(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
11 décembre 2003 (11.12.2003)

PCT

(10) Numéro de publication internationale
WO 03/102883 A1

(51) Classification internationale des brevets[7] : G07F 7/10, G06F 1/00

(21) Numéro de la demande internationale : PCT/FR03/01627

(22) Date de dépôt international : 28 mai 2003 (28.05.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/06592 30 mai 2002 (30.05.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Parc d'activités de Gèmenos, Avenue du Pic de Bertagne, F-13420 Gèmenos (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **PETIT, Sébastien** [FR/FR]; 3, boulevard Chanzy, F-83330 Le Beausset (FR). **TRIA, Assia** [FR/FR]; Chemin des Marseillais, F-13390 Auriol (FR). **BENOIT, Olivier** [FR/FR]; Résidence Central Parc, Bâtiment F, F-13400 Aubagne (FR).

(74) Mandataire : **AIVAZIAN, Denis**; Gemplus La Vigie, Service Brevets, B.P. 90, F-13705 La Ciotat Cedex (FR).

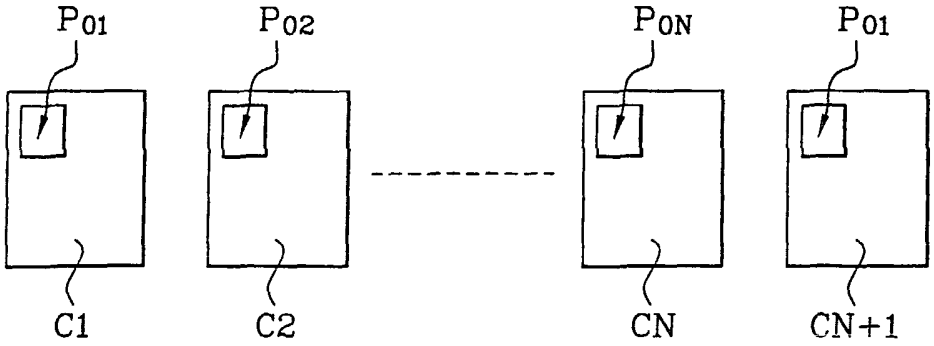
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, 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, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) **Title:** SECURED METHOD FOR DEPLOYING A COMPUTER PROGRAMME ON DISCRETE DATA SUPPORTS

(54) **Titre :** PROCEDE SECURISE DE DEPLOIEMENT D'UN PROGRAMME INFORMATIQUE SUR DES SUPPORTS D'INFORMATIONS DISTINCTS



(57) **Abstract:** The invention relates to a secured method for deployment of a programme (Po) which comprises providing N different versions (Po1, Po2, PoN) of said programme (Po) and loading different versions on discrete data supports (C1, , CN). The differentiation is preferably carried out by a compilation programme and a link editor programme (Ced) which introduce one or several variations at each compilation operation. The invention is applied to the secured deployment of programmes on different data supports such as portable devices with chipcards.

(57) **Abrégé :** L'invention concerne un procédé sécurisé de déploiement d'un programme Po consistant à fournir N versions diversifiées (Po1, Po2, PoN) de ce programme Po et à charger des versions différentes sur des supports d'informations distincts (C1,..., CN). Avantageusement, la diversification est réalisée par un programme de compilation et un programme éditeur de liens (Ced) qui introduisent une ou plusieurs variantes à chaque opération de compilation. L'invention s'applique au déploiement sécurisé des programmes sur des supports d'informations distincts tels que des dispositifs portables de type cartes à puce.

WO 03/102883 A1

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes 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, UZ, VC, VN, YU, ZA, ZM, ZW, 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, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes 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, UZ, VC, VN, YU, ZA, ZM, ZW, 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, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

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.

PROCEDE SECURISE DE DEPLOIEMENT D'UN PROGRAMME INFORMATIQUE SUR DES SUPPORTS D'INFORMATIONS DISTINCTS.

L'invention concerne un procédé sécurisé de déploiement d'un programme informatique sur des supports d'informations distincts. Elle concerne également un procédé de diversification de programmes informatiques. L'invention s'applique à la sécurisation de dispositifs électroniques contenant un ou plusieurs programmes informatiques et plus particulièrement à la sécurisation des dispositifs portables de type cartes à puce.

