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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 August 2001 (02.08.2001)

PCT

(10) International Publication Number
WO 01/56287 A2

(51) International Patent Classification[7]: H04N 7/167

(21) International Application Number: PCT/IB01/00094

(22) International Filing Date: 24 January 2001 (24.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

0166/00	28 January 2000 (28.01.2000)	CH
60/226,769	21 August 2000 (21.08.2000)	US

(71) Applicant *(for all designated States except US)*: **NAGRACARD S.A.** [CH/CH]; 22, route de Genève, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KUDELSKI, André** [CH/CH]; Chemin de Bellingard, CH-1095 Lutry (CH). **SASSELLI, Marco** [CH/CH]; Chemin des Roches 20, CH-1803 Chardonne (CH).

(74) Agent: **LEMAN CONSULTING SA**; 62 route de Clementy, CH-1260 Nyon (CH).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, 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, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, 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, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that 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.

WO 01/56287 A2

(54) Title: METHOD AND SYSTEM FOR TRANSMISSION OF DECRYPTING INFORMATION

(57) Abstract: At the moment of the diffusion of Pay-TV with multi-channel signals, each channel is associated to authorization messages (ECM) which allow to decrypt this channel according to the rights of the subscriber. When changing channel, a very short time is accepted before one has determined these new rights in relation with the new channel. The heavy encrypting algorithms are thus excluded. To avoid this drawback, to decrypt a channel, a system is proposed using the combination of the authorization information for a channel (ECM), and thus encrypted by a fast algorithm, with authorization information (MECM) for a group of channels. These latter are encrypted by a high security algorithm and are thus slower to decrypt.