(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
27 juin 2002 (27.06.2002)

PCT

(10) Numéro de publication internationale
WO 02/50658 A1

(51) Classification internationale des brevets[7] : G06F 7/72

(21) Numéro de la demande internationale :
PCT/FR01/04081

(22) Date de dépôt international :
19 décembre 2001 (19.12.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/16577 19 décembre 2000 (19.12.2000) FR

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

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **CORON, Jean-Sébastien** [FR/FR]; 4 rue Léon Delagrange, F-75015 PARIS (FR).

(74) Mandataire : **BRUYERE, Pierre**; C/O GEMPLUS, BP 100, F-13881 GEMENOS 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, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, 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, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, 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, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, 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, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, 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, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, 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: COUNTERMEASURE METHODS IN AN ELECTRONIC COMPONENT USING AN RSA-TYPE PUBLIC KEY ENCRYPTION ALGORITHM

(54) Titre : PROCEDES DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE RSA

(57) Abstract: The RSA encryption algorithm is the most used public key encryption algorithm. It has been observed that its use in the context of a smart card environment is vulnerable to differential power analysis (DPA) attacks. The invention concerns different countermeasure methods for protection against DPA-type attacks. Said countermeasures do not reduce the performance of the RSA algorithm and are of easy use in an electronic component such as a smart card.

(57) Abrégé : L'algorithme de chiffrement RSA est l'algorithme de chiffrement à clef publique le plus utilisé. Il est apparu que son application dans le cadre d'un environnement de type carte à puce était vulnérable à des attaques de type DPA (Differential Power Analysis). La présente invention consiste en la description de différents procédés de contre-mesure permettant de se prémunir contre ce type d'attaque DPA. Ces contre-mesures ne diminuent pas les performances de l'algorithme RSA et sont facilement utilisables dans un composant électronique de type carte à puce.

WO 02/50658 A1

— *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.

PROCEDES DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN ŒUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE RSA

La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en œuvre un algorithme de chiffrement à clé publique de type RSA.

Dans le modèle classique de la cryptographie à clef secrète, deux personnes désirant communiquer par l'intermédiaire d'un canal non sécurisé doivent au préalable se mettre d'accord sur une clé secrète de chiffrement K. La fonction de chiffrement et la fonction de déchiffrement utilisent la même clef K. L'inconvénient du système de chiffrement à clé secrète est que ledit système requiert la communication préalable de la clé K entre les deux personnes par l'intermédiaire d'un canal sécurisé, avant qu'un quelconque message chiffré ne soit envoyé à travers le canal non sécurisé. Dans la pratique, il est généralement difficile de trouver un canal de communication parfaitement sécurisé, surtout si la distance séparant les deux personnes est importante. On entend par canal sécurisé un canal pour lequel il est impossible de connaître ou de modifier les informations qui transitent par ledit canal. Un tel canal sécurisé peut être réalisé par un câble reliant deux terminaux, possédés par les deux dites personnes.

Le concept de cryptographie à clef publique fut inventé par Whitfield DIFFIE et Martin HELLMAN en 1976. La cryptographie à clef publique permet de résoudre le problème de la distribution des clefs à

travers un canal non sécurisé. Le principe de la cryptographie à clef publique consiste à utiliser une paire de clefs, une clef publique de chiffrement et une clef privée de déchiffrement. Il doit être calculatoirement infaisable de trouver la clef privée de déchiffrement à partir de la clef publique de chiffrement. Une personne A désirant communiquer une information à une personne B utilise la clef publique de chiffrement de la personne B. Seule la personne B possède la clef privée associée à sa clef publique. Seule la personne B est donc capable de déchiffrer le message qui lui est adressé.

Un autre avantage de la cryptographie à clé publique sur la cryptographie à clé secrète est que la cryptographie à clef publique permet l'authentification par l'utilisation de signature électronique.

