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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 April 2005 (14.04.2005)

PCT

(10) International Publication Number
WO 2005/034423 A1

(51) International Patent Classification[7]: H04L 9/14

(21) International Application Number:
PCT/SG2004/000320

(22) International Filing Date: 1 October 2004 (01.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/508,720 3 October 2003 (03.10.2003) US

(71) Applicant *(for all designated States except US)*: **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 20 Biopolis Way #07-01, Centros, Singapore 138668 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ANATHARAMAN, Lakshminarayanan** [IN/SG]; 421A Pasir Panjang Road, Singapore 118762 (SG). **BAO, Feng** [CN/SG]; Blk 157, Yung Loh Road, #11-38, Singapore 610157 (SG). **DENG, Huijie Robert** [SG/SG]; 2 Namly Rise, Singapore 267110 (SG). **LI, Tieyan** [CN/SG]; Blk 69, Chua Chu Kang Loop, #12-10, Singapore 689672 (SG).

(74) Agent: **VIERING, JENTSCHURA & PARTNER**; P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).

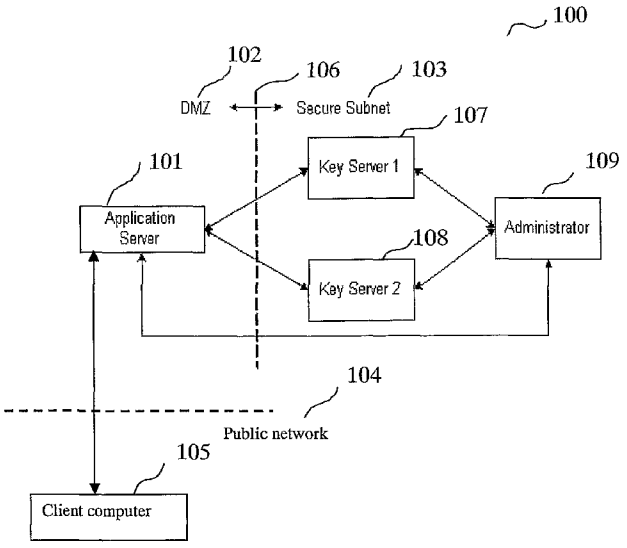
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, 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, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD FOR CRYPTOGRAPHICALLY PROCESSING A MESSAGE, METHOD FOR GENERATIING A CRYPTOGRAPHICALLY PROCESSED MESSAGE, METHOD FOR PERFORMING A CRYPTOGRAPHIC OPERATION ON A MESSAGE, COMPUTER SYSTEM, CLIENT COMPUTER, SERVER COMPUTER AND COMPUTER PROGRAM ELEMENTS



(57) Abstract: A method for cryptographically processing a message is disclosed, wherein a first partial cryptographic key and a second partial cryptographic key, which correspond to a decomposition of a private cryptographic key, are used, the message is processed using the first partial cryptographic key resulting in a first partially processed message, the message is processed using the second partial cryptographic key resulting in a second partially processed message and the first partially processed message and the second partially processed message are combined resulting in a cryptographically processed message.

WO 2005/034423 A1

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.