal d'activation, lui permettant de commencer le calcul de la clé de chiffrement. La clé ainsi calculée est transmise au module de cryptage/décryptage 6 qui l'utilise pour chiffrer les données avant que ces dernières ne soient mémorisées dans la mémoire 4.

Lorsque les données cryptées doivent être lues, l'unité de traitement 2 envoie au module de calcul 10 un deuxième signal d'activation pour recalculer dynamiquement la clé de chiffrement qui est ensuite utilisée par le module de cryptage/décryptage 6 pour décrypter lesdites données et les transmettre à l'unité centrale 2.

Un exemple particulier de calcul de la clé de chiffrement va être décrit maintenant en référence à la figure 2 représentant un exemple de réalisation de l'invention dans lequel le module 10 est constitué par la pompe de charge 12 destinée à fournir une tension analogique d'écriture des données dans la mémoire 4, un convertisseur analogique-numérique (CAN) 14 destiné à convertir un signal analogique extrait de ladite tension analogique en une séquence numérique constituant la clé de chiffrement, une horloge 16 reliée à la pompe de charge 12 destinée à fixer la durée du signal analogique extrait de la tension d'écriture.

La tension analogique peut être fournie par un générateur de tension analogique indépendant de la pompe de charge.

Dans un autre mode de réalisation non représenté, la carte à puce peut comporter un circuit

numérique indépendant de l'unité centrale 2 qui fournit directement une séquence numérique S.

La figure 3 représente schématiquement l'évolution en fonction du temps de la tension d'écriture 18 des données numériques provenant de l'unité centrale 2 dans la mémoire 4. Une valeur A de la tension 18 est fixée par programmation de la durée t au moyen de l'horloge 16. Cette valeur A est ensuite convertie par le CAN 14 en une séquence numérique S qui est utilisée par le module de cryptage/décryptage 6 pour crypter/décrypter les données numériques.

A chaque remise à zéro, le module de calcul 10 calcule la clé de chiffrement en prenant en considération la durée t programmée au moyen de l'horloge 16. Ainsi, si un pirate extrait les données numériques, il ne pourra pas recalculer la clé de chiffrement qui dépend de la valeur A qui est intrinsèque à la carte authentique. La clé de chiffrement est calculée pour la première fois lors de la personnalisation de la carte à puce.

Dans une variante de réalisation de l'invention, plusieurs durées t correspondant à plusieurs valeurs A peuvent être préprogrammées afin d'être utilisées successivement pour calculer plusieurs clés de chiffrement différentes, chaque clé pouvant être utilisée pendant une période prédéfinie.

Dans une autre variante de réalisation, la durée t peut être modifiée à distance.

REVENDICATIONS

1. Procédé de protection de données numériques stockées dans une mémoire (4) d'une carte à puce et préalablement cryptées par une clé de chiffrement, caractérisé en ce que ladite clé de chiffrement est définie dynamiquement en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite carte à puce.

2. Procédé selon la revendication 1, caractérisé en ce que lesdites données numériques cryptées sont des clés numériques destinées au codage cryptographique de messages EMM et ECM.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que le ledit paramètre de fonctionnement intrinsèque à la carte à puce est généré par un générateur de fonction intégré à la carte à puce.

4. Procédé selon la revendication 1, caractérisé en ce que ledit paramètre de fonctionnement est intrinsèque à la mémoire de la carte à puce.

5. Procédé selon la revendication 4, caractérisé en ce qu'il comporte les étapes suivantes :

•lors de la phase d'écriture des données dans la mémoire(4),

a) dériver un signal analogique d'une tension analogique (18) d'écriture dans la mémoire (4),

b) convertir ce signal en une séquence numérique S,

c) chiffrer les données à mémoriser au moyen de ladite séquence numérique S,

d) stocker les données chiffrées dans la mémoire (4),.