La première réalisation de schéma de chiffrement à clef publique fut mise au point en 1977 par Rivest, Shamir et Adleman, qui ont inventé le système de chiffrement RSA. La sécurité de RSA repose sur la difficulté de factoriser un grand nombre qui est le produit de deux nombres premiers. Depuis, de nombreux systèmes de chiffrement à clef publique ont été proposés, dont la sécurité repose sur différents problèmes calculatoires : (cette liste n'est pas exhaustive).

- " Sac à dos " de Merckle-Hellman :
  ce système de chiffrement est basé sur la difficulté du problème de la somme de

sous-ensembles ;

- McEliece :
  ce système de chiffrement est basé sur la théorie des codes algébriques. Il est basé sur le problème du décodage de codes linéaires ;

- ElGamal :
  ce système de chiffrement est basé sur la difficulté du logarithme discret dans un corps fini ;

- Courbes elliptiques :
  le système de chiffrement à courbe elliptique constitue une modification de systèmes cryptographiques existant pour les appliquer au domaine des courbes elliptiques. L'avantage des systèmes de chiffrement à courbes elliptiques est qu'ils nécessitent une taille de clef plus petite que pour les autres systèmes de chiffrement.

Le système de chiffrement RSA est le système de chiffrement à clé publique le plus utilisé. Il peut être utilisé comme procédé de chiffrement ou comme procédé de signature. Le système de chiffrement RSA est utilisé dans les cartes à puce, pour certaines applications de celles-ci. Les applications possibles de RSA sur une carte à puce sont l'accès à des banques de données, des applications bancaires, des applications de paiements à distance comme par

exemple la télévision à péage, la distribution d'essence ou le paiement de péages d'autoroute.

Le principe du système de chiffrement RSA est le suivant. Il peut être divisé en trois parties distinctes qui sont :

1) La génération de la paire de clés RSA
2) Le chiffrement d'un message clair en un message chiffré, et
3) Le déchiffrement d'un message chiffré en un message clair.

La première partie est la génération de la clef RSA. Chaque utilisateur crée une clé publique RSA et une clé privée correspondante, suivant le procédé suivant en 5 étapes :

1) Générer deux nombres premiers distincts p et q de même taille
2) Calculer $n=pq$ et $\phi=(p-1)(q-1)$
3) Sélectionner aléatoirement un entier e, $1<e<\phi$, tel que $pgcd(e, \phi)=1$
4) Calculer l'unique entier d, $1<d<\phi$ tel que $e*d=1 \bmod \phi$
5) La clé publique est (n,e); la clé privée est d ou (d,p,q)

Les entiers e et d sont appelés respectivement exposant de chiffrement et exposant de déchiffrement. L'entier n est appelé le module.

La seconde partie de la génération à clé RSA consiste au chiffrement d'un message clair noté m au moyen d'un algorithme avec $1<m<n$ en un message

chiffré noté c est le suivant :

Calculer c=m^e mod n.

La troisième partie de la génération de la clé RSA consiste au déchiffrement utilisant l'exposant privé d de déchiffrement au moyen d'un algorithme. L'algorithme de déchiffrement d'un message chiffré noté c avec 1<c<n en un message clair noté m est le suivant :

Calculer m=c^d mod n.

L'algorithme de déchiffrement RSA précédemment décrit peut s'effectuer par deux méthodes différentes. Ces deux méthodes sont : déchiffrement avec CRT et déchiffrement sans CRT. CRT est un acronyme pour Chinese Remainder Theorem. L'avantage de l'algorithme de déchiffrement avec CRT est qu'il est théoriquement 4 fois plus rapide que l'algorithme de déchiffrement sans CRT.
L'algorithme de déchiffrement sans CRT consiste à calculer m=c^d mod n comme décrit précédemment.

L'algorithme de déchiffrement avec CRT consiste en les 4 étapes suivantes :

1) Calculer cp=c modulo p et cq=c modulo q
2) Calculer dp=d modulo p-1 et dq=d modulo q-1
3) Calculer mp=cp^dp modulo p et mq=cq^dq modulo q
4) Calculer m=mp*q*(q^(-1) mod p)+mq*p*(p^(-

1) mod q)

Pour réaliser les exponentiations modulaires nécessaires dans les procédés de calcul décrits précédemment, plusieurs algorithmes existent :

- Algorithme appelé " square and multiply ";
- Algorithme avec chaines d'addition;
- Algorithme avec fenêtre;
- Algorithme avec représentation signée.