Le problème posé concerne d'une manière générale la sécurité des programmes d'ordinateurs contre les attaques qui permettent d'extraire des informations sensibles lorsque ces programmes sont susceptibles de traiter des données confidentielles. Ce problème concerne en particulier la sécurité contre la fraude de dispositifs portables de type cartes à puce, lesquels sont par nature, utilisés pour stocker et exploiter des données secrètes.

On constate malheureusement que ces dispositifs sont sujets à de nombreuses attaques malveillantes de nature diverses. Ces attaques ont été répertoriées et analysées et leurs principes vont être rappelés ci-dessous :

Une première attaque dite « side channel » consiste à étudier la consommation électrique, la radiation électromagnétique ou toute autre modification de l'environnement du composant électronique lorsqu'il participe à l'exécution d'un programme informatique. A partir de l'observation de cette consommation, il devient possible de déduire l'instant de traitement des

données confidentielles ainsi que les données elles-mêmes.

Une deuxième attaque consiste à modifier l'environnement physique du composant électronique (température, lumière ...) de manière à modifier le déroulement normal du programme qui est exécuté; il est alors possible de déterminer puis d'intervenir au moment précis du traitement des données confidentielles. Par exemple, une influence physique externe au moment du traitement d'un code confidentiel peut amener le programme à accepter un mauvais code.

Une troisième attaque possible consiste en une intrusion physique au sein des composants électroniques afin d'espionner ou de modifier les informations qui transitent sur des bus de données par exemple. Il est ainsi possible de déterminer l'instant précis où les données confidentielles sont manipulées afin de les intercepter.

Pour lutter contre ces fraudes, les solutions de sécurité de l'art antérieur consistent à prévoir des protections et contre-mesures qui repoussent au maximum ces attaques.

Globalement les solutions connues à ce jour ont pour but de rajouter des obstacles logiques ou physiques à toute tentatives de fraude. En pratique, ces obstacles augmentent le temps nécessaire et la complexité pour décoder le déroulement du programme. Malheureusement une fois que le déroulement du programme est connu, il est possible d'appliquer facilement cette connaissance sur tous les dispositifs contenant le même programme afin de récupérer les données confidentielles qu'ils peuvent détenir.

L'invention a donc pour but de remédier à ces inconvénients.

Elle a pour objet un procédé sécurisé de déploiement d'un programme Po principalement caractérisé en ce qu'il consiste à fournir N versions diversifiées de ce programme Po et à charger des versions différentes sur des supports d'informations distincts.

Les différentes versions d'un même programme réalisent les mêmes fonctions essentielles, donnent le même résultat mais ont un comportement légèrement différent lors de leur exécution.

Avantageusement, les N versions différentes du programme Po sont obtenues de la manière suivante :

le programme Po est écrit dans un langage quelconque,

le programme est ensuite traduit N fois par un programme de diversification.

Selon un mode de réalisation, le programme de diversification est un programme de compilation et un programme éditeur de liens qui introduisent une ou plusieurs variantes à chaque opération de compilation.

Les supports prévus peuvent être X dispositifs portables de type cartes à puce, les N versions étant réparties sur les X dispositifs, X étant supérieur ou égal à N.

L'invention a également pour objet un procédé de diversification d'un programme Po principalement caractérisé en ce qu'il consiste à prévoir un programme de diversification apte à introduire des variantes dans le programme Po de manière à obtenir N versions différentes dudit programme.

Selon un mode de réalisation, le programme de diversification est réalisé par un programme compilateur et un programme éditeur de liens, la

diversification se faisant durant la compilation et/ou l'édition de liens dudit programme Po.

Une première variante introduite durant la compilation et l'édition de liens consiste à modifier, d'une version à l'autre, les adresses des fonctions ou sous-programmes dudit programme Po, de la mémoire de programmes dans laquelle il sera enregistré.

Une deuxième variante introduite consiste à modifier, d'une version à l'autre, les adresses des registres tampons et des variables de la mémoire de travail.

Une troisième variante consiste à modifier au moins un paramètre dudit programme ou une instruction par une instruction équivalente, ou un sous-ensemble d'instructions par un autre sous-ensemble d'instructions fonctionnellement équivalent ou ajouter des opérations inutiles d'une version à l'autre dudit programme.

