



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 5/913	A1	(11) International Publication Number: WO 00/64157 (43) International Publication Date: 26 October 2000 (26.10.00)
(21) International Application Number: PCT/EP00/03205 (22) International Filing Date: 11 April 2000 (11.04.00) (30) Priority Data: 99302887.7 14 April 1999 (14.04.99) EP (71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL). (72) Inventors: TALSTRA, Johan, C.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). LINNARTZ, Johan, P., M., G.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). HALL, Trevor, G., R.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). (74) Agent: FAESSEN, Louis, M., H.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).		(81) Designated States: BR, JP, KR, MX, SG, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>With international search report.</i>
(54) Title: METHOD AND SYSTEM OF COPY PROTECTION OF INFORMATION		
(57) Abstract The invention relates to a method of copy-protection of information stored on an information carrying medium (1). The method allows a reading device (20) (e.g. a DVD drive) and an application device (30) (e.g. an MPEG decoder) to exchange copy-protection information regarding the information carrying medium (1) (e.g. an optical record carrier like a CD or DVD) and the content on that medium (1). The method is cryptographically secure, taking into account the situation where reading device (20) and application device (30) are connected to an open bus (40) in a personal computer. In view of the high-volume nature of the drive, the method can be implemented cheaply. The inventive method is robust against a so-called man-in-the-middle attack. The invention relates also to a method of exchanging copy-protection information, to a copy-protection system and to devices for carrying out these methods, in particular a reading device (20), an application device (30) and a device for playback and/or recording of information.		