(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 May 2008 (15.05.2008)

PCT

(10) International Publication Number
WO 2008/057804 A3

(51) International Patent Classification:
G06F 7/44 (2006.01)

(21) International Application Number:
PCT/US2007/082713

(22) International Filing Date: 26 October 2007 (26.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/556,894 6 November 2006 (06.11.2006) US

(71) Applicant *(for all designated States except US)*: **ATMEL CORPORATION** [US/US]; 2325 Orchard Parkway, San Jose, CA 95131 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DOUGUET, Michel** [FR/FR]; 152 Avenue de Mazargues, F-13008 Marseille (FR). **DUPAQUIS, Vincent** [FR/FR]; 22 Residence Victor Savine, F-13120 Biver (FR).

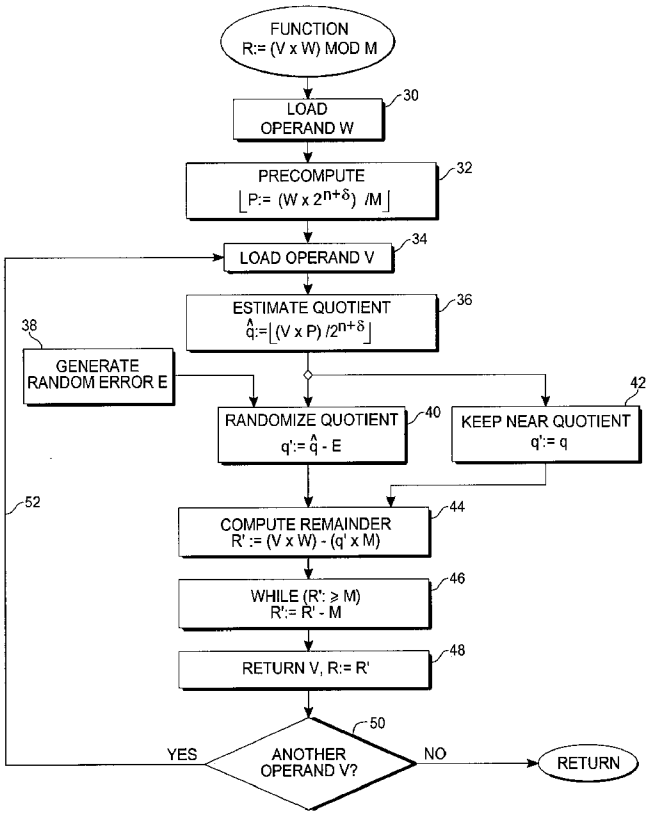
(74) Agents: **STEFFEY, Charles, E.** et al.; Schwegman, Lundberg & Woessner, P.A., P.O. Box 2938, Minneapolis, MN 55402 (US).

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

(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, MT, 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).

[Continued on next page]

(54) Title: MODULAR MULTIPLICATION METHOD WITH PRECOMPUTATION USING ONE KNOWN OPERAND



(57) Abstract: A modular multiplication method implemented in an electronic digital processing system takes advantage of the case where one of the operands W is known in advance or used multiple times with different second operands V to speed calculation. The operands V and W and the modulus M may be integers or polynomials over a variable X. A possible choice for the type of polynomials can be polynomials of the binary finite field GF (2^N). Once operand W is loaded (30; 60) into a data storage (12) location, a value $P = Lw\text{-}X^{n+\delta}/M$ J is pre- computed (32; 62) by the processing system (10). Then when a second operand V is loaded (34; 64), the quotient $\hat{q}$ for the product V.W being reduced modulo M is quickly estimated (36; 66), $\hat{q} = Lv\text{-}P/X^{n+\delta}J$, optionally randomized (40; 70), $q' = \hat{q} - E$, and can be used to obtain (44; 74) the remainder r' = V.W - q'-M, which is congruent to (V.W) mod M. A final reduction (46; 76) can be carried out, and the later steps repeated (52; 82) with other second operands V.

WO 2008/057804 A3

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report*

(88) Date of publication of the international search report:
31 July 2008

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 07/82713

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 7/44 (2008.04)
USPC - 708/503
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)
USPC - 708/503

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 708/100, 130, 490, 503, 620; 700/1, 90

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
USPTO WEST(USPAT, USPUB, EPO, JPO, DERWENT); Google Scholar
Search Terms Used: modular and multiplication and hardware and accessible and data and storage and computing and computations etc.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2005/0149595 A1 (Fischer et al.) 07 July 2005 (07.07.2005), para [0014]-[0015], [0022],[0037],[0009].	1-16
Y	US 2006/0061795 A1 (Walmsley) 23 March 2006 (23.03.2006), para [0526],[0554],[0559],[0560], [0621],[0653],[0664], [1690],[3232].	1-16
A	US 2004/0066934 A1 (Chen) 08 April 2004 (08.04.2004), entire document.	1-16

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

* 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 application or patent 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
13 April 2008 (13.04.2008)	30 APR 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)