

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
3 April 2003 (03.04.2003)

PCT

(10) International Publication Number
WO 03/027833 A1

(51) International Patent Classification⁷: G06F 7/72, 7/556

(21) International Application Number: PCT/US02/29802

(22) International Filing Date:
18 September 2002 (18.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/964,137 26 September 2001 (26.09.2001) US

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

(72) Inventor: RUEHLE, Mike; 2655 Kaystone Avenue, #30,
Santa Clara, CA 95051 (US).

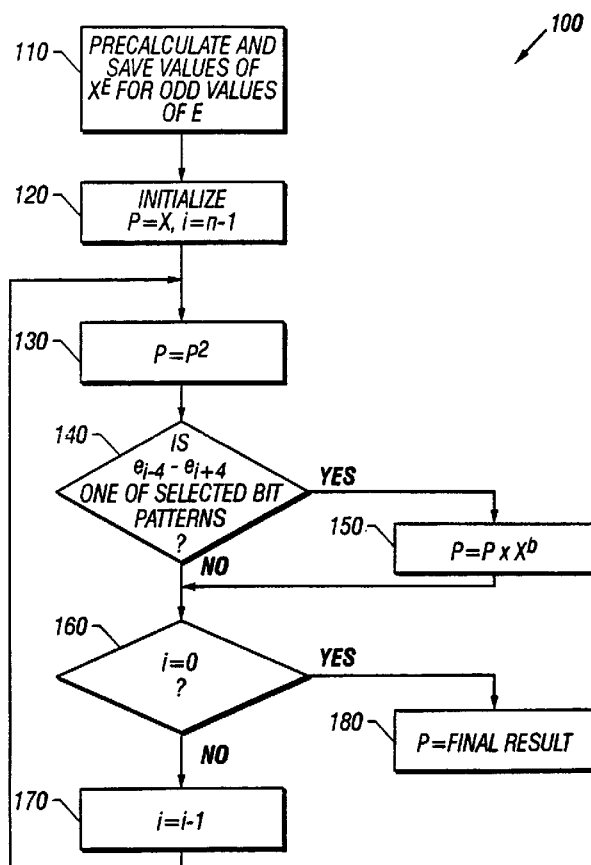
(74) Agents: MALLIE, Michael, J.; Blakely Sokoloff Taylor
& Zafman, 7th floor, 12400 Wilshire Boulevard, Los An-
geles, CA 90025 et al. (US).

(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,

[Continued on next page]

(54) Title: SQUARE-AND-MULTIPLY EXPONENT PROCESSOR



(57) Abstract: Processing exponents with a square-and-multiply technique that uses a flexible number of bits in the multiply stages. Multiple bits of the exponent can be handled in a single multiply operation, thus reducing the total number of multiply operations required to raise a number to a specified power. By examining prior and subsequent bits in the exponent in addition to the current bit, the quantity of bits that are handled in a particular multiply operation can be adjusted to the particular pattern of 1's and 0's in the exponent.

WO 03/027833 A1



TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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.

Published:

— *with international search report*