

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
16 March 2006 (16.03.2006)

PCT

(10) International Publication Number
WO 2006/029152 A3

(51) International Patent Classification:
G06F 7/52 (2006.01)

(21) International Application Number:
PCT/US2005/031709

(22) International Filing Date:
1 September 2005 (01.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/609,211 10 September 2004 (10.09.2004) US
11/044,648 27 January 2005 (27.01.2005) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier applications:
US 11/044,648 (CON)
Filed on 27 January 2005 (27.01.2005)
US 60/609,211 (CON)
Filed on 10 September 2004 (10.09.2004)

(71) Applicant (for all designated States except US): **CAVIUM NETWORKS** [US/US]; 2610 Augustine Drive, Santa Clara, California 95054 (US).

(72) Inventor; and

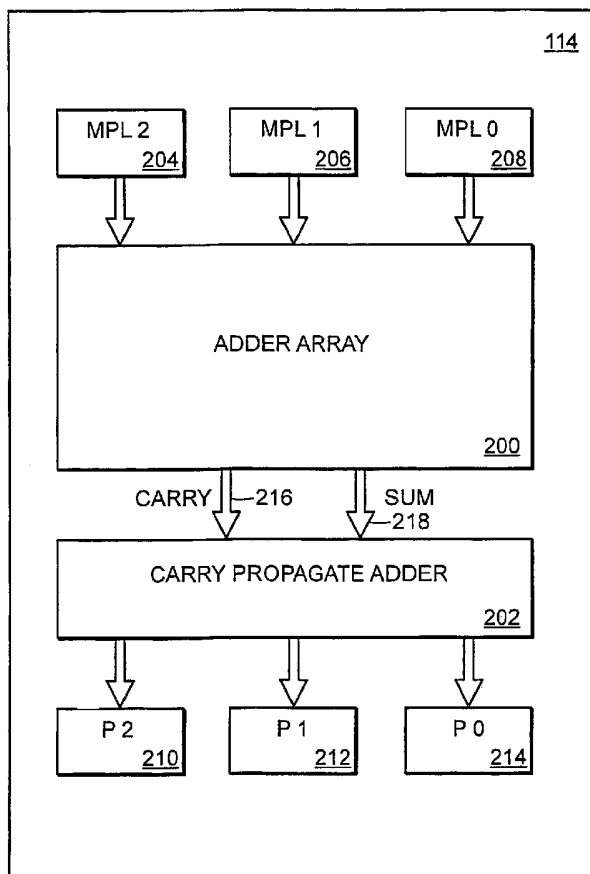
(75) Inventor/Applicant (for US only): **CARLSON, David, A.** [US/US]; 13909 Bates Aston Road, Haslet, Texas 76052 (US).

(74) Agents: **MEAGHER, Timothy, J.** et al.; HAMILTON, BROOK, SMITH & REYNOLDS, P.C., 530 Virginia Road, P.O. Box 9133, Concord, MA 01742-9133 (US).

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

[Continued on next page]

(54) Title: MULTIPLY INSTRUCTIONS FOR MODULAR EXPONENTIATION



(57) Abstract: A method and apparatus for increasing performance of a multiplication operation in a processor. The processor's instruction set includes multiply instructions that can be used to accelerate modular exponentiation. Prior to issuing a sequence of multiply instructions for the multiplication operation, a multiplier register in a multiply unit in the processor is loaded with the value of the multiplier. The multiply unit stores intermediate results of the multiplication operation in redundant format. The intermediate results are shifted and stored in the product register in the multiply unit so that carries between intermediate results are handled within the multiply unit.

WO 2006/029152 A3



(84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

(88) **Date of publication of the international search report:**

14 September 2006

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2005/031709

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F7/52

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)
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, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 121 431 A (WIENER ET AL) 9 June 1992 (1992-06-09) column 10; figure 2 column 2, line 53 - line 56 column 7, line 9 - line 17 column 7, line 60 - column 8, line 6 column 1, line 58 -----	1,2,5-8, 10,11, 14-17,19
X	US 6 484 194 B1 (HENDERSON ALVA ET AL) 19 November 2002 (2002-11-19) figures 1-5 column 2, line 44 - line 53 column 3, line 1 - line 18 column 5, line 24 - line 60 column 6, line 29 - line 67 ----- -/--	1,5-8, 10, 14-17,19

☒ Further documents are listed in the continuation of Box C.

☒ See patent family 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

5 April 2006

Date of mailing of the international search report

17. 07. 2006

Name and mailing address of the ISA/

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

Authorized officer

Pfab, S

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2005/031709

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 890 899 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD) 13 January 1999 (1999-01-13) abstract; figures 2-6,12 -----	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2005/031709

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1,2,5,6,7,8,10,11,14,15,16,17,19

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1,2,5,6,7,8,10,11,14,15,16,17,19

multiply instructions for modular exponentiation

2. claims: 3,12

clear product register when loading multiplier register

3. claims: 4,13

performing an add operation by storing a value of 1 in the multiplier register

4. claims: 9,18

result is stored in redundant format

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2005/031709

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5121431	A	09-06-1992	CA 2045385 A1	03-01-1992
US 6484194	B1	19-11-2002	NONE	
EP 0890899	A	13-01-1999	CN 1215862 A	05-05-1999
			DE 69821408 D1	11-03-2004
			DE 69821408 T2	16-12-2004
			TW 436729 B	28-05-2001
			US 6233597 B1	15-05-2001