

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
2 November 2006 (02.11.2006)

PCT

(10) International Publication Number
WO 2006/114684 A3

(51) International Patent Classification:
H04L 9/08 (2006.01) **H04H 1/00** (2006.01)

(21) International Application Number:
PCT/IB2006/000992

(22) International Filing Date: 24 April 2006 (24.04.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/674,959 25 April 2005 (25.04.2005) US

(71) Applicant (for all designated States except US): **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FI-02150 Espoo (FI).

(71) Applicant (for LC only): **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, Texas 75039 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **TARKKALA, Lauri** [FI/FI]; Tiklinkuja 8b4, FI-02660 Espoo (FI).

(74) Agents: **FILL, Peter, N.** et al.; Morgan & Finnegan, LLP, 3 World Financial Center, New York, New York 10281-2101 (US).

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

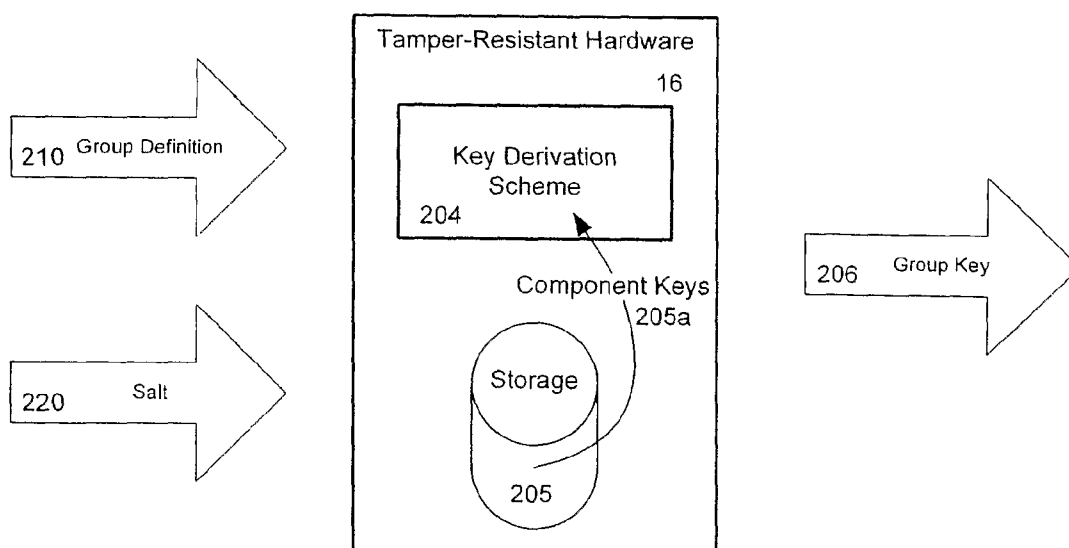
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT,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

Published:
— with international search report

(88) Date of publication of the international search report:
18 January 2007

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.

(54) Title: METHOD AND APPARATUS FOR GROUP KEY GENERATION



(57) Abstract: A key generation system is disclosed that provides for the generation of privileged group keys based on the input of a privileged group. The system performing the key generation has stored component keys corresponding to every possible subset X of the unitary set, where subsets X have k or fewer members. The privileged group key is generated for the privileged set by passing ordered component keys of subsets X that do not contain members of the privileged set to a pseudo random function.

WO 2006/114684 A3