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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 April 2003 (17.04.2003)

PCT

(10) International Publication Number
WO 03/032573 A2

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number: PCT/US02/32054

(22) International Filing Date: 8 October 2002 (08.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/973,301 9 October 2001 (09.10.2001) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121 (US).

(72) Inventors: HAWKES, Philip; 2/6-8 Belmore Street, Burwood, New South Wales 2134 (AU). LEUNG, Nikolai K., N.; 7710 Takoma Avenue, Takoma Park, MD 20912 (US). ROSE, Gregory G.; 6 Kingston Avenue, Mortlake, New South Wales 2137 (AU).

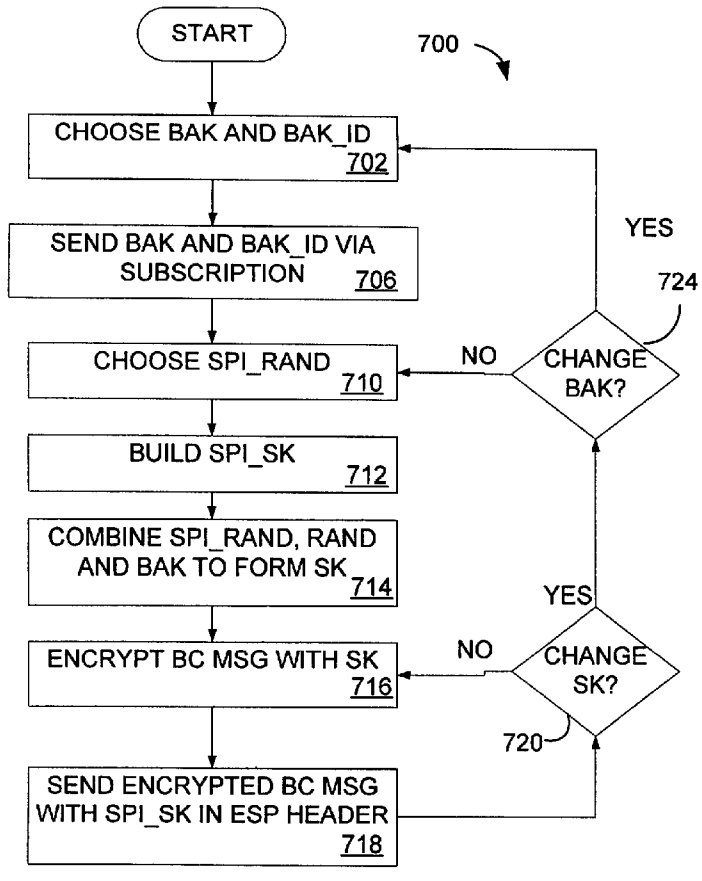
(74) Agents: WADSWORTH, Philip, R. et al.; QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, CA 92121 (US).

(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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, 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, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURITY IN A DATA PROCESSING SYSTEM



(57) Abstract: Method and apparatus for secure transmissions. Each user is provided a registration key. A long-time updated broadcast key is encrypted using the registration key and provided periodically to a user. A short-time updatedkey is encrypted using the broadcast key. The short-time key is available with each broadcast message,wherein sufficient information to calculate the short-time key is provided in an Internet protocol headerpreceding the broadcast content. Broadcasts are then encrypted using the short-time key, wherein the user decrypts the broadcast message using the short-time key.

WO 03/032573 A2

Published:

— *without international search report and to be republished upon receipt of that 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.