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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 April 2004 (08.04.2004)

PCT

(10) International Publication Number
WO 2004/030269 A3

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

(21) International Application Number:
PCT/GB2003/004064

(22) International Filing Date:
22 September 2003 (22.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/259,542 26 September 2002 (26.09.2002) US

(71) Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant *(for MG only)*: IBM UNITED KINGDOM LIMITED [GB/GB]; PO Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

(72) Inventor: LOTSPIECH, Jeffrey, Bruce; 2858 Hartwick Pines Drive, Henderson, NV 89052 (US).

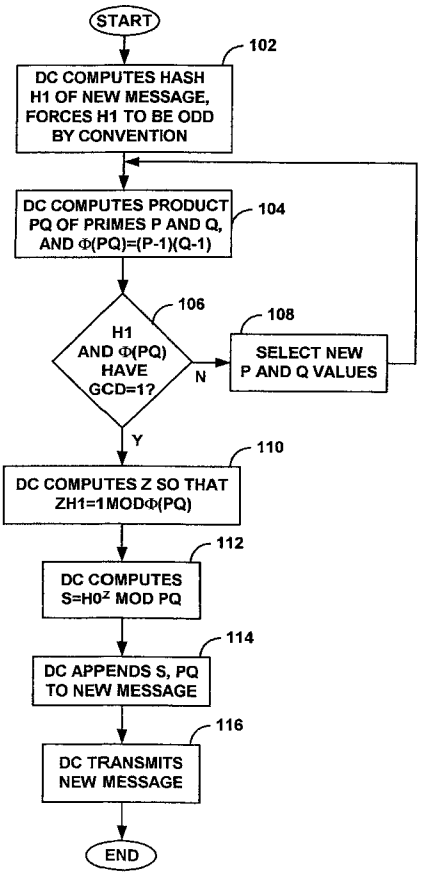
(74) Agent: LING, Christopher, John; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(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, EG, 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, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR GUARANTEEING SOFTWARE INTEGRITY



(57) Abstract: A system, method, and computer program product enabling user devices to authenticate and validate a digital message sent by a distribution centre, without requiring transmissions to the distribution centre. The centre transmits the message with an appended modulus that is the product of two specially selected primes. The transmission includes an appended authentication value based on an original message hash value, a new message hash value, and the modulus. The new message hash value is the centre's public RSA key; a corresponding private RSA key is also computed. Individual user devices combine a digital signet, a public modulus, unique secret numbers, and an original message hash to compute a unique integrity value K. Subsequent messages are similarly processed to determine new integrity values K', which equal K if and only if new messages originated from the centre and have not been corrupted.

WO 2004/030269 A3

SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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*

(88) Date of publication of the international search report:
12 August 2004

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.