

(51) International Patent Classification:
H04W 12/04 (2009.01) *H04W 12/08* (2009.01)(21) International Application Number:
PCT/US2010/040731(22) International Filing Date:
1 July 2010 (01.07.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/223,360 6 July 2009 (06.07.2009) US
12/643,675 21 December 2009 (21.12.2009) US(71) Applicant (for all designated States except US): **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95052 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SHARAGA, Avishay** [IL/IL]; 165 Jasmin Road, 73140 Beit Nehemya (IL). **YANG, Xiangying** [CN/US]; 15864 NW Ryegrass Street, Portland, Oregon 97229 (US).(74) Agents: **POLLACK, Caleb** et al.; Pearl Cohen Zedek Latzer, 1500 Broadway, 12th Floor, New York, New York 10036 (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, CL, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: METHOD AND APPARATUS OF DERIVING SECURITY KEY(S)

(57) Abstract: A method, apparatus and a wireless communication system to derive security key(s) over an air link in a secure manner by sending by a mobile station over the air a single direction permutation of a mobile station ID, establishing keys with the base station and sending the mobile station real ID in a secure manner.

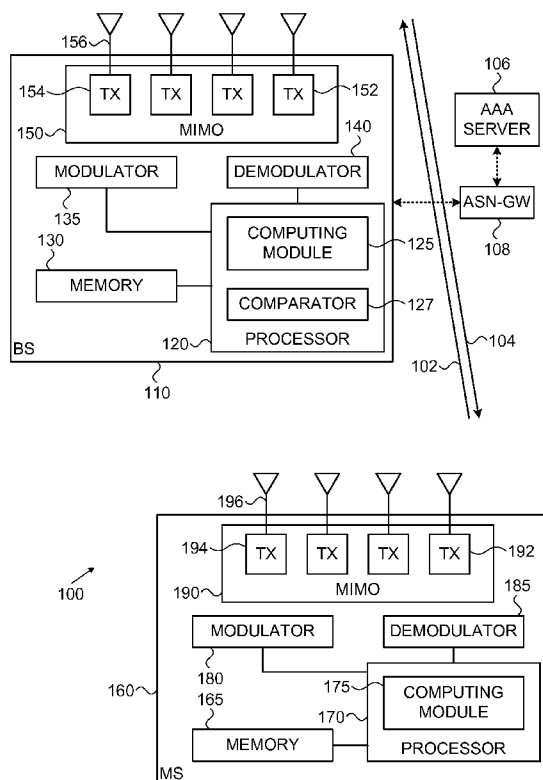


FIG. 1



(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, 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, SM, 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))*
- *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:

14 April 2011