Le procédé de diversification d'un programme Po, est avantageusement utilisé pour la mise en œuvre du déploiement sécurisé dudit programme Po sur des supports d'informations distincts tels que des dispositifs portables de type cartes à puce.

L'invention concerne en outre un procédé de personnalisation de supports d'informations de type cartes à puce principalement caractérisé en ce qu'il consiste à utiliser le procédé de déploiement sécurisé d'un programme Po énoncé ci-dessus.

D'autres particularités et avantages de l'invention apparaîtront clairement dans la description suivante, présentée à titre d'exemple non limitatif en regard des figures annexées qui représentent :

- la figure 1, un schéma classique illustrant la transformation classique d'un programme écrit en langage quelconque en un programme exécutable,
- la figure 2, illustre le principe de la présente invention permettant d'avoir plusieurs versions d'un même programme,
- la figure 3, illustre un premier exemple de diversification,
- la figure 4, illustre un deuxième exemple de diversification,
- la figure 5, illustre un troisième exemple de diversification.
- la figure 6, illustre le déploiement d'un programme sur des cartes à puces.

On rappelle pour mieux comprendre la suite qu'un programme principal Po écrit en langage de programmation fait l'objet d'une compilation réalisée par un programme de compilation pour pouvoir être compris par l'unité de traitement du dispositif support qui exécute le programme. Une unité de traitement comprend, et cela de manière classique, un processeur (ou microprocesseur ou microcontrôleur) et des mémoires volatiles et non volatiles. L'unité de traitement peut être installée soit dans un microordinateur soit dans tout autre dispositif électronique à base d'un microprocesseur.

Lorsque le programme principal Po fait appel à un ou plusieurs sous-programmes SP1, SP2, SP3, un autre programme appelé éditeur de liens ed, intègre les différents sous-programmes dans le programme principal Po compilé pour le rendre exécutable. Cette transformation est schématisée par le bloc Ced de la figure 1.

Afin de simplifier la description qui va suivre on désignera par F1, F2, F3, des fonctions ou des sous programmes du programme principal Po.

Selon l'invention, il est donc proposé de déployer le programme Po sous différentes versions Po1, Po2, PoN de manière à assurer une sécurité contre la fraude. La transformation réalisée est illustrée par le schéma de la figure 2.

Ce déploiement est réalisé par diversification du programme Po.

Plusieurs solutions de diversification vont être décrites dans la suite. Ces solutions peuvent être bien évidemment combinées c'est-à-dire qu'une même version présentera plusieurs variantes par rapport à une autre version. Ceci contribue à renforcer encore plus la sécurité apportée par la diversification.

Les N versions peuvent être obtenues bien entendu par une programmation individuelle de chacune d'elle ou au moyen d'un programme de diversification.

De façon avantageuse, il est prévu que cette diversification soit mise en œuvre par un programme compilateur réalisé à cet effet et/ ou par un programme éditeur de liens comme cela va être détaillé à travers les différents exemples donnés dans la suite.

Comme cela est illustré sur la figure 2, un programme Po unique écrit dans un langage quelconque (C par exemple), va donc pouvoir être fourni en N versions Po1, Po2 …, PoN, grâce aux opérations de compilation et d'édition de liens Ced. Les différentes versions assurent les mêmes fonctions que le programme Po tout en présentant des caractéristiques différentes qui font que la connaissante du comportement d'un programme ne permettra pas d'en retirer des informations utiles pour une autre version de ce même programme.

Une première solution proposée consiste à diversifier les adresses aux quelles se trouvent les fonctions ou sous-programmes nécessaires lors de l'exécution du programme Po, dans la mémoire de programme MP (mémoire électriquement programmable de type EEPROM ou Flash/EEPROM). Ces adresses sont donc modifiées par le compilateur (s'il s'agit de fonctions du programme) ou par l'éditeur de lien lorsqu'il s'agit de sous-programmes appelés. Cette solution est illustrée sur la figure 3.

