

(12)

DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 08.04.02.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 10.10.03 Bulletin 03/41.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : CANAL + TECHNOLOGIES Société anonyme — FR.

(72) Inventeur(s) : DAUVOIS JEAN LUC.

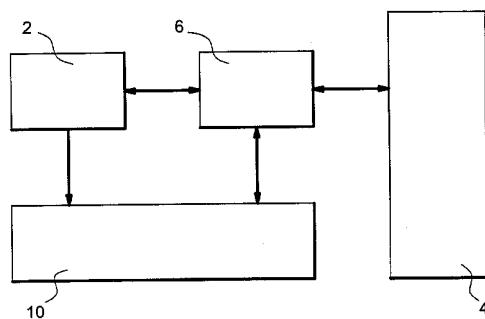
(73) Titulaire(s) :

(74) Mandataire(s) : BREVALEX.

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

(57) 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

5 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.

10 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

15 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 20 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 25 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 30 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,

5 b- convertir ce signal en une séquence numérique,

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

10 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

15 - 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.

20 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.

25 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.

5 - la figure 2 représente schématiquement un mode particulier de réalisation du dispositif de la figure 1.

10 - 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 15 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 20 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 :

25 - 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,

30 - 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.

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

10 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.

15 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.

20 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.

25 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 5 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 10 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 15 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 20 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 25 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.

30 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 5 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 10 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 15 convertisseur analogique-numérique (CAN) 14 destiné à convertir un signal analogique extrait de ladite tension analogique en une séquence numérique constituante la clé de chiffrement, une horloge 16 reliée à la pompe de charge 12 destinée à fixer la 20 durée du signal analogique extrait de la tension 25 d'écriture.

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

30 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 5 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 10 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 15 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 20 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 25 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.

10

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.

15

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.

20

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

25

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) ,

30 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), .

5 •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.

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

15 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
20 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
25 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
30 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,
5 caractérisé en ce que ledit paramètre de fonctionnement est intrinsèque à la mémoire de la carte à puce.

11. Dispositif selon la revendication 10,
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,
15 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,
25 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
30 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).

20 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.

30 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) 5 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 10 générer la séquence numérique (S) .

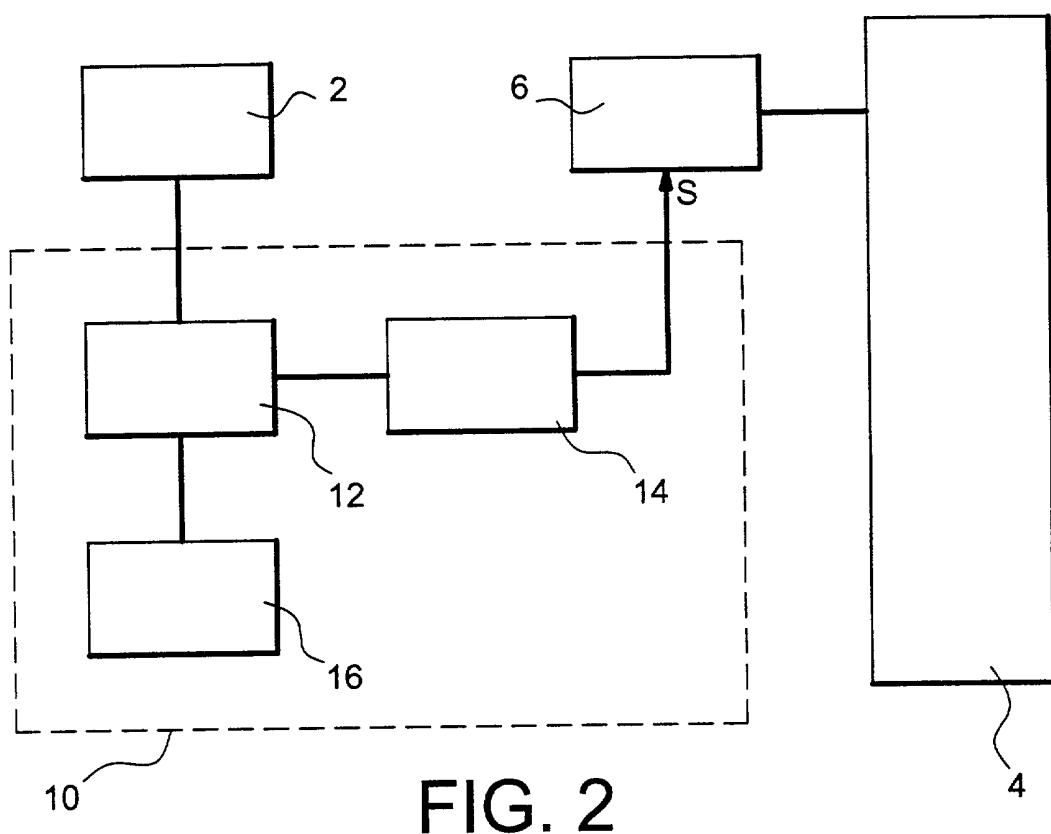
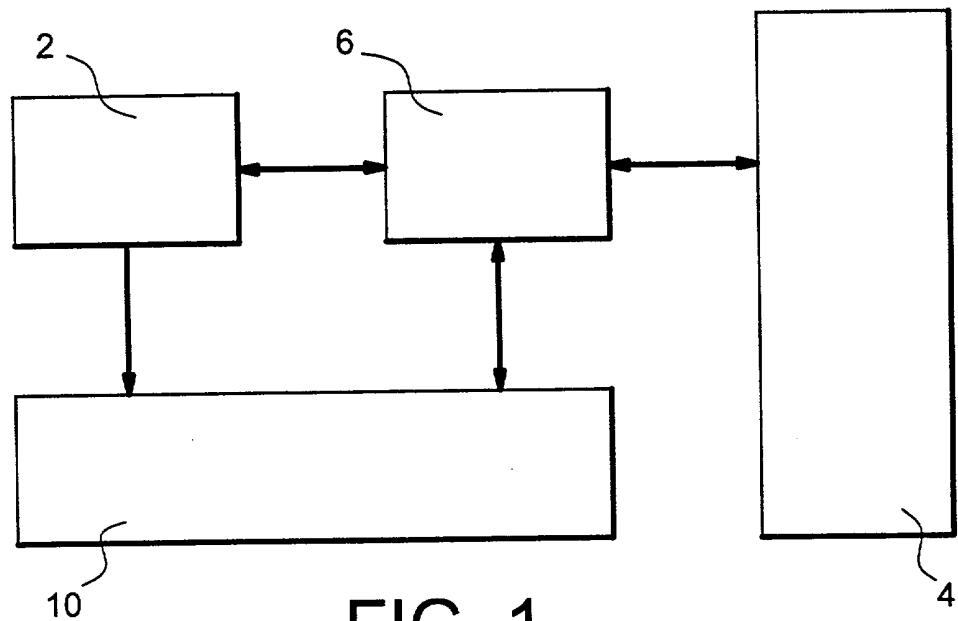
21. Carte à puce selon la revendication 15, caractérisée en ce que le module de chiffrement (6) est un circuit logique.

