

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
25 September 2003 (25.09.2003)

PCT

(10) International Publication Number
WO 03/079689 A1

(51) International Patent Classification⁷: **H04N 7/16, 7/167**

(21) International Application Number: **PCT/JP03/03232**

(22) International Filing Date: **18 March 2003 (18.03.2003)**

(25) Filing Language: **English**

(26) Publication Language: **English**

(30) Priority Data:
NO.2002-078397 20 March 2002 (20.03.2002) JP
NO.2002-364389 16 December 2002 (16.12.2002) JP
NO.2003-054134 28 February 2003 (28.02.2003) JP

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **ONO, Takatoshi** [JP/JP]; 110, Trusty Jimokuji 2-303, Azayamanoura, Oazajimokuji, Jimokujicho, Ama-gun, Aichi 490-1111 (JP). **KUMAZAKI, Yoji** [JP/JP]; 1390-155, Kagiyacho, Kasugai-shi, Aichi 480-0304 (JP). **YAMADA, Shigeru** [JP/JP]; 3-9-1-402, Aomataninishi, Mino-shi, Osaka 562-0023 (JP). **MURAKAMI, Hiroki** [JP/JP]; 2-8-5, Tsukumodai, Suita-shi, Osaka 565-0862 (JP). **INOUE, Tetsuya** [JP/JP]; 1-6-8-302, Masago, Ibaraki-shi, Osaka 567-0851 (JP). **OHMORI, Motoji** [JP/JP]; 1-9-3-402, Nasuzukuri, Hirakata-shi, Osaka 573-0071 (JP).

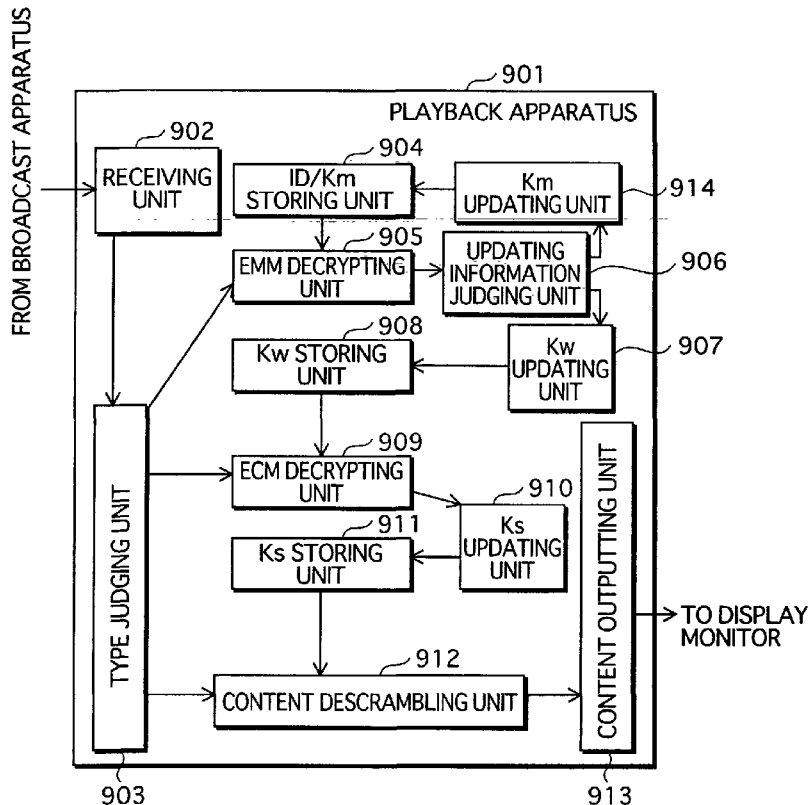
(74) Agent: **NAKAJIMA, Shiro**; 6F, Yodogawa 5-Bankan, 2-1, Toyosaki 3-chome, Kita-ku, Osaka-shi, Osaka 531-0072 (JP).

(71) Applicant (*for all designated States except US*): **MAT-SUSHITA ELECTRIC INDUSTRIAL CO., LTD.** [JP/JP]; 1006, Oazakadoma, Kadoma-shi, Osaka 571-8501 (JP).

(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, KE, KG, KP, KR, KZ, LC,

[Continued on next page]

(54) Title: **CONTENT PLAYBACK APPARATUS, METHOD, AND PROGRAM, AND KEY MANAGEMENT APPARATUS AND SYSTEM**



(57) Abstract: The present invention provides a technique which makes it possible to eliminate unauthorized playback of contents where unauthorized apparatuses are used and enable only authorized playback apparatuses to play back contents properly. The playback apparatus of the present invention obtains encrypted key information that has been encrypted by a first secret-key encrypting method, and decrypt the encrypted key information into key information using a secret key stored in a storing unit. When the key information is key-updating information, the playback apparatus updates the secret key according to the key-updating information. When the key information is a decryption key, the playback apparatus (i) obtains an encrypted content key that has been encrypted by a second secret-key encrypting method, (ii) decrypts the encrypted content key into a content key using the decryption key, (iii) obtains a scrambled content that has been scrambled by a scramble encrypting method, (iv) descramble the scrambled content using the decrypted content key, and (v) plays back the descrambled content.

WO 03/079689 A1



LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, 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, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

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.