On suppose, pour illustrer le propos que le programme Po fait appel aux trois fonctions et/ou sous-programmes F1, F2, F3, tel que cela est illustré sur la figure 2. Ces fonctions se trouvent classiquement à des adresses fixées de la mémoire de programme MP. Grâce à la transformation opérée par le compilateur, les fonctions vont se trouver à des adresses distinctes sur chaque version du programme. Sur la version Po1, F1 se trouve aux adresses ad1-adp ; F2 se trouve aux adresses adr-ads et F3 se trouve aux adresses ads-adn. Sur la version Po2, F1 se trouve aux adresses ado-ad4, F2 se trouve aux adresses ad4-adp et F3 se trouve aux adresses adp-adq. Sur la version PoN, F1 se trouve aux adresses ado-ad4, F2 se trouve aux adresses adp-adq et F3 se trouve aux adresses adq-adr.

Une autre solution consiste à effectuer ce même type de diversification d'adresse mais cette fois ci pour la mémoire de travail MT (mémoire volatile RAM).

On rappelle que classiquement et à titre d'exemple, pour exécuter une opération arithmétique par exemple C=A+B, l'unité arithmétique et logique du dispositif support utilise deux registres R1 et R2. Le compilateur charge la valeur A qui est à l'adresse AD1 de la mémoire de travail dans le registre R1 et charge la

valeur B qui est à l'adresse AD2 de cette mémoire dans le registre R2. Le résultat C est stocké à l'adresse AD3 (les instructions de chargement et de transfert sont utilisées pour la mise en œuvre de cette opération.)

Selon l'invention, il peut être prévu que le chargement du contenu de ces deux registres se fasse à des adresses différentes pour chaque version de programme Po.

De manière plus générale, pour une instruction I donnée, l'adresse de chargement du contenu des registres peut être modifiée par le compilateur. Un exemple pratique est illustré sur la figure 4, pour la mise en œuvre de l'opération C=A+B.

Une autre solution consiste à réaliser une diversification des paramètres du programme ou des instructions elles-mêmes.

Plusieurs exemples vont illustrer cette solution dans la suite :

Il peut être prévu par exemple d'exécuter une instruction d'une manière différente sans rien changer au résultat soit en rajoutant des opérations inutiles soit en changeant une instruction par une instruction équivalente.

Par exemple, une opération arithmétique telle que A+B peut être modifiée par le compilateur en A+C+B-C.

Les valeurs de C seront différentes d'une version à l'autre.

Une opération de transfert A→B peut être modifiée en A→C→B.

Une opération conditionnelle : si A+B alors F sinon G, peut être modifiée par l'opération conditionnelle : si A≠B alors G sinon F.

Ces différents exemples sont illustrés par le schéma de la figure 5.

Comme cela a été dit, l'invention s'applique tout particulièrement au déploiement de programmes contenant des données sensibles pour des dispositifs portables tels que les cartes à puce ou autres objets équivalents. Le ou les programmes déployés seront chargés en mémoire électriquement programmable de type EEPROM ou Flash/EEPROM.

Si un programme est modifié de manière à se trouver sous forme de 100 versions distinctes, ces 100 versions seront déployées de manière aléatoire pour équiper l'ensemble du parc de carte à puce prévu. Il est bien évident que si ce parc représente 1 million de cartes à puce distribuées sur tout un territoire géographique (qui peut être très étendu), des lots de cartes à puce posséderont une même version dudit programme. Cependant le nombre de carte à puce par lot sera insuffisant pour pouvoir retirer des caractéristiques intéressantes pour un fraudeur, d'autant plus que le déploiement géographique des cartes va empêcher pratiquement la reconstitution d'un même lot pour tout fraudeur.

La figure 6, illustre le déploiement des versions Po1, ...PoN, PoN+1 du programme Po sur des cartes à puce C1,... CN, CN+1.

Une version donnée d'un programme peut être chargée à tout moment dans une carte à puce, soit avant sa distribution aux organismes de personnalisation soit pendant la personnalisation soit après c'est-à-dire lorsqu'un utilisateur possède cette carte.

Les programmes pouvant faire l'objet d'une telle diversification peuvent être des programmes d'application mais aussi le programme du système d'exploitation (OS) du dispositif portable.

REVENDICATIONS

1. Procédé de déploiement d'un programme Po, caractérisé en ce qu'il consiste à fournir N versions diversifiées de ce programme Po et à charger des versions différentes sur des supports d'informations distincts assurant ainsi une sécurité contre la fraude par analyse des caractéristiques dudit programme.

