(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
9 octobre 2003 (09.10.2003)

PCT

(10) Numéro de publication internationale
WO 2003/083645 A3

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

(21) Numéro de la demande internationale :
PCT/FR2003/001058

(22) Date de dépôt international : 3 avril 2003 (03.04.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/04117 3 avril 2002 (03.04.2002) 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) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **JOYE, Marc** [BE/FR]; 19, rue Voltaire, F-83640 Saint Zacharie (FR). **CHEVALLIER-MAMES, Benoît** [FR/FR]; Résidence Le Général, 14, boulevard Ganteaume, F-13400 Aubagne (FR).

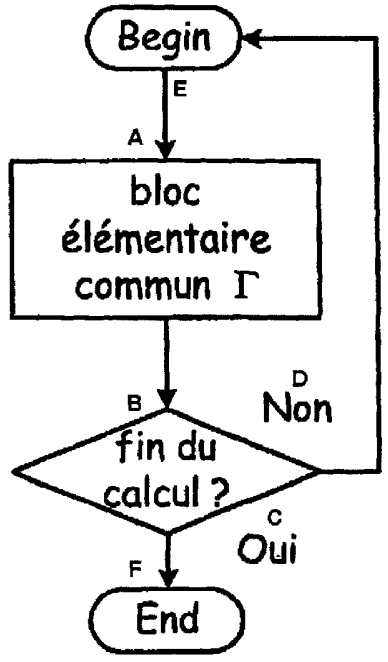
(74) Mandataire : **BRUN, Philippe**; c/o Gemplus, Service brevets, La Vigie, PB 90, F-13705 La Ciotat Cedex (FR).

(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.

[Suite sur la page suivante]

(54) **Title:** CRYPTOGRAPHIC METHOD PROTECTED AGAINST COVERT CHANNEL TYPE ATTACKS

(54) **Titre :** PROCEDE CRYPTOGRAPHIQUE PROTEGE CONTRE LES ATTAQUES DE TYPE A CANAL CACHE



A...BLOC ÉLÉMENTAIRE COMMUN:- COMMON ELEMENTARY BLOCK
B...FIN DE CALCUL?:- END OF CALCULATION?
C...OUI:- YES
D...NON:- NO
E...DEBUT
F...FIN

(57) **Abstract:** The invention relates to a cryptographic method secured against a covert channel attack. According to the invention, in order to carry out a selected block of instructions (?j) as a function of an input variable (D_1) amongst N predefined instruction blocks ($?_1$,, $?_N$), a common block (Γ (k,s)) is carried out on the predefined N instruction blocks ($?_1$,, $?_N$), a predefined number (L_j) of times, the predefined number (L_j) being associated with the selected instruction block ($?_j$).

(57) **Abrégé :** L'invention concerne un procédé cryptographique sécurisé contre une attaque à canal caché. Selon l'invention, pour exécuter un bloc d'instructions choisi (Πj) en fonction d'une variable d'entrée (D_1) parmi N blocs d'instructions prédéfinis (Π_1, , Π_N), on exécute un nombre prédéfini (L_j) de fois un bloc commun ((k,s)) aux N blocs d'instructions prédéfinis (Π_1, , Π_N), le nombre prédéfini (L_j) étant associé au bloc d'instructions choisi (Π_j).

WO 2003/083645 A3

(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).

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*

(88) Date de publication du rapport de recherche internationale: 1 avril 2004

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.

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR 03/01058

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, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MOELLER ET AL: "SECURING ELLIPTIC CURVE POINT MULTIPLICATION AGAINST SIDE-CHANNEL ATTACKS" INFORMATION SECURITY. 4TH INTERNATIONAL CONFERENCE, ISC 2001 MALAGA, SPAIN, OCTOBER 1-3, 2001, PROCEEDINGS, 1 October 2001 (2001-10-01), pages 324-334, XP001068194 Springer Verlag, Berlin DE * Algorithme 1 * page 10, paragraph 1 --- -/--	1,3,7-9, 15

[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
7 October 2003	23/10/2003

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	Verhoof, P

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/01058

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	OSWALD E ET AL: "RANDOMIZED ADDITION-SUBTRACTION CHAINS AS A COUNTERMEASURE AGAINST POWER ATTACKS" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. 3RD INTERNATIONAL WORKSHOP, CHES 2001, PARIS, FRANCCE, MAY 14 - 16, 2001 PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE, BERLIN: SPRINGER, DE, vol. 2162, 14 May 2001 (2001-05-14), pages 39-50, XP001061159 ISBN: 3-540-42521-7 * page 40, algorithme binalg(P,M,k) ; page 42, algorithme binalg'(P,M,k) * ---	1,3,7-9, 15
X	WO 00 25204 A (CERTICOM CORP ;GALLANT ROBERT P (CA); VANSTONE SCOTT A (CA)) 4 May 2000 (2000-05-04) figures 1,2 ---	1,3,7-9, 15
A	EP 1 158 384 A (INFINEON TECHNOLOGIES AG) 28 November 2001 (2001-11-28) paragraph '0030! - paragraph '0031! ---	3
X,P	WO 02 099624 A (JOYE MARC ;GEMPLUS CARD INT (FR)) 12 December 2002 (2002-12-12) claims page 10, line 25 -page 17, line 22 -----	1,3,4, 6-9,15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 03/01058