Cette liste n'est pas exhaustive. L'algorithme le plus simple et le plus utilisé est l'algorithme " square and multiply ". L'algorithme " square and multiply " prend en entrée un nombre c, un exposant d et un module n. L'exposant d est noté d=(d(t), d(t-1), d(0)), où (d(t), d(t-1),, d(0)) étant la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. Par exemple la représentation du nombre cinq en binaire est 101, provenant du fait que 5=1*2^2+0*2^1+1*2^0. Le premier 1 est le bit de poids fort et le dernier 1 le bit de poids faible. L'algorithme retourne en sortie le nombre m=c^d mod n. L'algorithme " square and multiply " comporte les 3 étapes suivantes :

1) Initialiser une variable entière A avec la valeur c ;
2) Pour i allant de t-1 à 0 faire:
   2a) Remplacer A par A*A mod n ;
   2b) Si d(i)=1 remplacer A par A*c mod n ;
3) Retourner à l'étape 1 ci-dessus.

Dans le cas du déchiffrement RSA sans CRT, le déchiffrement s'effectue comme décrit précédemment en utilisant l'algorithme " square and multiply ". Dans ce cas, l'algorithme " square and multiply " prend donc en entrée le message chiffré c, le module n et l'exposant de déchiffrement d.

Dans le cas du déchiffrement RSA avec CRT, le déchiffrement s'effectue comme décrit précédemment en utilisant deux fois l'algorithme " square and multiply " pour l'exécution de l'étape 3) de l'algorithme de déchiffrement avec CRT. La première fois, l'algorithme prend en entrée l'entier cp, le module p et l'exposant dp. La deuxième fois, l'algorithme prend en entrée l'entier cq, le module q et l'exposant dq.

Il est possible d'effectuer ces opérations à l'intérieur d'une carte à puce, lesdites opérations étant effectuées par le microprocesseur de la carte à puce. Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé publique du type RSA était vulnérable à des attaques consistant en une analyse de la consommation de courant permettant de retrouver la clé privée de déchiffrement. Ces attaques sont appelées attaques SPA, acronyme pour Simple Power Analysis. Le principe de ces attaques SPA repose sur le fait que la consommation de courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

En particulier, lorsqu'une instruction manipule une donnée dont un bit particulier est constant, la valeur des autres bits pouvant varier, l'analyse de la consommation de courant liée à l'instruction montre que la consommation moyenne de l'instruction n'est pas la même suivant que le bit particulier prend la valeur 0 ou 1. L'attaque de type SPA permet donc d'obtenir des informations supplémentaires sur les données intermédiaires manipulées par le microprocesseur de la carte lors de l'exécution d'un algorithme cryptographique.Ces informations supplémentaires peuvent dans certain cas permettre de révéler les paramètres privés de l'algorithme de déchiffrement,rendant le système cryptographique non sûr.

L'inconvénient de la méthode « square and multiply » décrite précédemment est que les bits de l'exposant privé d sont manipulés un par un, dans un ordre déterminé. Il est ainsi possible dans certains cas d'obtenir la valeur de ces bits en examinant la consommation de courant associée à l'exécution de la méthode « square and multiply », car la manipulation d'un bit de l'exposant d valant 1 ne donne pas la même consommation de courant que la manipulation d'un bit de l'exposant d valant 0.

Le procédé de l'invention consiste en l'élaboration d'une contremesure permettant de prévenir une attaque par mesure de courant dans laquelle l'attaquant est en mesure de lire les bits manipulés par le processeur réalisant l'opération d'exponentiation. Le procédé de l'invention consiste

à manipuler les bits de l'exposant d dans un ordre aléatoire, inconnu de l'attaquant, de telle sorte que même si l'attaquant est en mesure retrouver la valeur de ces bits, il ne peut pas déterminer l'exposant d correspondant.