2. Procédé sécurisé de déploiement d'un programme selon la revendication 1, caractérisé en ce que les N versions différentes du programme Po sont obtenues de la manière suivante :

le programme Po est écrit dans un langage quelconque,

le programme est ensuite traduit N fois par un programme de diversification.

3. Procédé sécurisé de déploiement d'un programme selon la revendication 2, caractérisé en ce que le programme de diversification est un programme de compilation et un programme éditeur de liens qui introduisent une ou plusieurs variantes à chaque opération de compilation.

4. Procédé sécurisé de déploiement d'un programme selon l'une quelconque des revendications précédentes, caractérisé en ce que les supports prévus sont X dispositifs portables de type cartes à puce, les N versions étant réparties sur les X dispositifs, X étant supérieur ou égal à N.

5. Procédé de diversification d'un programme Po, caractérisé en ce qu'il consiste à prévoir un programme de diversification apte à introduire des variantes dans le programme Po de manière à obtenir N versions différentes de ce programme Po, assurant les mêmes fonctions que celui-ci tout en ayant des caractéristiques de comportement différentes, la connaissance du comportement d'une version de programme ne permettant pas de retirer des informations utiles pour une autre version.

6. Procédé de diversification d'un programme Po selon la revendication 5, caractérisé en ce que le programme de diversification est réalisé par un programme compilateur et un programme éditeur de liens, la diversification se faisant durant la compilation et/ou l'édition de liens dudit programme Po.

7. Procédé de diversification d'un programme Po selon la revendication 5 ou 6, caractérisé en ce qu'une première variante introduite durant la compilation et l'édition de liens consiste à modifier, d'une version à l'autre, les adresses de chargement des fonctions ou sous-programmes dudit programme Po, de la mémoire de programmes dans laquelle il sera enregistré.

8. Procédé de diversification d'un programme Po, selon les revendications 5, 6 ou 7, caractérisé en ce qu'une deuxième variante introduite consiste à modifier, d'une version à l'autre, les adresses des registres tampons et des variables de la mémoire de travail utilisée pendant l'exécution dudit programme Po.

9. Procédé de diversification d'un programme Po, selon l'une quelconque des revendications 5 à 8, caractérisé qu'une troisième variante consiste à modifier au moins un paramètre dudit programme ou une instruction par une instruction équivalente, ou un sous-ensemble d'instructions par un autre sous-ensemble d'instructions fonctionnellement équivalent ou ajouter des opérations inutiles d'une version à l'autre dudit programme.

10. Procédé de diversification d'un programme Po, selon l'une quelconque des revendications 5 à 9, caractérisé en ce qu'il est mis en œuvre pour réaliser un déploiement sécurisé dudit programme Po sur des supports d'informations distincts tels que des dispositifs portables de type cartes à puce et assurer ainsi une sécurité contre la fraude par analyse des caractéristiques dudit programme.

11. Procédé de personnalisation de supports d'informations de type cartes à puce, caractérisé en ce qu'il comprend le chargement d'un programme Po, ce chargement étant mis en œuvre le procédé de déploiement selon la revendication 1.

