(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
19 février 2004 (19.02.2004)

PCT

(10) Numéro de publication internationale
WO 2004/015559 A3

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

(21) Numéro de la demande internationale :
PCT/FR2003/050022

(22) Date de dépôt international : 29 juillet 2003 (29.07.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/09942 5 août 2002 (05.08.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **EVERBEE NETWORKS** [FR/FR]; 41, boulevard des Capucines, F-75002 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **STEHLE, Jean-Luc** [FR/FR]; 300, rue de Vaugirard, F-75015 Paris (FR).

(74) Mandataire : **GRYNWALD, Albert**; Cabinet Grynwald, 127, rue du Faubourg Poissonnière, F-75009 Paris (FR).

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

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :
— *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: 13 mai 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.

(54) **Title:** METHOD FOR ACCELERATING CALCULATIONS IN MODULAR ARITHMETIC

(54) **Titre :** PROCEDE POUR ACCELERER DES CALCULS EN ARITHMETIQUE MODULAIRE

(57) **Abstract:** The invention a method for accelerating exponentiation calculations in arithmetic modulo, a number N stored on q words. The exponentiations are especially involved in cryptography protocols implemented by means of computer resources. According to said method, a first algorithm is suitable for replacing an argument, stored on 2q words, by a result which is congruent modulo N to said argument and the q low-order words of which are null and a first operator takes two entries each stored on q words and outputs a number W, stored on q words, the product by R of which is congruent modulo N to the product of both entries, whereby R is a power of two higher than N. Said method allows computation power and memory space to be saved.

(57) **Abrégé :** L'invention concerne un procédé permettant d'accélérer les calculs d'exponentiation en arithmétique modulo un nombre N stocké sur q mots. Les exponentiations interviennent notamment dans des protocoles de cryptographie mis en œuvre à l'aide de ressources informatiques. Le procédé comporte : un premier algorithme ayant pour objet de remplacer un argument, stocké sur 2q mots, par un résultat qui est congru modulo N audit argument et dont les q mots de poids faibles sont nuls, un premier opérateur prenant deux entrées stockées chacune sur q mots et fournissant en sortie un nombre W, stocké sur q mots, dont le produit par R est congru modulo N au produit des deux entrées. R est une puissance de deux supérieure à N. Le procédé permet d'économiser de la puissance de calcul et de l'espace mémoire.

WO 2004/015559 A3

INTERNATIONAL SEARCH REPORT

Interna Application No
PCT/FR 03/50022

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, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DUSSE S R ET AL: "A CRYPTOGRAPHIC LIBRARY FOR THE MOTOROLA DSP56000" LECTURE NOTES IN COMPUTER SCIENCE. ADVANCES IN CRYPTOLOGY- EUROCRYPT '90, 21-24 MAY 1990, AARHUS, DK, 1991, pages 230-244, XP000471664 Springer Verlag, BERLIN, DE page 2342, line 13 -page 234, line 19 --- -/--	1,3,4, 6-8,10, 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
6 February 2004	16/02/2004

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

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

INTERNATIONAL SEARCH REPORT

Interna pplication No
PCT/FR 03/50022

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	ARAZI B: "DOUBLE-PRECISION MODULAR MULTIPLICATION BASED ON A SINGLE-PRECISIONMODULAR MULTIPLIER AND A STANDARD CPU" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE INC. NEW YORK, US, vol. 11, no. 5, 1 June 1993 (1993-06-01), pages 761-769, XP000399844 ISSN: 0733-8716 * paragraphe IV.C * page 767 ---	1,3,4, 6-8,10, 11
A	US 5 499 299 A (TAKENAKA MASAHIKO ET AL) 12 March 1996 (1996-03-12) column 7, line 39 - line 41; figure 1 ---	1,7
A	EP 0 939 362 A (ST MICROELECTRONICS SA) 1 September 1999 (1999-09-01) claim 1 -----	4,5,11, 12

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna Application No
PCT/FR 03/50022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5499299 A	12-03-1996	JP 7020778 A	24-01-1995
EP 0939362 A	01-09-1999	FR 2775368 A1	27-08-1999
		DE 69900306 D1	31-10-2001
		DE 69900306 T2	04-07-2002
		EP 0939362 A1	01-09-1999
		US 6341299 B1	22-01-2002

RAPPORT DE RECHERCHE INTERNATIONALE

Demar nationale No
PCT/FR 03/50022

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, 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	DUSSE S R ET AL: "A CRYPTOGRAPHIC LIBRARY FOR THE MOTOROLA DSP56000" LECTURE NOTES IN COMPUTER SCIENCE. ADVANCES IN CRYPTOLOGY- EUROCRYPT '90, 21-24 MAY 1990, AARHUS, DK, 1991, pages 230-244, XP000471664 Springer Verlag, BERLIN, DE page 2342, ligne 13 -page 234, ligne 19 --- -/--	1,3,4, 6-8,10, 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
6 février 2004	16/02/2004

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

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

RAPPORT DE RECHERCHE INTERNATIONALE

Deman nationale No
PCT/FR 03/50022

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	ARAZI B: "DOUBLE-PRECISION MODULAR MULTIPLICATION BASED ON A SINGLE-PRECISIONMODULAR MULTIPLIER AND A STANDARD CPU" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE INC. NEW YORK, US, vol. 11, no. 5, 1 juin 1993 (1993-06-01), pages 761-769, XP000399844 ISSN: 0733-8716 * paragraphe IV.C * page 767 ---	1,3,4, 6-8,10, 11
A	US 5 499 299 A (TAKENAKA MASAHIKO ET AL) 12 mars 1996 (1996-03-12) colonne 7, ligne 39 - ligne 41; figure 1 ---	1,7
A	EP 0 939 362 A (ST MICROELECTRONICS SA) 1 septembre 1999 (1999-09-01) revendication 1 -----	4,5,11, 12

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande nationale No
PCT/FR 03/50022

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5499299 A	12-03-1996	JP 7020778 A	24-01-1995
EP 0939362 A	01-09-1999	FR 2775368 A1	27-08-1999
		DE 69900306 D1	31-10-2001
		DE 69900306 T2	04-07-2002
		EP 0939362 A1	01-09-1999
		US 6341299 B1	22-01-2002