1 Pos copy
20000 1462-1

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 7/16, 7/167

A1

(11) International Publication Number: WO 99/18729

(43) International Publication Date: 15 April 1999 (15.04.99)

(21) International Application Number: PCT/IB98/01610

(22) International Filing Date: 2 October 1998 (02.10.98)

(30) Priority Data:

97402322.8	2 October 1997 (02.10.97)	EP
98401388.8	9 June 1998 (09.06.98)	EP
98401389.6	9 June 1998 (09.06.98)	EP

(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).

Published
With international search report.

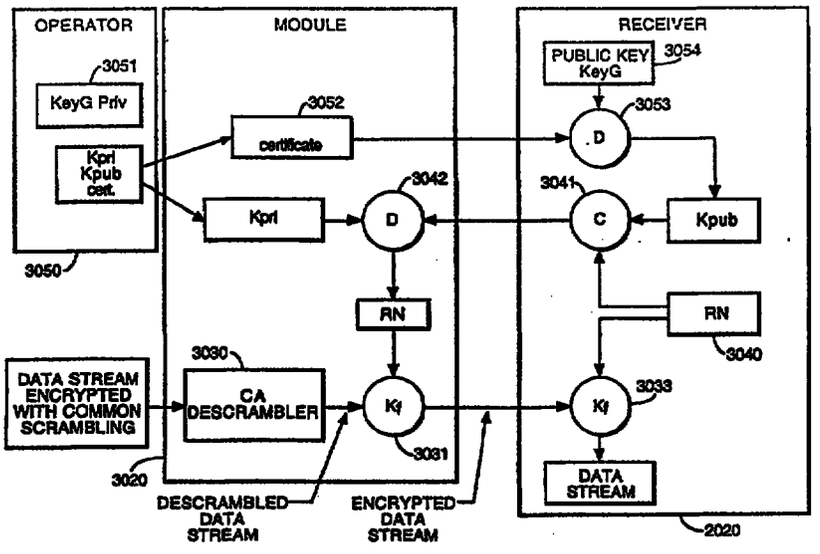
(71) Applicant *(for all designated States except US)*: CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai André-Citroen, F-75711 Paris Cedex 15 (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: MAILLARD, Michel [FR/FR]; 42, avenue du Maréchal-Leclerc, F-28130 Maintenon (FR). BENARDEAU, Christian [FR/FR]; 13, allée des Puisatiers, F-77600 Bussy-Saint-Georges (FR). DAUVOIS, Jean-Luc [FR/FR]; 19, rue Eugène-Manuel, F-75116 Paris (FR).

(74) Agents: COZENS, Paul, Dennis et al.; Mathys & Squire, 100 Grays Inn Road, London WC1X 8AL (GB).

(54) Title: METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM TRANSMISSION



(57) Abstract

A method of transmission and reception of scrambled data in which the scrambled data is transmitted to a decoder (2020), the scrambled data being passed to and descrambled by a security module or smart card (3020) inserted in the decoder (2020) and characterised in that the scrambled data stream is passed from the smart card (2020) back to the decoder (3020) in an encrypted form. The encryption of the data stream may be carried out on the card (2020) or as a secondary encryption step at transmission. The data stream may correspond directly to audiovisual data descrambled in the security module or to a stream of control word data subsequently used by the decoder to descramble a transmission.