20020742776

25 NOV 2002

(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 01/93497 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/GB01/02365

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

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0013356.1 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) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GEIRINGER, Felix, Egmont** [GB/GB]; 33 Regent Street, Oxford OX4 1DX (GB). **SHELTON, Daniel** [GB/GB]; 51 St. Bartholomews Road, Reading RG1 3QA (GB).

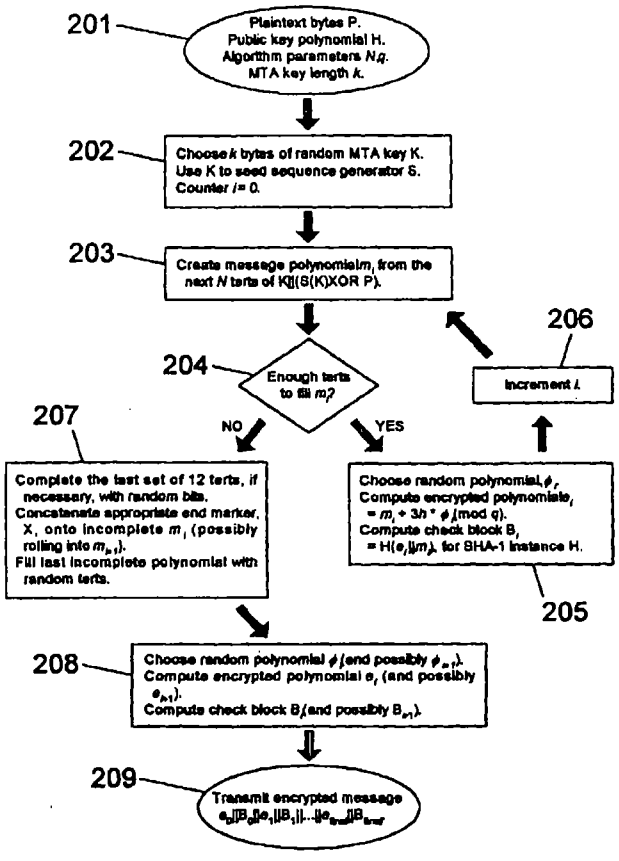
(74) Agents: **MAGGS, Michael, Norman** et al.; Kilburn & Strode, 20 Red Lion Street, London WC1R 4PJ (GB).

(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.

(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,

[Continued on next page]

(54) Title: A METHOD OF VALIDATING AN ENCRYPTED MESSAGE



(57) Abstract: A method of validating an encrypted message comprises; (a) representing the message (P) as a message polynomial (m_i); (b) encrypting the message polynomial (m_i) to form a cipher polynomial (e_i); (c) hashing first and second hash function inputs representative of the message polynomial and the cipher polynomial to create one or more hash outputs (B_i); and (d) transmitting to a recipient both an encrypted message defined by the cipher polynomial and the said one or more hash outputs. The method is particularly applicable to public key cryptosystems.

162162

ACTION

WO 01/93497 A1