

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
3 January 2003 (03.01.2003)

PCT

(10) International Publication Number
WO 2003/001362 A3

(51) International Patent Classification⁷: **G06F 7/72**
(21) International Application Number:
PCT/IL2002/000318
(22) International Filing Date: 22 April 2002 (22.04.2002)
(25) Filing Language: English
(26) Publication Language: English
(30) Priority Data:
143951 21 June 2001 (21.06.2001) IL
(71) Applicant (for all designated States except US): **DIS-
CRETIX TECHNOLOGIES LTD.** [IL/IL]; Hamelacha
Street 43, Beit Etgarim, Poleg Industrial Zone, 42502
Netanya (IL).

(81) Designated States (*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) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,
GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR,
NE, SN, TD, TG).

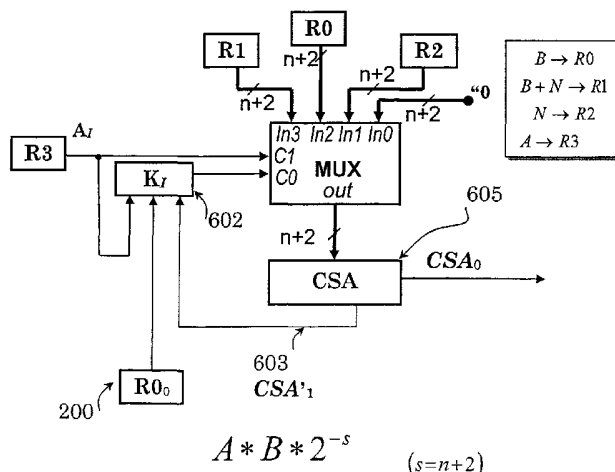
Published:

— with international search report

(88) Date of publication of the international search report:
4 March 2004

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

(54) Title: A METHOD AND APPARATUS FOR CARRYING OUT EFFICIENTLY ARITHMETIC COMPUTATIONS IN
HARDWARE



(57) Abstract: A method for carrying out modular arithmetic computations involving multiplication operations by utilizing a non-reduced and extended Montgomery multiplication between a first A and a second B integer values, in which the number of iterations required is greater than the number of bits n of an odd modulo value N. The method comprises storing n+2 bit values in an accumulating device (S) capable of, of adding n+2-bit values (X) to its content, and of dividing its content by 2. Whenever desired, the content of the accumulating device is set to zero value. At least s(>n+1) iterations of the following steps are performed, while in each iteration choosing one bit, in sequence, from the value of said first integer value A, starting from its least significant bit: adding to the content of the accumulating device S the product of the selected bit and said second integer value B; adding to the resulting content the product of its current least significant bit and N; dividing the result by 2; and obtaining a non-reduced and extended Montgomery multiplication result by repeating these steps s-1 additional times while in each time using the previous result (S).

WO 2003/001362 A3

INTERNATIONAL SEARCH REPORT

Int **nal** Application No
PCT/IL 02/00318

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)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BLUM T ET AL: "Montgomery modular exponentiation on reconfigurable hardware" COMPUTER ARITHMETIC, 1999. PROCEEDINGS. 14TH IEEE SYMPOSIUM ON ADELAIDE, SA, AUSTRALIA 14-16 APRIL 1999, LOS ALAMITOS, CA, USA, IEEE COMPUT. SOC, US, 14 April 1999 (1999-04-14), pages 70-77, XP010332298	1-13, 16-23
Y	ISBN: 0-7695-0116-8 paragraph '03.2! paragraph '0004! --- -/--	14,15
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input type="checkbox"/> 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. *8* document member of the same patent family		
Date of the actual completion of the international search 24 January 2003		Date of mailing of the international search report 20/02/2003
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 Cohen, B

INTERNATIONAL SEARCH REPORT

Int. Patent Application No
PCT/IL 02/00318

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	<p>ARAZI B: "DOUBLE-PRECISION MODULAR MULTIPLICATION BASED ON A SINGLE-PRECISIONMODULAR MULTIPLIER AND A STANDARD CPU"</p> <p>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</p> <p>ISSN: 0733-8716</p> <p>paragraph 'OI.C!</p> <p>paragraph 'IV.B!</p> <p>paragraph 'IV.D!</p> <p>-----</p>	14
Y		15