PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:	WO 99/27437
G06F 7/36	A1	(43) International Publication Date:	3 June 1999 (03.06.99)

(21) International Application Number: PCT/US98/23476

(22) International Filing Date: 4 November 1998 (04.11.98)

(30) Priority Data:
08/979,803 26 November 1997 (26.11.97) US

(71) Applicant: ATMEL CORPORATION [US/US]; 2325 Orchard Parkway, San Jose, CA 95131 (US).

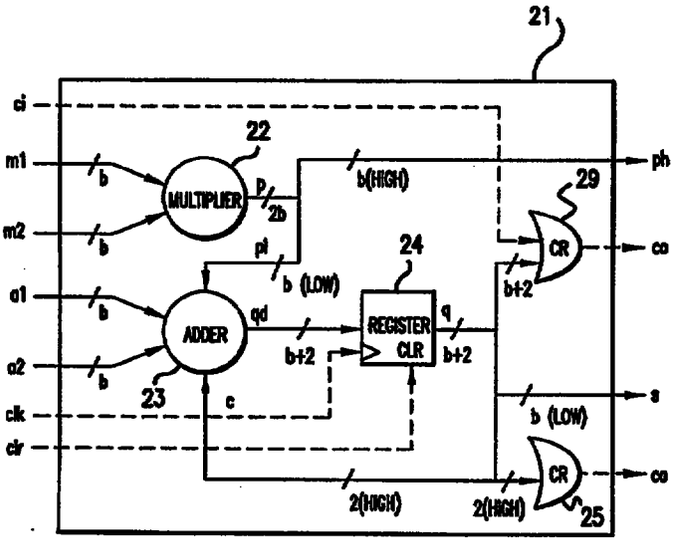
(72) Inventors: SABIN, Michael, J.; 883 Mango Avenue, Sunnyvale, CA 94087 (US). HEISING, Mark, W.; 557 East Crescent Drive, Palo Alto, CA 94301 (US).

(74) Agent: NEWMAN, David, B., Jr.; David Newman Chartered, P.O. Box 2728, La Plata, MD 20646-2728 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, 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), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: APPARATUS FOR MULTIPRECISION INTEGER ARITHMETIC



(57) Abstract

A system and method for performing multiplication and modular reduction of large integers. The system includes at least one large integer unit (21), each large integer unit having a multiplier (22), an adder (23), and a register (24). First and second multiplier inputs are applied to the multiplier, and first and second adder inputs are applied to the adder. One output of the multiplier is also applied to the adder. A plurality of large integer units may be connected into a large integer unit array (39) that includes a complementing gate (35) and a latching register (34). A second output of the multiplier is applied to the first adder input of a next large integer unit, with processing speed increasing as additional large integer units are added to the array.