

(51) International Patent Classification:
H04W 12/04 (2009.01) *H04L 29/06* (2006.01)(21) International Application Number:
PCT/IB2009/005129(22) International Filing Date:
30 March 2009 (30.03.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/042,478 4 April 2008 (04.04.2008) US
61/043,857 10 April 2008 (10.04.2008) US(71) Applicant (for all designated States except US): **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **FORSBERG, Dan, Lars, Anders** [FI/FI]; Melkonkatu 7 A 33, FIN-00210 Helsinki (FI). **NIEMI, Pentti, Valtteri** [FI/CH]; Chemin de Pierrefleur 23 B, CH-1004 Lausanne (FI). **BLOMMAERT, Marc** [BE/BE]; Bokmolenstraat 2A, B-9140 Temse (BE).(74) Common Representative: **NOKIA CORPORATION**;
C/o Nokia Inc., 6021 connection Drive, MS 2-5-520, Irving, TX 75039 (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, ST, 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, MK, 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).

Published:

— with international search report (Art. 21(3))

[Continued on next page]

(54) Title: METHODS, APPARATUSES, AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING MULTI-HOP CRYPTOGRAPHIC SEPARATION FOR HANDOVERS

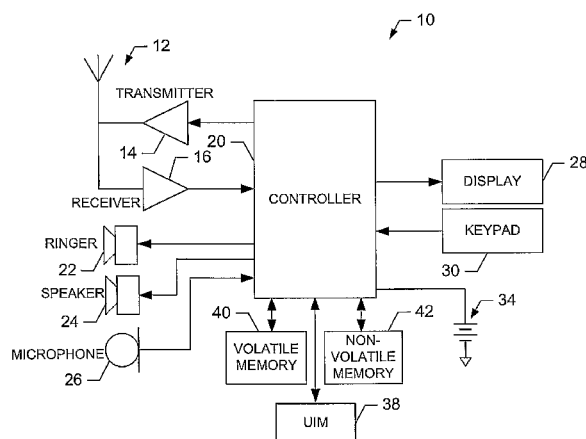


FIG. 1.

(57) Abstract: A method, apparatus and computer program product are provided to provide cryptographical key separation for handovers. A method is provided which includes calculating a key based at least in part upon a previously stored first intermediary value. The method also includes calculating a second intermediary value based at least in part upon the calculated key. The method additionally includes sending a path switch acknowledgement including the second intermediary value to a target access point. The method may further include receiving a path switch message including an indication of a cell identification and calculating the encryption key based upon the indication of the cell identification. The method may further include storing the second intermediary value. The calculation of the key may further comprise calculating the key following a radio link handover. Corresponding apparatuses and computer program products are also provided.



— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(88) Date of publication of the international search report:
1 April 2010