•et lors d'une phase ultérieure de lecture des données mémorisées,

- recalculer la clé de chiffrement définie aux étapes a et b, et
- décrypter les données au moyen de la clé recalculée.

6. Procédé selon la revendication 5, caractérisé en ce que la tension analogique d'écriture (18) est fournie par une pompe de charge (12).

7. Dispositif de protection de données numériques stockées dans une mémoire (4) d'une carte à puce et préalablement cryptées par une clé de chiffrement, caractérisé en ce qu'il comporte un module de calcul (10) apte à définir la clé de chiffrement desdites données en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite carte à puce.

8. Dispositif selon la revendication 7, caractérisé en ce que lesdites données numériques sont des clés numériques destinées au codage cryptographique de messages EMM et ECM.

9. Dispositif selon la revendication 7, caractérisé en ce que le ledit paramètre de fonctionnement intrinsèque à la carte à puce est généré

par un générateur de fonction intégré à la carte à puce.

10. Dispositif selon la revendication 9, caractérisé en ce que ledit paramètre de fonctionnement est intrinsèque à la mémoire de la carte à puce.

11. Dispositif selon la revendication 10, caractérisé en ce que ladite clé de chiffrement est calculée à partir d'une tension analogique (18) d'écriture des données dans la mémoire de la carte à puce.

12. Dispositif selon la revendication 11, caractérisé en ce que ladite tension analogique d'écriture est délivrée par une pompe de charge.

13. Dispositif selon les revendications 7 et 11, caractérisé en ce que le module de calcul (10) extrait un signal analogique de ladite tension (18) et convertit ce signal analogique en une séquence numérique pour constituer la clé de chiffrement.

14. Dispositif selon la revendication 13, caractérisé en ce que le module de calcul (10) comporte un convertisseur analogique/numérique (14).

15. Carte de contrôle d'accès comportant une unité centrale de traitement de données, au moins une mémoire de stockage de données, un module de chiffrement (6) desdites données numériques et un

module de calcul (10) d'au moins une clé de chiffrement desdites données, caractérisée en ce que ledit module de calcul (10) comporte des moyens pour définir la clé de chiffrement en fonction d'au moins un paramètre de fonctionnement intrinsèque à ladite mémoire (4), et des moyens pour recalculer dynamiquement ladite clé de chiffrement à chaque lecture des données mémorisées.

16. Carte de contrôle d'accès selon la revendication 15, caractérisé en ce que la tension analogique est fournie par un générateur de tension indépendant de la pompe de charge.

17. Carte de contrôle d'accès selon la revendication 15, caractérisée en ce que le module de calcul (10) est fonctionnellement indépendant de l'unité centrale (2) de sorte que le calcul de la clé de chiffrement n'est pas supervisé par l'unité centrale de traitement(2).

18. Carte à puce selon la revendication 17, caractérisée en ce que le module de calcul (10) comporte une pompe de charge (12) destinée à fournir une tension analogique (18) d'écriture des données dans la carte à puce, un convertisseur analogique-numérique (14) destiné à convertir un signal analogique extrait de ladite tension analogique (18) en une séquence numérique S constituant la clé de chiffrement.

19. Carte à puce selon la revendication 18, caractérisée en ce que le module de calcul (10)

comporte un générateur de fonction analogique destiné à fournir une tension analogique, un convertisseur analogique-numérique (14) destiné à convertir ladite tension analogique en une séquence numérique (S) constituant la clé de chiffrement.

20. Carte à puce selon la revendication 19, caractérisée en ce qu'elle comporte un circuit numérique indépendant de l'unité centrale (2) destiné à générer la séquence numérique (S).

