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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 December 2004 (02.12.2004)

PCT

(10) International Publication Number
WO 2004/105305 A1

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

(21) International Application Number:
PCT/EP2004/050854

(22) International Filing Date: 19 May 2004 (19.05.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03011696.6 23 May 2003 (23.05.2003) EP

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

(72) Inventors; and

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

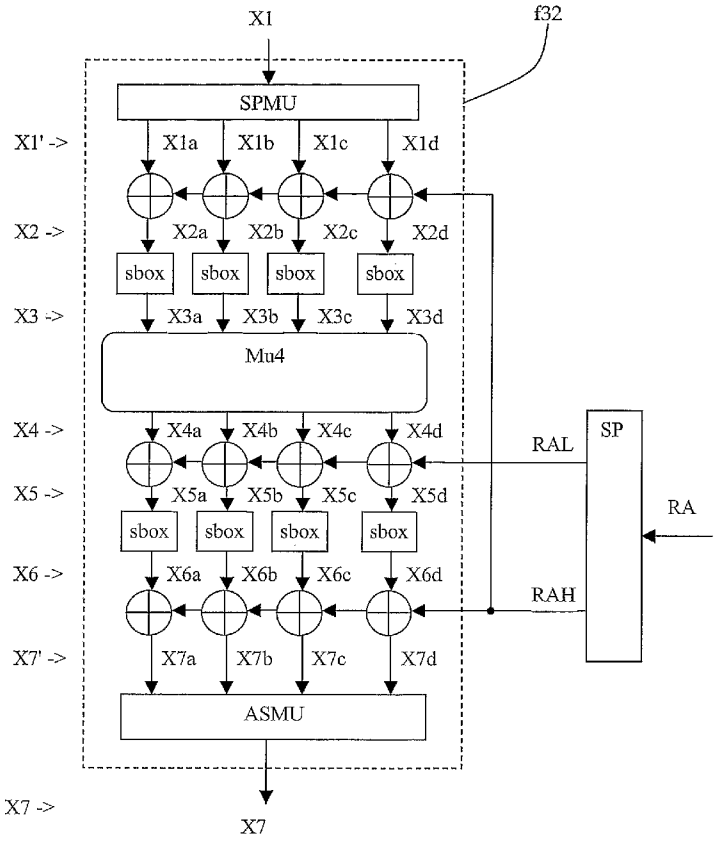
(74) Agent: **LEMAN CONSULTING S.A.**; WENGER Joel, Route de Clémenty 62, CH-1260 Nyon (CH).

(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, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Continued on next page]

(54) Title: DEVICE AND METHOD FOR ENCRYPTING AND DECRYPTING A BLOCK OF DATA



(57) Abstract: Method to encrypt or decrypt blocks of data X to Y, based on a main key R, this method using several serially connected modules, each module using a sub-key RA derived from the main key R and comprising the steps of: - inputting at least two initial values XOL and XOR, and mixing these values to form a mixed value X1, - obtaining a value X2 by mixing a first part RAH of the sub-key RA with the value X1, - obtaining a value X3 by applying the value X2 to a substitution layer, comprising at least one substitution box (sbox), - obtaining a value X4 by using a diffusion box of multi-permutation type based on the value X3, - obtaining a value X5 by mixing a second part RAL of the sub-key RA with the value X4, - obtaining the value X6 by applying to the value X5 a substitution layer, - obtaining a value X7 by mixing a first part RAH of the sub-key RA with the value X6, - mixing the value X7 with the initial at least two values XOL and XOR to obtain the at least two values X8L and X81R, X8L and X8R representing the output value X8 of the module. This method using at least two modules, and applies to at least one of the value X8L or X8R an orthomorphism function before feeding them to the next module.

WO 2004/105305 A1

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).

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.

Published:

— *with international search report*