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0025204 A	04-05-2000	AU 5964299 A	15-05-2000
		WO 0025204 A1	04-05-2000
		EP 1044405 A1	18-10-2000
		JP 2002528771 T	03-09-2002
EP 1158384 A	28-11-2001	EP 1158384 A1	28-11-2001
		WO 0190854 A1	29-11-2001
		US 2003110390 A1	12-06-2003
WO 02099624 A	12-12-2002	FR 2825863 A1	13-12-2002
		WO 02099624 A1	12-12-2002

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/01058

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, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	MOELLER ET AL: "SECURING ELLIPTIC CURVE POINT MULTIPLICATION AGAINST SIDE-CHANNEL ATTACKS" INFORMATION SECURITY. 4TH INTERNATIONAL CONFERENCE, ISC 2001 MALAGA, SPAIN, OCTOBER 1-3, 2001, PROCEEDINGS, 1 octobre 2001 (2001-10-01), pages 324-334, XP001068194 Springer Verlag, Berlin DE * Algorithme 1 * page 10, alinéa 1 --- -/--	1,3,7-9, 15

[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'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention 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
7 octobre 2003	23/10/2003

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	Verhoof, P

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 03/01058

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
X	OSWALD E ET AL: "RANDOMIZED ADDITION-SUBTRACTION CHAINS AS A COUNTERMEASURE AGAINST POWER ATTACKS" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. 3RD INTERNATIONAL WORKSHOP, CHES 2001, PARIS, FRANCCE, MAY 14 - 16, 2001 PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE, BERLIN: SPRINGER, DE, vol. 2162, 14 mai 2001 (2001-05-14), pages 39-50, XP001061159 ISBN: 3-540-42521-7 * page 40, algorithme binalg(P,M,k) ; page 42, algorithme binalg'(P,M,k) *	1,3,7-9, 15
X	WO 00 25204 A (CERTICOM CORP ;GALLANT ROBERT P (CA); VANSTONE SCOTT A (CA)) 4 mai 2000 (2000-05-04) figures 1,2	1,3,7-9, 15
A	EP 1 158 384 A (INFINEON TECHNOLOGIES AG) 28 novembre 2001 (2001-11-28) alinéa '0030! - alinéa '0031!	3
X,P	WO 02 099624 A (JOYE MARC ;GEMPLUS CARD INT (FR)) 12 décembre 2002 (2002-12-12) revendications page 10, ligne 25 -page 17, ligne 22	1,3,4, 6-9,15

Demande internationale n°
PCT/FR 03/01058

RAPPORT DE RECHERCHE INTERNATIONALE

Cadre I Observations – lorsqu'il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (suite du point 1 de la première feuille)

Conformément à l'article 17.2)a), certaines revendications n'ont pas fait l'objet d'une recherche pour les motifs suivants:

1. [X] Les revendications n^{os} 19,20
se rapportent à un objet à l'égard duquel l'administration n'est pas tenue de procéder à la recherche, à savoir:

voir feuille supplémentaire SUITE DES RENSEIGNEMENTS PCT/ISA/210

2. [ ] Les revendications n^{os}
se rapportent à des parties de la demande internationale qui ne remplissent pas suffisamment les conditions prescrites pour qu'une recherche significative puisse être effectuée, en particulier:

3. [ ] Les revendications n^{os}
sont des revendications dépendantes et ne sont pas rédigées conformément aux dispositions de la deuxième et de la troisième phrases de la règle 6.4.a).

Cadre II Observations – lorsqu'il y a absence d'unité de l'invention (suite du point 2 de la première feuille)

L'administration chargée de la recherche internationale a trouvé plusieurs inventions dans la demande internationale, à savoir:

1. [ ] Comme toutes les taxes additionnelles ont été payées dans les délais par le déposant, le présent rapport de recherche internationale porte sur toutes les revendications pouvant faire l'objet d'une recherche.

2. [ ] Comme toutes les recherches portant sur les revendications qui s'y prêtaient ont pu être effectuées sans effort particulier justifiant une taxe additionnelle, l'administration n'a sollicité le paiement d'aucune taxe de cette nature.

3. [ ] Comme une partie seulement des taxes additionnelles demandées a été payée dans les délais par le déposant, le présent rapport de recherche internationale ne porte que sur les revendications pour lesquelles les taxes ont été payées, à savoir les revendications n ^{os}

4. [ ] Aucune taxe additionnelle demandée n'a été payée dans les délais par le déposant. En conséquence, le présent rapport de recherche internationale ne porte que sur l'invention mentionnée en premier lieu dans les revendications; elle est couverte par les revendications n ^{os}

Remarque quant à la réserve

[ ] Les taxes additionnelles étaient accompagnées d'une réserve de la part du déposant.

[ ] Le paiement des taxes additionnelles n'était assorti d'aucune réserve.

Suite du cadre I.1

Revendications nos.: 19,20

Règle 39.1(iii) PCT - Plan, principe et méthode dans l'exercice d'activités intellectuelles. Bien que l'activité intellectuelle (activité de programmation) de la revendication indépendante 19 puisse éventuellement être effectuée par un ordinateur, ceci n'est ni divulgé de manière explicite, ni de manière implicite.

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR 03/01058

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0025204	A	04-05-2000	AU	5964299 A	15-05-2000
			WO	0025204 A1	04-05-2000
			EP	1044405 A1	18-10-2000
			JP	2002528771 T	03-09-2002
EP 1158384	A	28-11-2001	EP	1158384 A1	28-11-2001
			WO	0190854 A1	29-11-2001
			US	2003110390 A1	12-06-2003
WO 02099624	A	12-12-2002	FR	2825863 A1	13-12-2002
			WO	02099624 A1	12-12-2002