21. Carte à puce selon la revendication 15, caractérisée en ce que le module de chiffrement (6) est un circuit logique.

22. Carte à puce selon l'une des revendications 15 à 21, caractérisée en ce que la mémoire (4) est du type EEPROM.

23. Carte à puce selon la revendication 22, caractérisée en ce que la mémoire (4) est du type flash.

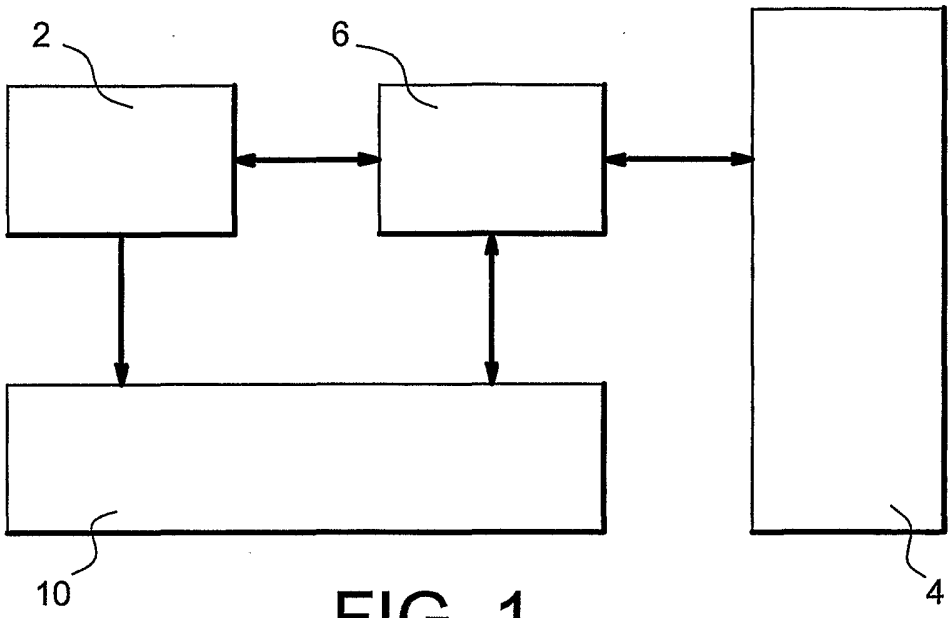


FIG. 1

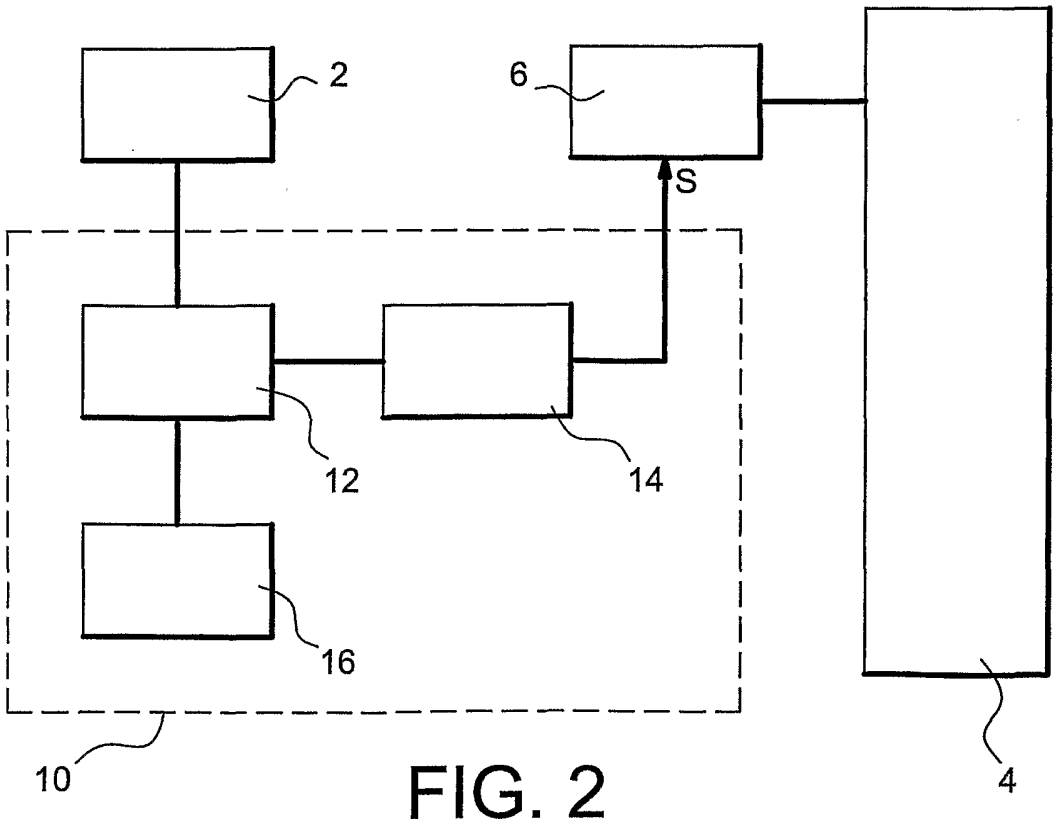


FIG. 2

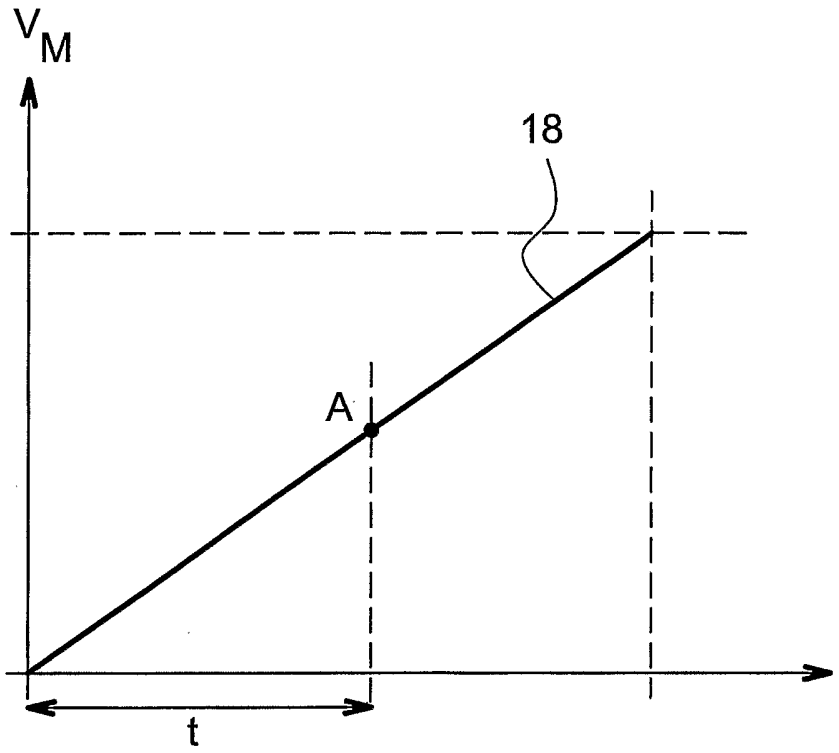


FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/01024

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 818 738 A (EFFING WOLFGANG) 6 October 1998 (1998-10-06) abstract	1-4, 7-11,15, 17,21-23
A	column 2, line 1 - line 21 column 2, line 37 - line 49 column 4, line 17 - line 32 column 6, line 54 -column 7, line 13 column 8, line 4 - line 42 column 11, line 25 - line 51 column 15, line 59 - line 67 figures 1,4A,4B,4C,10 --- -/--	5,6, 12-14, 16,18-20

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 September 2003	12/09/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, L

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/01024

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 233 339 B1 (HIROTA MASAKI ET AL) 15 May 2001 (2001-05-15) column 4, line 39 - line 53 column 16, line 5 - line 57 figure 17	1,7,15
A	EP 0 984 403 A (MINDPORT BV) 8 March 2000 (2000-03-08) column 2, line 57 -column 3, line 40	2,8
A	US 6 047 068 A (RHELIMI ALAIN ET AL) 4 April 2000 (2000-04-04) abstract column 1, line 13 - line 15	1,2,8

