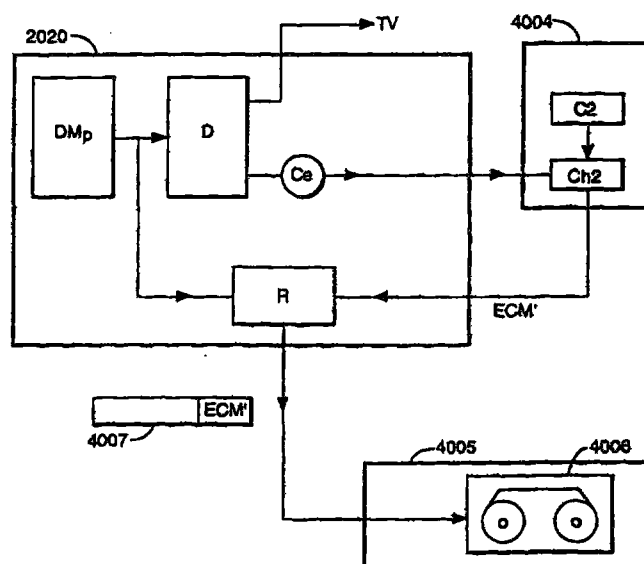




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04N 5/913		A1	(11) International Publication Number: WO 99/16244
			(43) International Publication Date: 1 April 1999 (01.04.99)
(21) International Application Number: PCT/IB98/01511 ✓		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 22 September 1998 (22.09.98) ✓			
(30) Priority Data: ✓ ① 97402238.6 ✓ 25 September 1997 (25.09.97) ✓ EP ✓			
(71) Applicant (for all designated States except US): CANAL+ SOCIÉTÉ ANONYME [FR/FR]; 85/89, quai André-Citroën, F-75711 Paris Cedex 15 (FR). ✓			
(72) Inventor; and (75) Inventor/Applicant (for US only): ① MAILLARD, Michel [FR/FR]; 42, avenue du Maréchal-Leclerc, F-28130 Maintenon (FR). ✓		Published With international search report. /	
(74) Agents: COZENS, Paul, Dennis et al.; Mathys & Squire, 100 Grays Inn Road, London WC1X 8AL (GB).		1 PD. 1 appl. (Look out fr symbols) 1 inv. (see 1B/306) IPC = H04N 5/913 IPER 29/3/99	

(54) Title: METHOD AND APPARATUS FOR RECORDING OF ENCRYPTED DIGITAL DATA ✓



(57) Abstract

A method for transmission and recording of encrypted information (Ce), in which the information (Ce) is encrypted by a first key and transmitted in encrypted form, the encrypted information (Ce) being received by a decoder (2020) possessing an equivalent of the first key necessary to decrypt the information and characterised in that the decrypted information (Ce) is re-encrypted by means of a second key (C2) stored in a portable support device (4004) adapted to be received by the decoder (2020) and/or digital recording device (4005), the re-encrypted information being thereafter recorded on the digital recording medium (4006). When replaying the recording, the information is decrypted by means of the second key (C2) stored on the support means (4004). In a particularly preferred embodiment, the information (Ce) corresponds to a control word used to scramble and descramble transmitted data, the re-encrypted control word (Ce) being stored on the recording medium (4006) together with the still scrambled transmitted data.