METHOD AND APPARATUS FOR DECRYPTING ENCRYPTED DATA BY USING COPY CONTROL INFORMATION

A method of decrypting encrypted data includes reading decryption control information representing the encrypted data from an information storage, and changing the decryption control information into a decryptable condition by using a decryption coupon stored in a decryption device if the decryption control information indicates an undecryptable condition. Decryptability is additionally established in copy control information to increase data safety, enable various interactions with users, and facilitate access controls of the contents.
Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published: with international search report

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.
Description

METHOD AND APPARATUS FOR DECRYPTING ENCRYPTED DATA BY USING COPY CONTROL INFORMATION

Technical Field

[1] The present invention relates to digital data processing, and more particularly, to a method of and an apparatus for decrypting encrypted data.

Background Art

[2] Digital data are used in a variety of fields such as digital media, networks, and computing devices. Since digital data can be repeatedly copied without any quality degradation, in communication systems such as computer networks and remote communication systems, they need to be encrypted and then delivered to allow only authorized users to use the data, for the purpose of data security and management. In addition, digital data are encrypted and then stored in a data storage medium in order to allow only authorized users to use the data.

[3] However, if an authorized user decrypts the encrypted data by using a decryption key and then copies and distributes the decrypted data, unauthorized users can use the decrypted data freely. In this case, data providers may suffer an irreparable loss.

[4] Therefore, typically, information indicating that the data can be encrypted or allowed to be copied freely, i.e., CCI (copy control information), is added to the data and then provided to the users. However, since the CCI can not completely indicate that the encrypted data can be decrypted, complex processes for a decryption control need to be prepared in a reproducing step.

Disclosure of Invention

Technical Solution

[5] Accordingly, the present invention provides a method of and an apparatus for decrypting encrypted data in which decryptability information of the encrypted data is added to the encrypted data, so that data safety can be increased and various interactions with users can be made to create a new business model, and a computer readable recording medium storing a program for implementing the method of decrypting the encrypted data.

Advantageous Effects

[6] According to the method of and apparatus for decrypting encrypted data of the present invention, decryptability information is additionally established in the copy
control information, so that data safety can be increased, various interactions can be made with users, and an access control can be facilitated for the contents.

**Description of Drawings**

[7] The above and other features and advantages of the present invention will become more apparent by describing in detail exemplary embodiments thereof with reference to the attached drawings in which:

[8] FIG. 1 is a CCI table specifying copy control information;

[9] FIG. 2 is a schematic diagram showing how to process the copy control information;

[10] FIG. 3 is a CCI table showing an exemplary embodiment of extended CCI including decryptability information;

[11] FIG. 4 is a flowchart showing an exemplary embodiment of a method of decrypting encrypted data by using 'decrypt never CCI';

[12] FIG. 5 is a CCI ID table showing an exemplary embodiment of a CCI ID;

[13] FIG. 6 is a schematic diagram showing an exemplary embodiment of purchasing an encrypted CCI coupon by using both disc and device bindings;

[14] FIG. 7 is a schematic diagram showing an exemplary embodiment of purchasing an encrypted CCI coupon by using only a disc binding;

[15] FIG. 8 is a schematic diagram showing an exemplary embodiment of purchasing an encrypted CCI coupon by using only a device binding;

[16] FIG. 9 is a schematic diagram showing an exemplary embodiment of purchasing an encrypted CCI coupon by using a user's public key;

[17] FIG. 10 is a schematic diagram showing an exemplary embodiment of a method of providing contents by using 'decrypt never CCI'; and

[18] FIG. 11 is a schematic diagram showing an exemplary embodiment of a method of providing contents when a coupon is provided by changing a user's level.

**Best Mode**

[19] According to an exemplary aspect of the present invention, there is provided a method of decrypting encrypted data comprising steps of: reading out decryption control information representing decryptability of the encrypted data from an information storage medium; and changing the decryption control information into a decryptable condition by using a decryption coupon stored in a decryption device if the decryption control information indicates an undecryptable condition.

[20] According to another exemplary aspect of the present invention, there is provided an apparatus for decrypting encrypted data comprising: a reader which reads out
encrypted data and decryption control information representing decryptability of the encrypted data from an information storage medium; a coupon storage unit which stores the decryption coupon for the encrypted data; a decryption information changing unit which changes a condition of the decryption control information into a decryptable condition by using the decryption coupon stored in the coupon storage unit if the decryption control information indicates an undecryptable condition; and a data decryption unit which decrypts the encrypted data if the decryption control information indicates a decryptable condition.