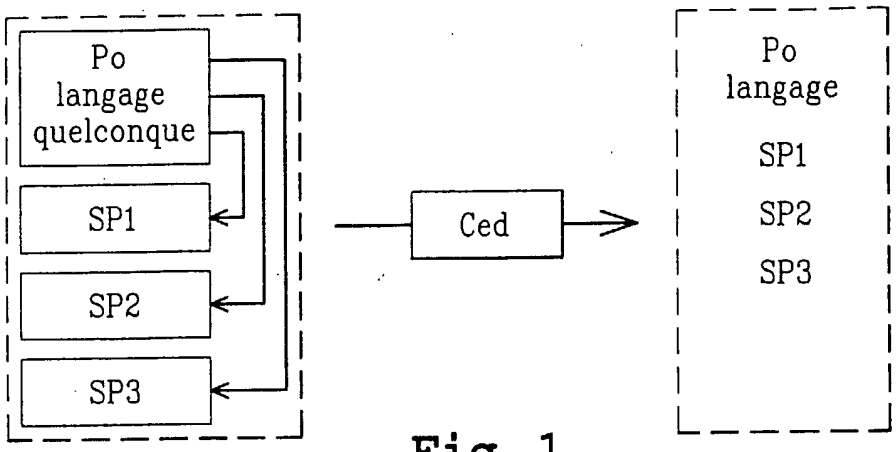

Po
langage
quelconque
SP1
SP2
SP3
Ced
Po
langage
SP1
SP2
SP3

Fig. 1

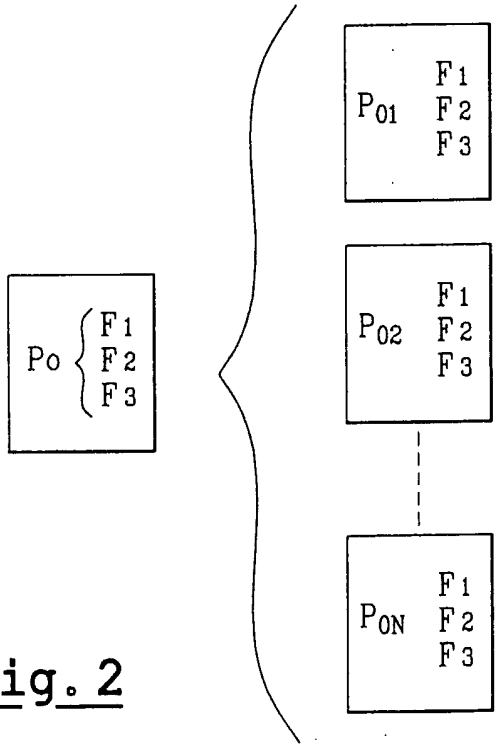

Po
F1
F2
F3
P01
F1
F2
F3
P02
F1
F2
F3
PON
F1
F2
F3

Fig. 2

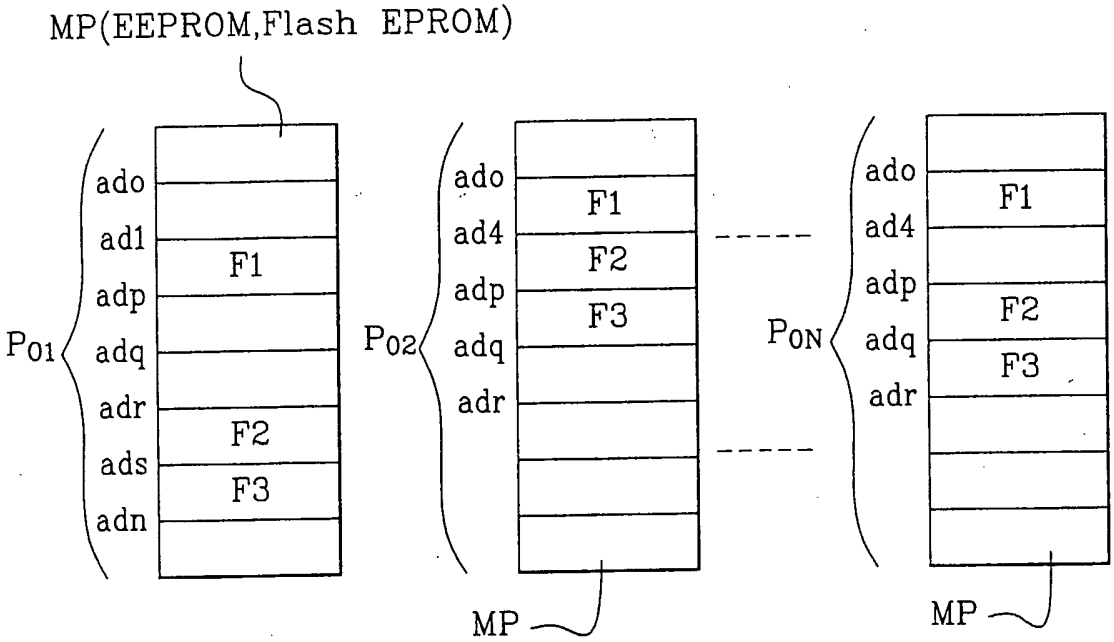

MP(EEPROM,Flash EPROM)
