PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G11B 20/00 — A2

(11) International Publication Number: WO 00/30100

(43) International Publication Date: 25 May 2000 (25.05.00)

(21) International Application Number: PCT/EP99/08631

(22) International Filing Date: 9 November 1999 (09.11.99)

(30) Priority Data:
98203890.3 19 November 1998 (19.11.98) EP

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: STARING, Antonius, A., M.; 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: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, 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), 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.

(54) Title: METHOD OF AND DEVICE FOR GENERATING A KEY

(57) Abstract

Method and read and/or write apparatus for generating a key (18) to control the access to information present on an information carrier (1). The key comprises a M-bit master key (12) and an information carrier key (2). The apparatus is adapted to read and/or write information on an information carrier (1). The apparatus is further adapted to generate the M-bit master key (12). The information carrier key (2) is read from the information carrier. The M-bit master key (12) is derived by determining a number p based on an identifier R and by reading out an N-bit string (11) from a position defined by the number p. In this way it is possible to prevent illegal copying of information from one information carrier to another.

