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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 March 2005 (17.03.2005)

PCT

(10) International Publication Number
WO 2005/025123 A1

(51) International Patent Classification[7]: H04L 9/06

(21) International Application Number:
PCT/EP2004/052020

(22) International Filing Date:
2 September 2004 (02.09.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03103307.9 5 September 2003 (05.09.2003) EP

(71) Applicant *(for all designated States except US)*: **MEDIACRYPT AG** [CH/CH]; Technoparkstrasse 1, CH-8005 Zurich (CH).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VAUDENAY, Serge** [CH/CH]; Chemin de Riant-Mont 4, CH-1023 Crissier (CH). **JUNOD, Pascal** [CH/CH]; Chemin de Montétan 13, CH-1004 Lausanne (CH).

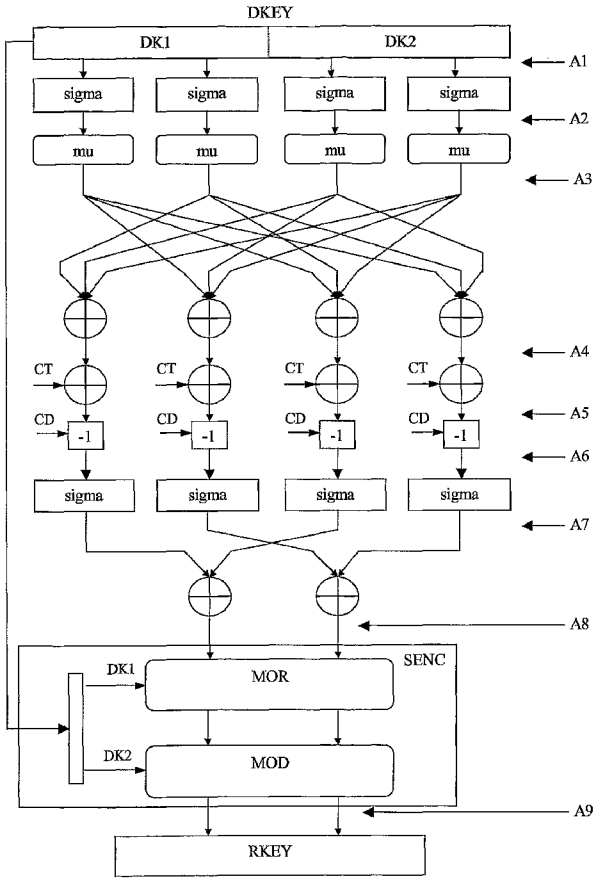
(74) Agent: **LEMAN CONSULTING S.A.**; WENGER Joel, Route de Clémenty 62, CH-1260 Nyon (CH).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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,

[Continued on next page]

(54) Title: METHOD FOR GENERATING PSEUDO-RANDOM SEQUENCE



(57) Abstract: The aim of this invention is to propose a method to generate sequences or sub-keys based on a main key, in which each sub-key gives no information to recover the main key or any other sub-keys. The aim is achieved with a method to generate sub-keys based on a main key (MKEY), comprising the following steps: - obtaining a first value (A1) by applying to the main key (MKEY) a linear diversification layer by mixing the main key (MKEY) with a constant, - applying to the first value (A1) a non-linear transformation, this transformation comprising the steps of: - obtaining a second value (A2) by applying the first value (A1) to a substitution layer, the substitution layer comprising at least one substitution box (sbox), each substitution box containing at least one table of constants for which the input serves as the pointer and the pointed constant serves as the output, - obtaining a third value (A3) by using a diffusion box of multi-permutation type based on the second value (A2), - dividing the third value (A3) in N blocks of same size, obtaining the output fourth value (A4) formed by N blocks, each block of the fourth value (A4) being the result of the combination of N-1 blocks of the third value (A3), the missing block being the block of the same index, - obtaining the fifth value (A5) by applying to the fourth value (A4) a substitution layer, - obtaining the sub-key (RKEY) by applying to the fifth value (A5) a symmetrical encryption module, the first value (A1) serving as the key input for this module.

WO 2005/025123 A1

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, IT, LU, 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*

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.