20020708894

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 01/93013 A1

(51) International Patent Classification[7]: G06F 7/58, H04L 9/22

(21) International Application Number: PCT/GB01/02337

(22) International Filing Date: 24 May 2001 (24.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0013349.6 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).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GEIRINGER, Felix, Egmont** [GB/GB]; 33 Regent Street, Oxford OX4 1DX (GB).

(74) Agents: **MAGGS, Michael, Norman** et al.; Kilburn & Strode, 20 Red Lion Street, London WC1R 4PJ (US).

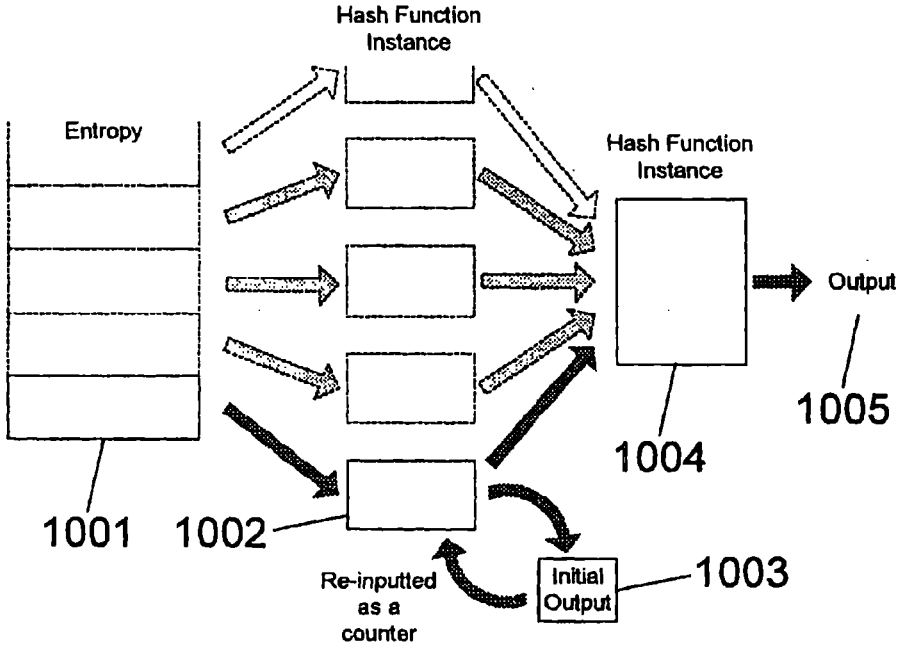
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(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 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).

Published:
— *with international search report*

[Continued on next page]

(54) Title: PSEUDO-RANDOM NUMBER GENERATOR



(57) Abstract: A pseudo-random number generator comprises: (a) a plurality of first-tier (1002) means each capable of receiving an entropy input (1001) and generating a respective hash output; and (b) a second-tier hashing means (1004), which takes as input the respective first-tier hash outputs and generates as output a pseudo-random number (1005). The generator of the present invention has particular application in cryptosystems, and particularly in public key cryptosystems where long sequences of data chosen from a large space of possible sequences need to be created quickly.

WO 01/93013 A1

ACTION