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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/030015 A2

(51) International Patent Classification[7]: G06F 17/10

(21) International Application Number: PCT/US02/30448

(22) International Filing Date:
24 September 2002 (24.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/966,224 28 September 2001 (28.09.2001) US

(71) Applicant: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors: **RUEHLE, Mike**; 2655 Kaystone Avenue, #30, Santa Clara, CA 95051 (US). **MORELLI, John**; 2113 Skyline Drive, Milpitas, CA 95035 (US).

(74) Agents: **MALLIE, Michael, J.**; Blakely Sokoloff Taylor & Zafman, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025 et al. (US).

(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, UZ, VC, 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, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

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.

WO 03/030015 A2

(54) Title: METHOD AND APPARATUS FOR PERFORMING MODULAR EXPONENTIATION

(57) Abstract: A method and apparatus for performing modular exponentiation is disclosed. An apparatus in accordance with one embodiment of the present invention includes a first modular exponentiator and a second modular exponentiator and a coupling device interposed between the first modular exponentiator and the second modular exponentiator to recerve a control signal and to selectively couple the first modular exponentiator to the second modular exponentiator in response to a state of the control signal. In one embodiment, the apparatus has a first mode of operation corresponding to a first state of the control signal wherein the first modular exponentiator is operably separated from the second modular exponentiator and a second mode of operation corresponding to a second state of the control signal wherein the first modular exponentiator is operably coupled to the second modular exponentiator via the coupling device.