Le procédé de l'invention consiste en une méthode permettant de réaliser l'exponentiation c=m^d modulo N, où m est un entier, N le module, d est l'exposant, et c le résultat de l'exponentiation.

Le procédé de l'invention divise l'exposant en blocks de k bits, chacun des blocks étant divisé en sous-blocks de r bits. On note t le nombre de bits de l'exposant. On suppose que t est un multiple de l'entier k. Si ce n'est pas le cas, on augmente en conséquence le nombre de bits de l'exposant d. On suppose de plus que la taille d'un block k est un multiple de la taille d'un sous-block de r bits. On note u l'entier tel que k=u*r.

On divise l'exposant d en L blocks de k bits, et on note :

d=bd[L-1].bd[L-2]…bd[1].bd[0].

Chacun des blocks bd est divisé en sous blocks de r bits, et on note :

bd[i]=sd[i,u-1]…sd[i,0]

Le procédé de l'invention comporte les étapes suivantes :

1) Calculer et mettre en mémoire dans un

tableau d'entiers a[i] la valeur de m^(2^(r*i)) modulo N pour les entiers i allant de 0 à u-1 ;

2) Initialiser la variable c à 1 ;

3) Pour l'entier i variant entre 0 et L-1, on effectue :

3)1) Initialiser un ensemble d'entiers S à l'ensemble vide.

3)2) Tirer aléatoirement un entier j compris entre 0 et u-1, qui n'appartient pas à l'ensemble S ;

3)3) Calculer le résultat de l'exponentiation modulo N de a[j] avec l'exposant sd[i,j] ; cette exponentiation peut se réaliser par exemple à l'aide de la méthode « square and multiply » ; mettre le résultat en mémoire dans le tableau d'entiers b[j] ;

3)4) Ajouter l'élément j à l'ensemble S ;

3)5) Retourner à l'étape 3)2) tant que l'ensemble S ne comprend pas tous les entiers entre 0 et u-1 ;

3)6) Effectuer le produit modulo N de tous les éléments b[j] pour j variant de 0 à u-1 ; mettre le résultat dans la variable entière a ;

3)7) Effectuer le calcul a*c^(2^k) et mettre le résultat dans c ;

4) Renvoyer le résultat c.

Le procédé de la contre-mesure peut s'appliquer à tout procédé utilisant une exponentiation

modulaire, que ce soit pour réaliser un procédé de chiffrement, un procédé de signature, un procédé d'authentification, un procédé d'échange de clef. Le procédé de la contre-mesure peut aussi s'appliquer dans le cadre de l'utilisation de méthode à base de courbe elliptique.

L'application du procédé de contre-mesure précédent permet de protéger l'algorithme d'exponentiation contre les attaques par mesure de courant. Le principe du procédé consiste à rendre aléatoire la lecture de l'exposant utilisé dans l'exponentiation. L'invention est particulièrement destinée à être utilisée dans un objet portable électronique de type carte à puce.

REVENDICATIONS

1. Procédé de contre-mesure consistant à prévenir une attaque par mesure de courant en réalisant le calcul d'exponentiation de formulation c=m^d modulo N, m étant un entier, N étant le module, d étant l'exposant, c étant le résultat de ladite exponentiation, ledit procédé divisant l'exposant en blocks de k bits, chacun des blocks étant divisé en sous-blocks de r bits, le nombre de bits de l'exposant étant un multiple de k, la taille d'un block k étant telle que k=u*r pour un entier u donné, l'exposant d étant divisé en L blocks de k bits, d étant représenté par d=bd[L-1].bd[L-2]…bd[1].bd[0], chacun des blocks bd étant divisé en sous-blocks de r bits, un block bd étant noté bd[i]=sd[i,u-1]…sd[i,0], ledit procédé étant caractérisé en ce qu'il comprend les étapes suivantes :

