PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 7/72 — A1

(11) International Publication Number: WO 00/05645

(43) International Publication Date: 3 February 2000 (03.02.00)

(21) International Application Number: PCT/US99/00826

(22) International Filing Date: 13 January 1999 (13.01.99)

(30) Priority Data:
09/120,835 22 July 1998 (22.07.98) US

(71) Applicant: MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

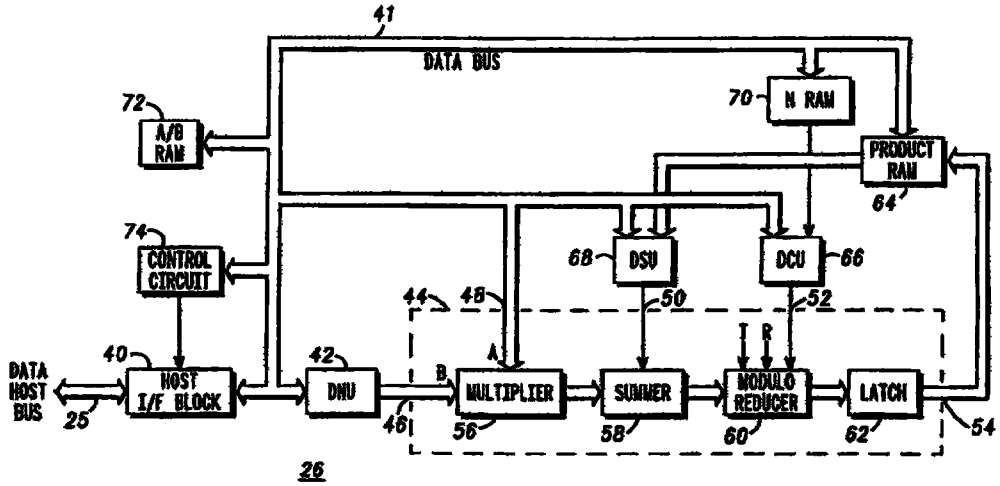
(72) Inventors: FOSTER, Robert, L.; 4055 N. Recker Road #62, Mesa, AZ 85215 (US). BUSS, John, Michael; 1066 W. Vera Lane, Tempe, AZ 85284 (US). TESCH, Rodney, C.; 7026 N. 13th Street, Phoenix, AZ 85020 (US). DWORKIN, James, Douglas; 6802 W. Shannon Street, Chandler, AZ 85226 (US). TORLA, Michael, J.; 5301 W. Del Rio Street, Chandler, AZ 85226 (US).

(74) Agents: INGRASSIA, Vincent, B. et al.; Motorola Inc., Intellectual Property Dept., P.O. Box 10219, Scottsdale, AZ 85271-0219 (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, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, 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: CIRCUIT AND METHOD OF MODULO MULTIPLICATION



(57) Abstract

A co-processor (44) executes an arithmetical algorithm that computes modular exponentiation equations for encrypting or decrypting data. A pipelined multiplier (56) receives sixteen bit data values stored in an A/B RAM (72) and generates a partial product. The generated partial product is summed in a summer (58) with a previous partial product stored in a product RAM (64). A modulo reducer (60) causes a binary data value N to be aligned and added to the summed value when a particular data bit location of the summed value has a logic one value. An N RAM (70) stores the data value N that is added in a modulo reducer (60) to the summed value.