(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 01/93496 A1

(51) International Patent Classification[7]: H04L 9/30

(21) International Application Number: PCT/GB01/02349

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

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0013398.3 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).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GEIRINGER, Felix, Egmont** [GB/GB]; 26 Southfield Road, Oxford OX4 1NZ (GB). **SHELTON, Daniel** [GB/GB]; 51 St. Bartholomews Road, Reading RG1 3QA (GB).

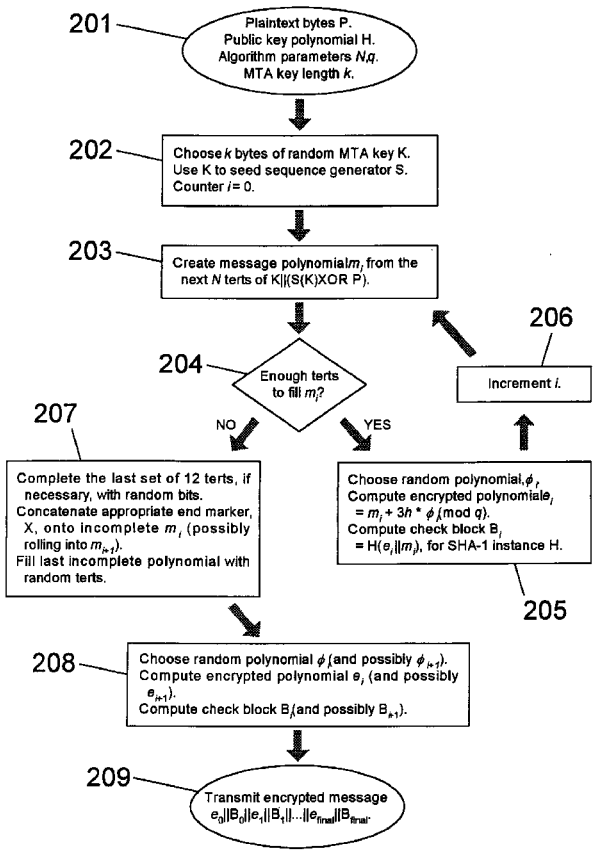
(74) Agents: **MAGGS, Michael, Norman** et al.; Kilburn & Strode, 20 Red Lion Street, London WC1R 4PJ (GB).

(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, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: A METHOD OF PROTECTING A CRYPTOSYSTEM FROM A MULTIPLE TRANSMISSION ATTACK



(57) Abstract: A method of protecting a cryptosystem from a multiple transmission attack (202, 203), comprises: a) applying to a plaintext message P to be encrypted to a protective cipher having a cipher key*k*, to produce a protected message (S(K)XOR P); b) creating from the protected message and the cipher key *k* an encryption input message (K|(S(K)XOR P); and c) encrypting the message. The invention find particular although not exclusive application within public key cryptosystems. The invention, when used in association with a strong standard cipher, protects against multiple transmission attack MTA by ensuring that the text which is encrypted differs every time a message is sent, even if identical messages are sent multiple times.

WO 01/93496 A1

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.