1) Calculer et mettre en mémoire dans un tableau d'entiers a[i] la valeur de m^(2^(r*i)) modulo N pour les entiers i allant de 0 à u-1 ;
2) Initialiser la variable c à 1 ;
3) Pour l'entier i variant entre 0 et L-1, on effectue :
   3)1) Initialiser un ensemble d'entiers S à l'ensemble vide ;
   3)2) Tirer aléatoirement un entier j compris entre 0 et u-1, qui n'appartient pas à l'ensemble S ;
   3)3) Calculer le résultat de l'exponentiation modulo N de a[j] avec l'exposant sd[i,j] et mettre le résultat

en mémoire dans le tableau d'entiers b[j] ;

3)4) Ajouter l'élément j à l'ensemble S ;

3)5) Retourner à l'étape 3)2) tant que l'ensemble S ne comprend pas tous les entiers entre 0 et u-1 ;

3)6) Effectuer le produit modulo N de tous les éléments b[j] pour j variant de 0 à u-1 ; mettre le résultat dans la variable entière a ;

3)7) Effectuer le calcul a*c^(2^k) et mettre le résultat dans c ;

4) Renvoyer le résultat c.

2. Procédé de contre-mesure consistant à prévenir une attaque par mesure de courant selon la revendication 1, caractérisé en ce que l'exponentiation réalisée à l'étape 3)3) comporte les 3 étapes suivantes :

1) Initialiser une variable entière at avec la valeur a[j] ;

2) Pour it allant de r-1 à 0 faire:

2a) Remplacer at par at*at modulo N ;

2b) Si sd[i,it]=1 remplacer at par at*a[j] modulo N;

3) Renvoyer le résultat at.

3. Procédé de contre-mesure selon la revendication 1 ou 2, caractérisé en ce qu'il s'applique à une méthode de chiffrement.

4. Procédé de contre-mesure selon la revendication 1

ou 2, caractérisé en ce qu'il s'applique à une méthode de signature électronique.

5. Procédé de contre-mesure selon la revendication 1 ou 2, caractérisé en ce qu'il s'applique à une méthode d'échange de clefs.

6. Procédé de contre-mesure selon la revendication 1 ou 2, caractérisé en ce qu'il s'applique à une méthode d'authentification.

7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le procédé utilise la méthode des courbes elliptiques.

8. Composant électronique utilisant le procédé selon l'une quelconque des revendications précédentes caractérisé en ce qu'il peut être une carte à puce.

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/FR 01/04081

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

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

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, INSPEC, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 00 67410 A (MOTOROLA INC) 9 November 2000 (2000-11-09) abstract; figure 3	1-8
Y	US 5 999 627 A (LEE PIL-JOONG ET AL) 7 December 1999 (1999-12-07) column 3, line 46 - line 67 column 5, line 41 -column 6, line 52; figure 3	1-8

☐ Further documents are listed in the continuation of box C.

☒ 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
15 April 2002	23/04/2002

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	Verhoof, P

INTERNATIONAL SEARCH REPORT

mation on patent family members

Ir al Application No
PCT/FR 01/04081

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0067410 A	09-11-2000	US 6298135 B1	02-10-2001
		AU 4673900 A	17-11-2000
		WO 0067410 A1	09-11-2000
US 5999627 A	07-12-1999	KR 138277 B1	01-07-1998
		JP 8202263 A	09-08-1996

RAPPORT DE RECHERCHE INTERNATIONALE

De le Internationale No
PCT/FR 01/04081

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F7/72

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

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, INSPEC, PAJ, 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
Y	WO 00 67410 A (MOTOROLA INC) 9 novembre 2000 (2000-11-09) abrégé; figure 3	1-8
Y	US 5 999 627 A (LEE PIL-JOONG ET AL) 7 décembre 1999 (1999-12-07) colonne 3, ligne 46 - ligne 67 colonne 5, ligne 41 -colonne 6, ligne 52; figure 3	1-8

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ 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'appartenant 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
15 avril 2002	23/04/2002

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	Verhoof, P

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

De la demande internationale No
PCT/FR 01/04081

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0067410	A	09-11-2000	US	6298135 B1	02-10-2001
			AU	4673900 A	17-11-2000
			WO	0067410 A1	09-11-2000
US 5999627	A	07-12-1999	KR	138277 B1	01-07-1998
			JP	8202263 A	09-08-1996