

(19) World Intellectual Property Organization
International Bureau



G00002



(43) International Publication Date
10 October 2002 (10.10.2002)

PCT

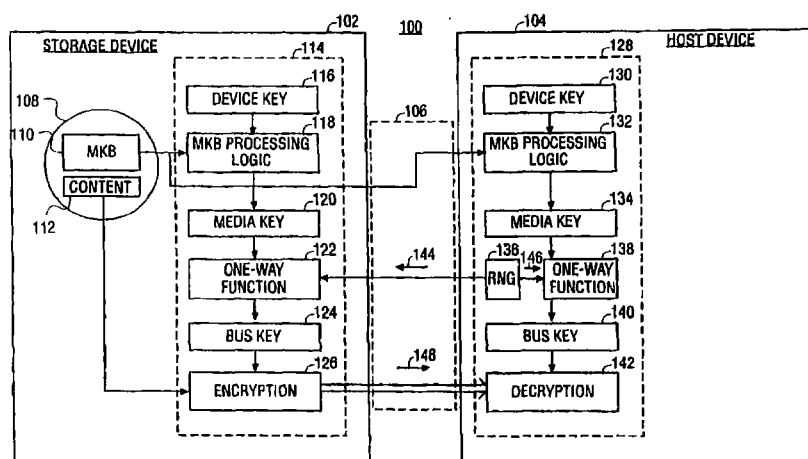
(10) International Publication Number
WO 02/080170 A3

- (51) International Patent Classification⁷: **G11B 20/00**, H04N 7/167
- (21) International Application Number: PCT/US02/07085
- (22) International Filing Date: 7 March 2002 (07.03.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
09/823,423 29 March 2001 (29.03.2001) US
- (71) Applicant: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).
- (72) Inventors: **TRAW, Brendan**; 10859 NW Supreme Court, Portland, OR 97229 (US). **RIPLEY, Mike**; 1222 NE 56th Court, Hillsboro, OR 97124 (US).
- (74) Agents: **MALLIE, Michael, J.**; Blakely, Sokoloff, Taylor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 et al. (US).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, 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, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:**
— with international search report
- (88) Date of publication of the international search report:
5 June 2003
- 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.

(54) Title: METHOD AND SYSTEM FOR PROVIDING BUS ENCRYPTION BASED ON CRYPTOGRAPHIC KEY EXCHANGE



162162



(57) Abstract: A system is described for protecting digital content stored (112) on a storage medium (108) from unauthorized copying. The system includes a number generator to generate a nonce, an encryption subsystem (114) and a decryption subsystem (128). The encryption subsystem encrypts data accessed from a storage medium containing a key distribution data block (MKB, 110) using an encryption bus key (124) prior to transmitting the encrypted data via a data bus (106). The encryption bus key is derived based on at least a portion of the key distribution data block (110), at least one device key (116) assigned to the encryption subsystem and the nonce generated by the number generator. The decryption subsystem is coupled to the data bus to decrypt the encrypted data received over the data bus using a decryption bus key (140) derived based on at least a portion of the key distribution data block, at least one device key (130) assigned to the decryption subsystem and the nonce generated by the number generator.

WO 02/080170 A3