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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 February 2008 (28.02.2008)

PCT

(10) International Publication Number
WO 2008/024999 A3

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2007/076800

(22) International Filing Date: 24 August 2007 (24.08.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/840,141	24 August 2006 (24.08.2006)	US
11/843,583	22 August 2007 (22.08.2007)	US

(71) Applicant *(for all designated States except US)*: **QUALCOMM INCORPORATED** [US/US]; International IP Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NARAYANAN, Vidya** [IN/US]; 5775 Morehouse Drive, San Diego, California 92121 (US). **DONDETI, Lakshminath, Reddy** [IN/US]; 5775 Morehouse Drive, San Diego, California 92121 (US). **AGASHE, Parag, Arun** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US). **BENDER, Paul, E.** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).

(74) Agents: **BACHAND, Richard, A.** et al.; International IP Administration, 5775 Morehouse Drive, San Diego, Califonia 92121 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

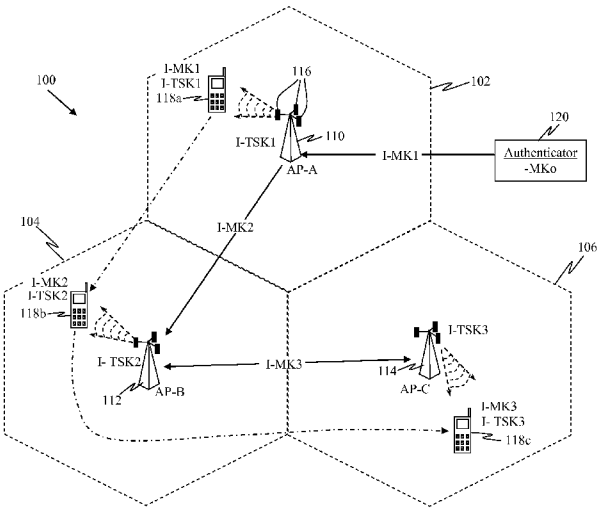
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, 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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR KEY MANAGEMENT FOR WIRELESS COMMUNICATIONS SYSTEMS



(57) Abstract: A novel key management approach is provided for securing communication handoffs between an access terminal (118) and two access points (110,112). This approach provides for securely handing off communications between an access terminal and access point without risking exposure a master key for the access terminal. Temporary master keys (I-MK) are derived for low latency handoffs and secure authentication between a new access point (112) and the access terminal! In one aspect, a distributive key management scheme is provided in which a current access point (110) generates a new security key (based on its own security key) that is used by the next access point with which an access terminal communicates. In another aspect, a centralized key management scheme is provided in which a central authenticator (120) maintains, generates, and distributes new security keys (based on a master security key associated with the access terminal) to access points.

WO 2008/024999 A3

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

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:
15 May 2008