

(19) World Intellectual Property Organization
International Bureau



162162

(43) International Publication Date
6 December 2001 (06.12.2001)

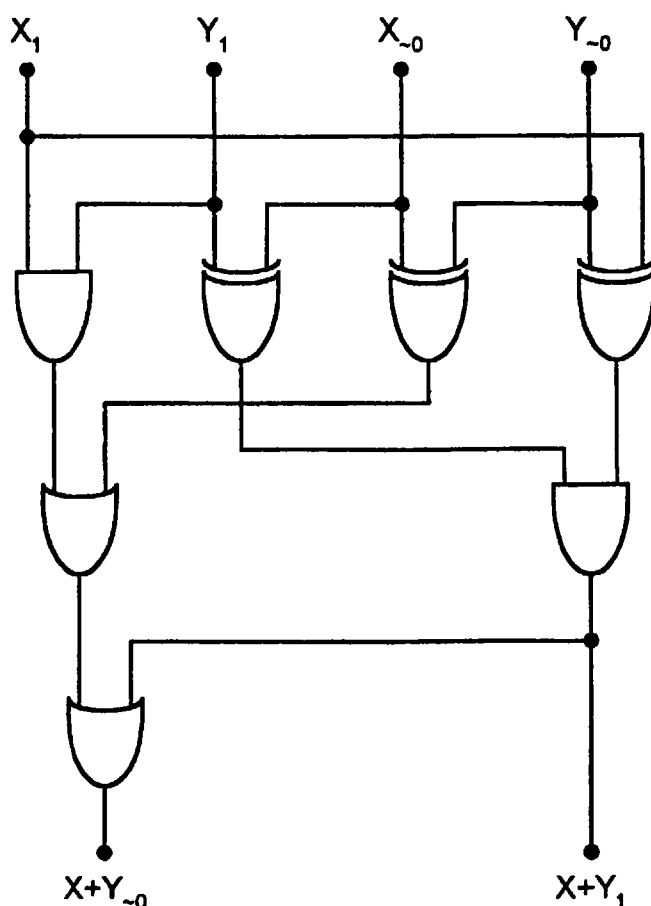
(10) International Publication Number
WO 01/93015 A1

PCT

- | | | | |
|---|---|--|---|
| (51) International Patent Classification ⁷ : | G06F 7/72 | | Felix, Egmont [GB/GB]; 26 Southfield Road, Oxford OX4 1NZ (GB). |
| (21) International Application Number: | PCT/GB01/02354 | | SHELTON, Daniel [GB/GB]; 51 St Bartholomews Road, Reading RG1 3QA (GB). |
| (22) International Filing Date: | 25 May 2001 (25.05.2001) | (74) Agents: | MAGGS, Michael, Norman et al.; Kilburn & Strode, 20 Red Lion Street, London WC1R 4PJ (GB). |
| (25) Filing Language: | English | (81) Designated States (<i>national</i>): | 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, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW. |
| (26) Publication Language: | English | (84) Designated States (<i>regional</i>): | ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European |
| (30) Priority Data: | 0013355.3
1 June 2000 (01.06.2000)
GB | (71) Applicant (<i>for all designated States except US</i>): | TAO GROUP LIMITED [GB/GB]; 62/63 Suttons Business Park, Earley, Reading RG6 1AZ (GB). |
| (72) Inventors; and | | (75) Inventors/Applicants (<i>for US only</i>): | GEIRINGER, |

[Continued on next page]

(54) Title: PARALLEL MODULO ARITHMETIC USING BITWISE LOGICAL OPERATIONS



(57) Abstract: Parallel modulo arithmetic calculations are carried out on a device adapted to perform bitwise logical operations by storing the numbers to be operated upon in a vector form, and performing arithmetical operations on multiple numbers in parallel. The invention finds particular application in cryptosystems, as well as in other fields.

WO 01/93015 A1

G00002

WO 01/93015 A1

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, 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*