ado
ad1
adp
adq
adr
ads
adn
F1
F2
F3
P01
P02
PON
MP
MP

Fig. 3

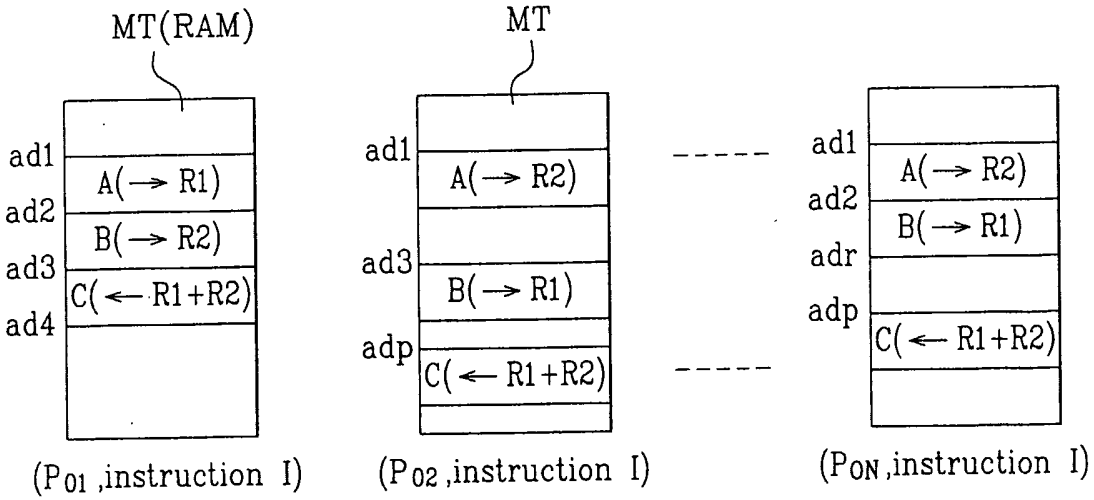

MT(RAM)
MT
ad1
ad2
ad3
ad4
adp
adr
A(→ R1)
B(→ R2)
C(← R1+R2)
A(→ R2)
B(→ R1)
C(← R1+R2)
(P01 ,instruction I)
(P02 ,instruction I)
(PON ,instruction I)