According to still another exemplary aspect of the present invention, there is provided a computer readable recording medium which stores a program for implementing steps of: reading out decryption control information representing decryptability of encrypted data from an information storage medium; and changing a condition of the decryption control information into a decryptable condition by using a decryption coupon stored in a decryption device if the decryption control information indicates an undecryptable condition.

**Mode for Invention**

To fully understand advantages of the present invention, operation thereof, and objects to be attained by exemplary embodiments of the present invention, the accompanying drawings illustrating exemplary embodiments of the present invention and contents described in the accompanying drawings should be referred to.

Hereinafter, exemplary embodiments of the present invention will be described with reference to the accompanying drawings to explain the present invention in detail. The same elements in the drawings are indicated by the same reference numerals.

In digital data, particularly, AV (audio and/or video) data streams, CCI (copy control information) representing copyability is included to allow only authorized users to use contents.

FIG. 1 is a CCI table showing an exemplary meaning of CCI.

The CCI is composed of 2 bit codes so that 4 modes can be set. In other words, one of modes “copy free,” “copy free but encrypted,” “copy one generation,” and “copy never” (or “no more copy”) can be set.

If the CCI is set to the mode “copy free,” the contents are not encrypted, and they are unrestrictedly and freely copyable.

If the CCI is set to the mode “copy free but encrypted,” the contents are encrypted, but they are unrestrictedly copyable.

If the CCI is set to the mode “copy one generation,” the contents are encrypted, and
they are one-time copyable. In other words, once the contents are copied, the CCI is set to "no more copy."

[30] If the CCI is set to the mode "copy never," the contents are encrypted and they are never copyable. The "no more copy" has the same meaning as the "copy never," but particularly designates the case that the mode "copy one generation" is changed into the mode "copy never."

[31] FIG. 2 shows how to process the CCI. A contents provider 100 or distributor 110 determines the CCI value and inserts the determined CCI into a header of the stream to be transmitted to a user’s device 200. Then, a CPS (copy protection system) 232 within the user’s device 200 translates the CCI for the transmitted data and performs processes corresponding to the contents in FIG. 1. When the operation to be processed by the user’s device 200 corresponds with the CCI, a key needed for the decryption is provided to decrypt and reproduce the encrypted contents.

[32] As described above, since the CCI indicates only whether or not the contents are encrypted and copyable, it is impossible to represent decryptability, and a separate complex method is needed for a decryption control. Therefore, the present invention provides a method of providing extended copy control information including decryptability information together with the encrypted contents.

[33] FIG. 3 shows a CCI table showing an exemplary embodiment of the extended CCI including decryptability information.

[34] The decryptability information added to the extended CCI has two modes: "decrypt free" and "decrypt never." Hereinafter, the decryptability-added CCI is referred to as "decrypt never CCI" for convenience of description.

[35] If the "decrypt never CCI" is set to the mode "decrypt free," the corresponding contents are encrypted by using only an encryption key, so that copyability is determined by CCI values except for the "decrypt never CCI."

[36] If the "decrypt never CCI" is set to the mode "decrypt never," the corresponding contents are encrypted by using an encryption key and a decryption coupon which is necessary to decrypt the contents. Therefore, the functions intended in the present invention can be achieved when the added CCI according to the present invention is set to the mode "decrypt never," thus calling it "decrypt never CCI."

[37] FIG. 4 is a flowchart showing an exemplary embodiment of a method of decrypting the encrypted data by using the "decrypt never CCI."

[38] First, the "decrypt never CCI" stored in an information storage medium is read out (S100). Then, it is determined if the "decrypt never CCI" is set to the mode "decrypt
free" (S110). If the “decrypt never CCI” is set to the mode “decrypt free,” a decryptable condition exists and the encrypted data are decrypted (S160).

[39] If the “decrypt never CCI” is set to the mode “decrypt never,” an undecryptable condition exists and the value of the “decrypt never CCI” is changed by using a decryption coupon in the decryption device (S150).

[40] If the decryption coupon is not stored in the decryption device, a procedure for acquiring the decryption coupon is initiated (S120). The decryption coupon can be acquired by purchasing and downloading it from a decryption coupon selling server, reading it out from an information storage medium storing the decryption coupon, or buying it at a contents shop 120 shown in FIG. 2 and then inputting it to the decryption device.

[41] Also, the decryption coupon can be created by encrypting a CCI ID (copy control information identification). In this case, the decryption coupon is referred to as a “CCI coupon.”

[42] FIG. 5 is a CCI ID table showing an exemplary embodiment of the CCI ID.

