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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 November 2005 (10.11.2005)

PCT

(10) International Publication Number
WO 2005/107141 A1

(51) International Patent Classification[7]: H04L 9/30, 9/14

(21) International Application Number:
PCT/CA2005/000676

(22) International Filing Date: 2 May 2005 (02.05.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/566,790 30 April 2004 (30.04.2004) US

(71) Applicant *(for all designated States except US)*: **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors; and

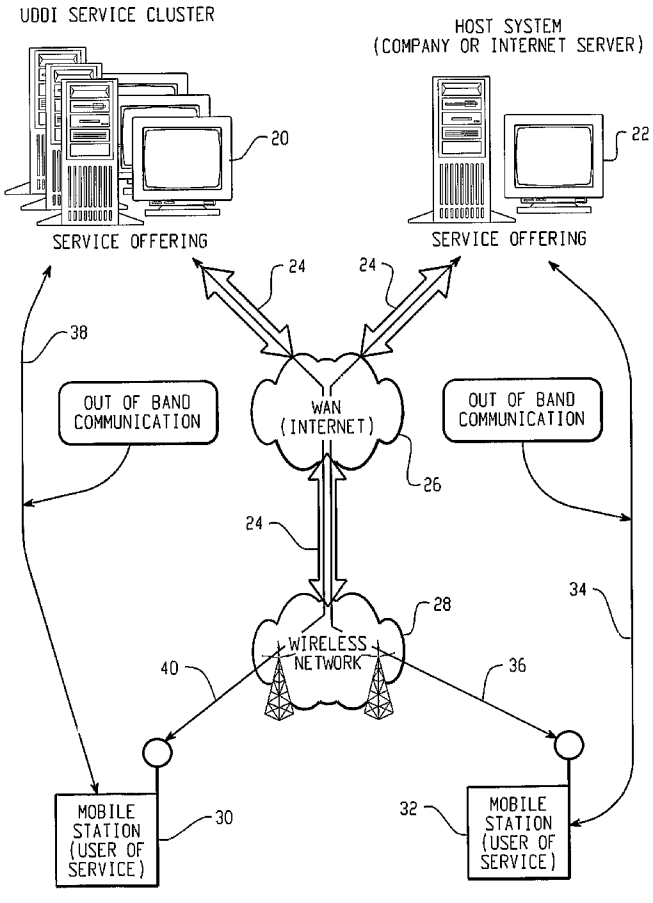
(75) Inventors/Applicants *(for US only)*: **BROWN, Michael, K.** [CA/CA]; 8 Fernwood Place, Kitchener, Ontario N2M 2Z2 (CA). **LITTLE, Herbert, A.** [CA/CA]; 504 Old Oak Place, Waterloo, Ontario N2T 2V8 (CA). **MACFARLANE, David, Victor** [CA/CA]; 518 Beaverwood Street, Waterloo, Ontario N2V 2M2 (CA). **BROWN, Michael, S.** [CA/CA]; 350 University Down Cres., Waterloo, Ontario N2K 4B1 (CA). **DAVIS, Dinah, Lea, Marie** [CA/CA]; 205-305 Margaret Avenue, Kitchener, Ontario N2H 6S4 (CA).

(74) Agents: **WONG, Jeffrey, W.** et al.; Borden Ladner Gervais LLP, 100 Queen Street, Suite 1100, Ottawa, Ontario K1P 1J0 (US).

(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, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM,

[Continued on next page]

(54) Title: SYSTEMS AND METHODS TO SECURELY GENERATE SHARED KEYS



(57) Abstract: A method for secure bidirectional communication between two systems is described. A first key pair and a second key pair are generated, the latter including a second public key that is generated based upon a shared secret. First and second public keys are sent to a second system, and third and fourth public keys are received from the second system. The fourth public key is generated based upon the shared secret. A master key for encrypting messages is calculated based upon a first private key, a second private key, the third public key and the fourth public key. For re-keying, a new second key pair having a new second public key and a new second private key is generated, and a new fourth public key is received. A new master key is calculated using elliptic curve calculations using the new second private key and the new fourth public key.

WO 2005/107141 A1

PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, 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, IS, IT, LT, 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*

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.