

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
6 November 2008 (06.11.2008)

PCT

(10) International Publication Number
WO 2008/134564 A1

(51) International Patent Classification:
H04L 12/22 (2006.01) **H04Q 7/38** (2006.01)

(21) International Application Number:
PCT/US2008/061645

(22) International Filing Date: 25 April 2008 (25.04.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/914,033 26 April 2007 (26.04.2007) US
12/109,082 24 April 2008 (24.04.2008) US

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

(72) Inventor; and

(75) Inventor/Applicant (for US only): **VANDERVEEN, Michaela** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).

(74) Agent: **KIM, Won Tae**; Attn: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: A METHOD AND APPARATUS FOR NEW KEY DERIVATION UPON HANDOFF IN WIRELESS NETWORKS

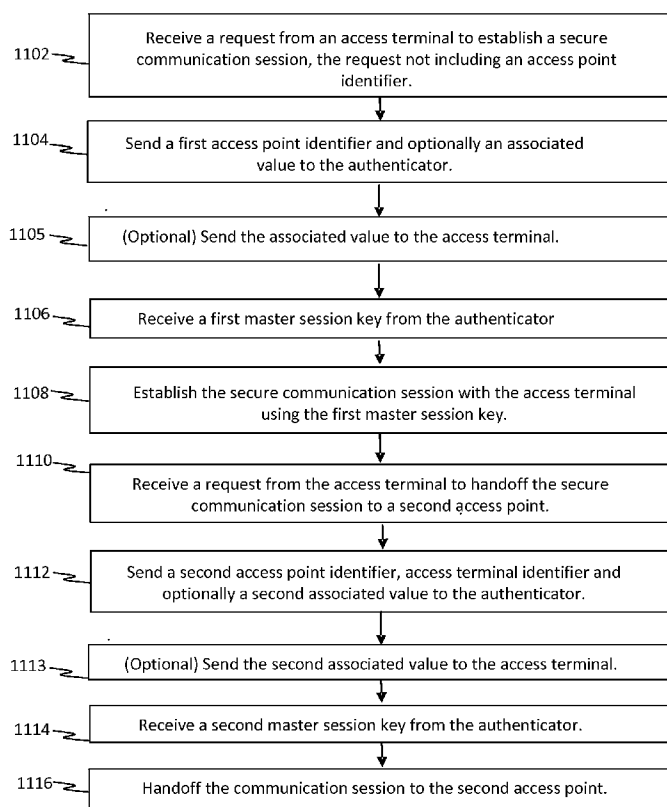


Figure 11

(57) Abstract: A novel key management approach is provided for securing communication handoffs between an access terminal and two access points. As an access terminal moves from a current access point to a new access point, the access terminal sends a short handoff request to the new access point. The short handoff request may include the access terminal ID; it does not include the access point ID. The new access point may then send its identifier and the access terminal's identifier to the authenticator. Using a previously generated master transient key, the access point identifier and the access terminal identifier, an authenticator may generate a master session key. The master session key may then be sent to the access point by the authenticator. The access terminal independently generates the same new security key with which it can securely communicate with the new access point.

WO 2008/134564 A1



Declarations under Rule 4.17:

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