

2002070910

25 NOV 2002



162162

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

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/93015 A1(51) International Patent Classification⁷: **G06F 7/72****Felix, Egmont** [GB/GB]; 26 Southfield Road, Oxford
OX4 1NZ (GB). **SHELTON, Daniel** [GB/GB]; 51 St
Bartholomews Road, Reading RG1 3QA (GB).

(21) International Application Number: PCT/GB01/02354

(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

(26) Publication Language: English

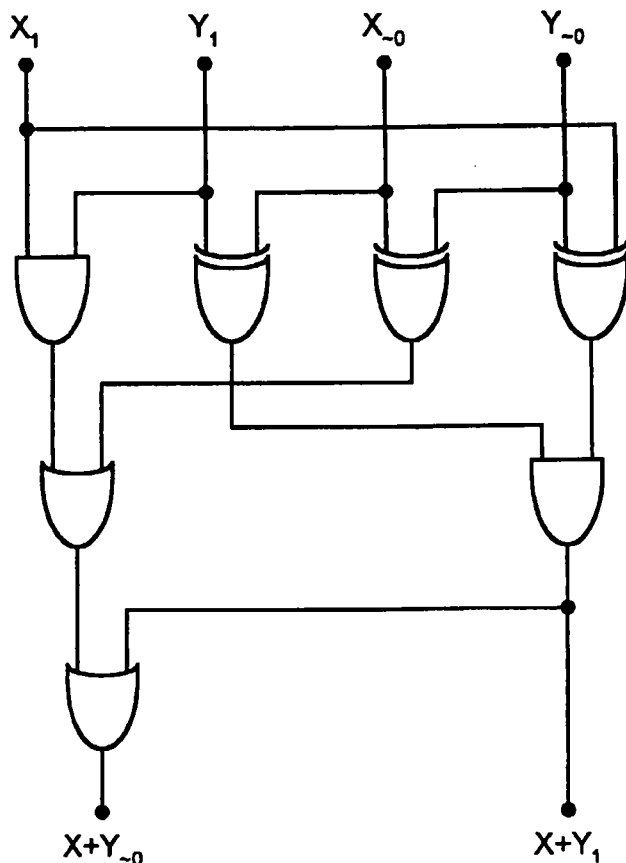
(30) Priority Data:
0013355.3 1 June 2000 (01.06.2000) GB(71) Applicant (for all designated States except US): **TAO
GROUP LIMITED** [GB/GB]; 62/63 Suttons Business
Park, Earley, Reading RG6 1AZ (GB).(81) Designated States (*national*): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, 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, PL, PT, RO, RU, SD, SE, SG, SI, SK,
SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA,
ZW.

(72) Inventors; and

(84) Designated States (*regional*): 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(75) Inventors/Applicants (for US only): **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 opera-
tions 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



ACTION