Fig. 4

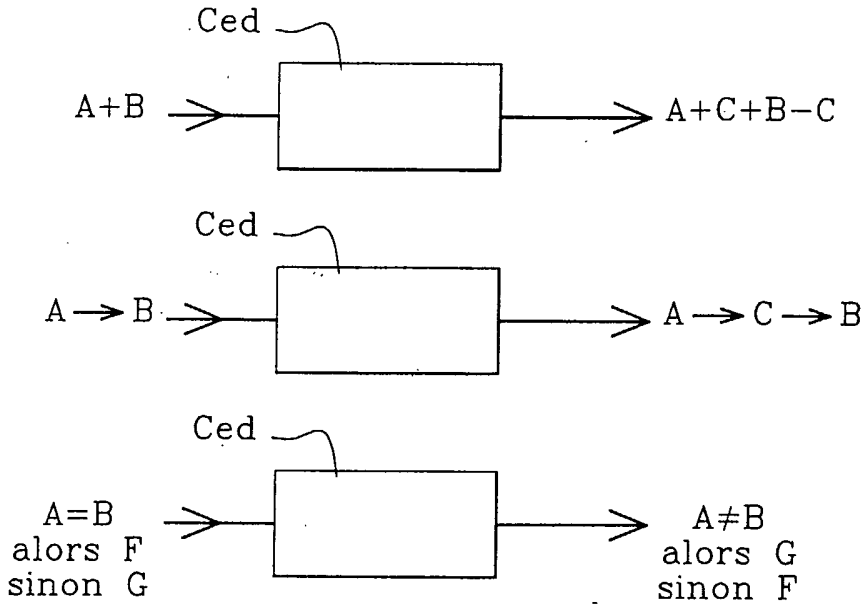

Ced
A+B
A+C+B−C
Ced
A → B
A → C → B
Ced
A=B
alors F
sinon G
A≠B
alors G
sinon F

Fig. 5

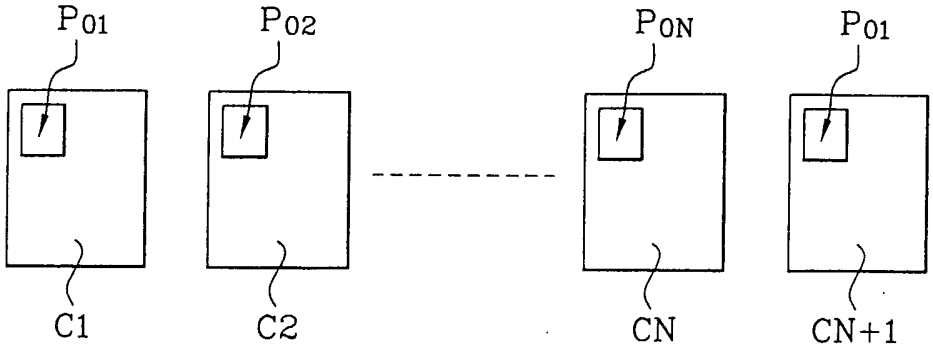

P01
P02
PON
P01
C1
C2
CN
CN+1

Fig. 6

INTERNATIONAL SEARCH REPORT

Internati pplication No
PCT/FR 03/01627

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 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 G07F G06F

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 559 884 A (R.L. DAVIDSON) 24 September 1996 (1996-09-24) abstract; claims; figures column 1, line 65 -column 2, line 25	1,5,7, 10,11
A	FR 2 809 847 A (GEMPLUS) 7 December 2001 (2001-12-07) abstract; claims; figures	1-3,5,6, 9-11

-/--

[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
21 October 2003	27/10/2003

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	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	COHEN F B: "OPERATING SYSTEM PROTECTION THROUGH PROGRAM EVOLUTION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 12, no. 6, 1 October 1993 (1993-10-01), pages 565-584, XP000415701 ISSN: 0167-4048 the whole document ---	1,5,9-11
A	WO 96 28795 A (SIEMENS) 19 September 1996 (1996-09-19) -----	

INTERNATIONAL SEARCH REPORT

Internati Application No
PCT/FR 03/01627

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5559884 A	24-09-1996	NONE	
FR 2809847 A	07-12-2001	FR 2809847 A1	07-12-2001
		AU 6402801 A	17-12-2001
		WO 0195271 A1	13-12-2001
WO 9628795 A	19-09-1996	DE 19508724 C1	31-10-1996
		AT 170647 T	15-09-1998
		CN 1176701 A	18-03-1998
		WO 9628795 A1	19-09-1996
		DE 59600517 D1	08-10-1998
		DK 813723 T3	07-06-1999
		EP 0813723 A1	29-12-1997
		ES 2120809 T3	01-11-1998
		NO 974055 A	10-11-1997

RAPPORT DE RECHERCHE INTERNATIONALE

Demand nationale No
PCT/FR 03/01627

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10 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 G07F G06F

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, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 5 559 884 A (R.L. DAVIDSON) 24 septembre 1996 (1996-09-24) abrégé; revendications; figures colonne 1, ligne 65 -colonne 2, ligne 25	1,5,7, 10,11
A	FR 2 809 847 A (GEMPLUS) 7 décembre 2001 (2001-12-07) abrégé; revendications; figures	1-3,5,6, 9-11

-/--

[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
21 octobre 2003	27/10/2003

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	David, J

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/01627

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	COHEN F B: "OPERATING SYSTEM PROTECTION THROUGH PROGRAM EVOLUTION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 12, no. 6, 1 octobre 1993 (1993-10-01), pages 565-584, XP000415701 ISSN: 0167-4048 le document en entier	1,5,9-11
A	WO 96 28795 A (SIEMENS) 19 septembre 1996 (1996-09-19)	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande nationale No
PCT/FR 03/01627

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 5559884	A	24-09-1996	AUCUN		
FR 2809847	A	07-12-2001	FR	2809847 A1	07-12-2001
			AU	6402801 A	17-12-2001
			WO	0195271 A1	13-12-2001
WO 9628795	A	19-09-1996	DE	19508724 C1	31-10-1996
			AT	170647 T	15-09-1998
			CN	1176701 A	18-03-1998
			WO	9628795 A1	19-09-1996
			DE	59600517 D1	08-10-1998
			DK	813723 T3	07-06-1999
			EP	0813723 A1	29-12-1997
			ES	2120809 T3	01-11-1998
			NO	974055 A	10-11-1997