[43] The CCI ID is a combination of characters and numbers. The CCI ID includes the “decrypt never CCI,” and particularly in FIG. 5, the last symbol of the CCI ID represents the “decrypt never CCI.”

[44] Therefore, the CCI IDS in FIG. 5 are same for the same AV contents except portions representing the “decrypted never CCI.”

[45] Security of data encryption can be further increased if the decryption coupon is decrypted and complex processes are needed to obtain a key during the step of obtaining the CCI ID. For this purpose, information uniquely given to each disc can be used during an encryption step, or information uniquely given to each device can be used. In this case, the scheme using the information uniquely given to each disc is referred to as a “disc binding” scheme, and the scheme using the information uniquely given to each device is referred to as a “device binding” scheme. In addition, information uniquely given to each user can be also used.

[46] The information uniquely given to each disc includes a disc ID or a disc key, and the information uniquely given to each device includes a device ID. In addition, the information given to each user includes a user’s public key used in a public key algorithm.

[47] FIG. 6 shows an exemplary embodiment of a method of purchasing an encrypted CCI coupon by using both the disc and device binding schemes.

[48] A result of an exclusive OR operation for the disc ID, the disc key, the device ID,
and the user’s public key is used as an encryption key (S200). In this case, the CCI coupon can be decrypted only when the disc having the disc information used for the encryption and the device having the device information used for the encryption are used.

[49] FIG. 7 shows an exemplary embodiment of a method of purchasing an encrypted CCI coupon by using only the “disc binding” scheme.

[50] When only the “disc binding” scheme is used, a result of an exclusive OR operation for the disc ID, the disc key, and the user’s public key is used as an encryption key (S210). In this case, the CCI coupon can be decrypted only when the disc having the disc information used for the encryption is used.

[51] FIG. 8 shows an exemplary embodiment of a method of purchasing an encrypted CCI coupon by using only the “device binding” scheme.

[52] When only the “device binding” scheme is used, a result of an exclusive OR operation for the device ID and the user’s public key is used as an encryption key (S220). In this case, the CCI coupon can be decrypted only when the device having the device ID used for the encryption is used.

[53] FIG. 9 shows an exemplary embodiment of a method of purchasing an encrypted CCI coupon by using only the user’s public key.

[54] When the CCI coupon is encrypted by using only the user’s public key (S230), the user can decrypt the CCI coupon by using the user’s own secret key.

[55] Referring to FIG. 4, a method of changing the value of the “decrypt never CCI” by using a decryption coupon will be described as follows.

[56] In order to obtain the CCI ID, the CCI coupon is decrypted (S130). At this point, the key used for the decryption is an encryption key used to create the coupon or the corresponding decryption key. The information used for creating the encryption key is also used for creating the decryption key.

[57] The CCI ID obtained by decrypting the CCI coupon is compared with the CCI ID included in the encrypted data (S140). If corresponding portions of both CCI IDs, i.e., the portions except for the “decrypt never CCI,” are the same, the “decrypt never CCI” value is changed into “decrypt free” (S150), and the encrypted data are decrypted (S160).

[58] If the corresponding portions of both CCI IDs are not the same, the data cannot be decrypted because the CCI coupon is not appropriate.

[59] Now, a new business model using the “decrypt never CCI” will be described.

[60] FIG. 10 shows an exemplary embodiment of a method of providing contents by
using the “decrypt never CCI.”

[61] A contents provider 100 or distributor 110 provides encrypted contents, of which “decrypt never CCI” is set to the mode “decrypt never,” to users for free (S300). Conventionally, the selling items are the encrypted contents not a “decryption coupon.” On the contrary, according to the present invention, the data having the “decrypt never CCI” are not necessary to be paid when the data is provided.

[62] The contents may be transmitted to users by broadcasting, the Internet, or discs. Even if the users are provided with the contents for free, they can not reproduce the contents. In other words, when a user is attempting to reproduce them, the reproducing device requires the decryption coupon to be downloaded or input by the user, or a disc storing the coupon to be inserted.

[63] In this case, in order to purchase the decryption coupon, the user may get an access to a decryption coupon selling server through a user’s interface provided by the reproducing device. Also, the user may purchase the decryption coupon or a disc storing the coupon at a contents shop 120 (S310).

[64] This will provide following marketing advantages. If a user has the encrypted contents in advance, she/he has a strong impulse to know what the contents are. In other words, a user has a stronger impulse to purchase a decryption coupon when she/he already possesses the contents that has not been decrypted than to purchase the contents that has not been encrypted in advance.

[65] In addition, different contents can be encrypted according to user’s levels, and coupons corresponding to the levels can be issued.

