

(19) World Intellectual Property Organization
International Bureau



162162

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

PCT

(10) International Publication Number
WO 02/078419 A2

(51) International Patent Classification: Not classified

(21) International Application Number: PCT/JP02/03055

(22) International Filing Date: 28 March 2002 (28 03 2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2001-095730 29 March 2001 (29 03 2001) JP
2001-285608 19 September 2001 (19 09 2001) 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)

Nasuzukuri 1-chome, Hirakata-shi, Osaka 573-0071 (JP) **MATSUZAKI, Natsume** [JP/JP], 1-6-7-803, Aomadamn-rshi, Minou-shi, Osaka 562-0023 (JP) **TATEBAYASHI, Makoto** [JP/JP], 1-16-21, Metu, Takarazuka-shi, Hyogo 665-0852 (JP)

(74) Agent: **NAKAJIMA, Shiro** 6F, Yodogawa 5-Bankan, 2-1, Toyosaki 3-chome, Kita-ku, Osaka-shi, Osaka 531-0072 (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, KI, 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, US, UZ, VN, YU, ZA, ZM, ZW

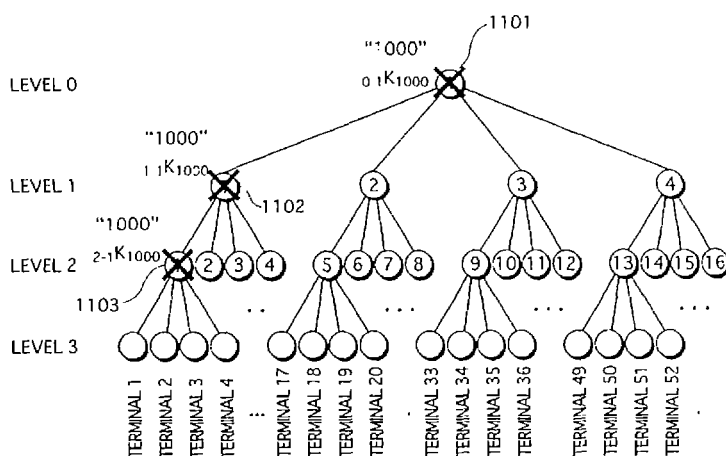
(72) Inventors; and

(75) Inventors/Applicants (for US only): **NAKANO, Toshi-hisa** [JP/JP], 3-35-15, Shimenou, Neyagawa-shi, Osaka 572-0077 (JP) **OHMORI, Motoji** [JP/JP], 9-3-402,

(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,

[Continued on next page]

(54) Title: DATA PROTECTION SYSTEM THAT PROTECTS DATA BY ENCRYPTING THE DATA



(57) Abstract: The object of the present invention is to provide a data protection system that reduces to a degree the amount of encrypted data that is distributed to a multiplicity of terminals, and that has a structure in which a terminal whose decryption keys are exposed by a dishonest party is made unable to decrypt the data correctly, while other terminals are able to decrypt the data correctly. The present invention is a data protection system that includes a multiplicity of terminals, and an encryption device that encrypts distribution data that is distributed to each terminal. Each terminal is corresponded with one node on a lowest level of 4-ary tree structure or the like that has a plurality of hierarchies. The data

protection system, for each node in the tree structure, excluding those on the lowest level, determines a plurality of combination patterns that include combinations of two or more of all four nodes that are reached one level below the node, decides an individual decryption key for each determined combination pattern, further decides an individual decryption key for each node on the lowest level, and has each terminal store all decryption keys decided for the nodes on the path from the node on the lowest level that corresponds to the terminal through to the node on the highest level. The data protection system prescribes nodes reached from the node on the lowest level that corresponds to the terminal through to the node on the highest level that correspond to a terminal that has been dishonestly analyzed as invalid nodes. For invalid nodes, other than invalid nodes on the lowest level, the data protection system designates an encryption key that corresponds to the decryption key decided in correspondence with the combination pattern that combines all nodes, excluding invalid nodes, of the four nodes that are reached one level below the node, and has the encryption device encrypt distribution data that uses each of the designated encryption keys.

WO 02/078419 A2



GB, GR, IL, 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)

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

Published:

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