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/01024

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5818738 A	06-10-1998	DE 3736882 A1	13-07-1989
		AT 87383 T	15-04-1993
		DE 3879616 D1	29-04-1993
		WO 8904022 A1	05-05-1989
		EP 0313967 A1	03-05-1989
		ES 2039551 T3	01-10-1993
		HK 60395 A	28-04-1995
		JP 2501961 T	28-06-1990
		JP 2925152 B2	28-07-1999
US 6233339 B1	15-05-2001	JP 10187546 A	21-07-1998
EP 0984403 A	08-03-2000	EP 0984403 A1	08-03-2000
		CN 1317127 T	10-10-2001
		WO 0013151 A1	09-03-2000
		JP 2002524785 T	06-08-2002
US 6047068 A	04-04-2000	FR 2738970 A1	21-03-1997
		FR 2738971 A1	21-03-1997
		AT 187271 T	15-12-1999
		DE 69605445 D1	05-01-2000
		DE 69605445 T2	21-06-2000
		EP 0861479 A1	02-09-1998
		WO 9711442 A1	27-03-1997
		JP 11514466 T	07-12-1999

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 03/01024

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 5 818 738 A (EFFING WOLFGANG) 6 octobre 1998 (1998-10-06) abrégé	1-4, 7-11,15, 17,21-23
A	colonne 2, ligne 1 - ligne 21 colonne 2, ligne 37 - ligne 49 colonne 4, ligne 17 - ligne 32 colonne 6, ligne 54 -colonne 7, ligne 13 colonne 8, ligne 4 - ligne 42 colonne 11, ligne 25 - ligne 51 colonne 15, ligne 59 - ligne 67 figures 1,4A,4B,4C,10	5,6, 12-14, 16,18-20

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
3 septembre 2003	12/09/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Arbutina, L

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 03/01024

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
X	US 6 233 339 B1 (HIROTA MASAKI ET AL) 15 mai 2001 (2001-05-15) colonne 4, ligne 39 - ligne 53 colonne 16, ligne 5 - ligne 57 figure 17	1,7,15
A	EP 0 984 403 A (MINDPORT BV) 8 mars 2000 (2000-03-08) colonne 2, ligne 57 -colonne 3, ligne 40	2,8
A	US 6 047 068 A (RHELIMI ALAIN ET AL) 4 avril 2000 (2000-04-04) abrégé colonne 1, ligne 13 - ligne 15	1,2,8

RAPPORT DE RECHERCHE INTERNATIONALE

Dema[redacted] Internationale No
PCT/FR 03/01024

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 5818738	A	06-10-1998	DE	3736882 A1	13-07-1989
			AT	87383 T	15-04-1993
			DE	3879616 D1	29-04-1993
			WO	8904022 A1	05-05-1989
			EP	0313967 A1	03-05-1989
			ES	2039551 T3	01-10-1993
			HK	60395 A	28-04-1995
			JP	2501961 T	28-06-1990
			JP	2925152 B2	28-07-1999
US 6233339	B1	15-05-2001	JP	10187546 A	21-07-1998
EP 0984403	A	08-03-2000	EP	0984403 A1	08-03-2000
			CN	1317127 T	10-10-2001
			WO	0013151 A1	09-03-2000
			JP	2002524785 T	06-08-2002
US 6047068	A	04-04-2000	FR	2738970 A1	21-03-1997
			FR	2738971 A1	21-03-1997
			AT	187271 T	15-12-1999
			DE	69605445 D1	05-01-2000
			DE	69605445 T2	21-06-2000
			EP	0861479 A1	02-09-1998
			WO	9711442 A1	27-03-1997
			JP	11514466 T	07-12-1999