15

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

20

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



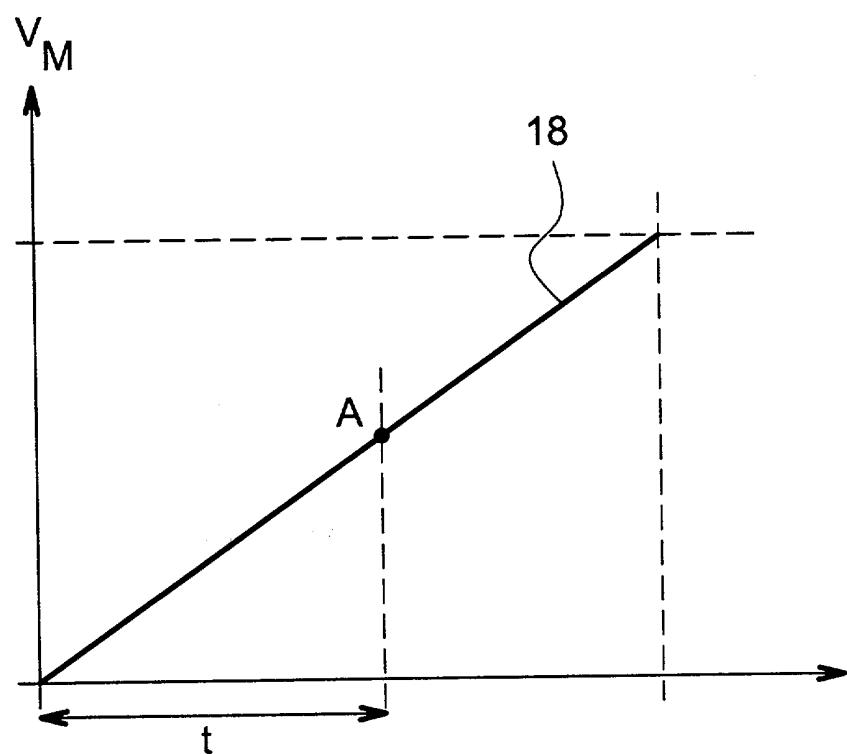


FIG. 3

RAPPORT DE RECHERCHE
PRÉLIMINAIRE

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

FA 622033
FR 0204321

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI		
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes				
X	US 5 818 738 A (EFFING WOLFGANG) 6 octobre 1998 (1998-10-06)	1-4, 7-11, 15, 17, 21-23	G06F12/14 H04L9/32 G06K19/07		
A	* abrégé * * 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	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	G06F G07F		
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			
1		Date d'achèvement de la recherche	Examinateur		
21 janvier 2003		Arbutina, L			
CATÉGORIE DES DOCUMENTS CITÉS					
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 bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant					

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0204321 FA 622033**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **21-01-2003**.

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française.

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 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	13-07-1989
US 6233339	B1	15-05-2001	JP	10187546 A	21-07-1998
EP 0984403	A	08-03-2000	EP CN WO JP	0984403 A1 1317127 T 10-10-2001 0013151 A1 09-03-2000 2002524785 T 06-08-2002	08-03-2000
US 6047068	A	04-04-2000	FR FR AT DE DE EP WO JP	2738970 A1 21-03-1997 2738971 A1 21-03-1997 187271 T 15-12-1999 69605445 D1 05-01-2000 69605445 T2 21-06-2000 0861479 A1 02-09-1998 9711442 A1 27-03-1997 11514466 T 07-12-1999	21-03-1997