[66] FIG. 11 shows an exemplary embodiment of a method of providing contents when the coupon is provided according to user’s levels.

[67] A contents provider 100 or distributor 110 provides the encrypted contents, of which “decrypt never CCI” is set to the mode “decrypt never,” to users for free. In this case, the encrypted contents include a plurality of CCI IDs and the “decrypt never CCI” corresponding to each CCI ID.

[68] If a user purchases a coupon having an access limitation up to 2nd secret level, only the corresponding “decrypt never CCI” is allowed to be changed into the mode “decrypt free.” In this case, the user cannot reproduce the portions set to 1st secret level. Particularly, this can be useful when limitedly accessible contents are provided to persons under a certain age. For example, if the contents are made into two versions: a juvenile inhibited version and a juvenile admitted version, the “decrypt never CCI” can be differently set for different versions, so that the decryption can be easily
controlled.

[69] In addition, if an access needs to be controlled only for a part of the contents (this case is called “walled garden”), conventionally, different keys are used to control accesses for different contents. However, there may be problems in the key management. In this case, “decrypt never CCI” of the present invention will make it possible to implement an access control effectively.

[70] The present invention can be applied to all kinds of digital appliances for storing and/or reproducing AV data streams.

[71] The present invention can be implemented as computer readable codes stored in a computer readable recording medium. The computer includes all kinds of data processing devices, particularly including user’s terminals. The computer readable recording medium includes all kinds of recording devices storing computer readable data, such as ROMs, RAMs, flash memories, magnetic storages including floppy discs, hard discs, and magnetic tapes, optical storage media including CD-ROMs and DVDs, and carrier waves including the internet transmission.

[72] Exemplary embodiments of the present invention are disclosed in the drawings and the specification, as described above. In addition, although specific terms have been used hereto, the terms are intended to explain the present invention, but not intended to limit a meaning or restricting the scope of the present invention written in the following claims. Accordingly, it will be understood by those of ordinary skill in the art that various changes in form and details may be made therein without departing from the spirit and scope of the present invention as defined by the following claims.
Claims

1. A method of decrypting encrypted data comprising:
   (a) reading out decryption control information on decryptability of the encrypted data from an information storage medium; and
   (b) changing a condition of the decryption control information into a decryptable condition by using a decryption coupon stored in a decryption device if the decryption control information indicates an undecryptable condition.

2. The method according to claim 1, wherein the decryption control information is established in copy control information.

3. The method according to claim 1, further comprising
   (c) if the decryption coupon is not stored in the decryption device, accessing a decryption coupon selling server, purchasing the decryption coupon, and storing the decryption coupon in the decryption device.

4. The method according to claim 1, further comprising
   (c) if the decryption coupon is not stored in the decryption device, receiving a user’s input for the decryption coupon and storing the decryption coupon in the decryption device.

5. The method according to claim 1, further comprising
   (c) if the decryption coupon is not stored in the decryption device, reading out the decryption coupon from the information storage medium and storing the decryption coupon in the decryption device.

6. The method according to claim 1, wherein the encrypted data includes encrypted digital contents.

7. The method according to claim 1, wherein the decryption coupon is created by encrypting a copy control information identification uniquely given to the encrypted data by using a predetermined encryption key.

8. The method according to claim 7, wherein the copy control information identification is a combination of characters and numbers.

9. The method according to claim 8, wherein a last symbol of the copy control information identification is a number representing the decryption control information.

10. The method according to claim 7, wherein the predetermined encryption key is created by applying an exclusive OR operation for a medium identification uniquely given to the information storage medium, a medium key uniquely given
to the information storage medium, and a device identification uniquely given to the
decryption device.
11. The method according to claim 7, wherein the predetermined encryption key
is a user's public key uniquely given to the user.
12. The method according to claim 7, wherein the predetermined encryption key
is created by applying an exclusive OR operation for a device identification
uniquely given to the decryption device and a user's public key uniquely given to
the user.
13. The method according to claim 7, wherein the predetermined encryption key
is created by applying an exclusive OR operation for a medium identification
uniquely given to the information storage medium, a medium key uniquely given
to the information storage medium, and a user's public key uniquely given to the
user.
14. The method according to claim 1, wherein (b) comprises:
(b-1) decrypting the decryption coupon to obtain a copy control information
identification;
(b-2) comparing the decrypted copy control information identification and a
copy control information identification included in the encrypted data; and
(b-3) changing a condition of the decryption control information into a decryptable condition if corresponding portions of both the copy control in-
formation identifications are the same.
15. An apparatus for decrypting encrypted data comprising:
a reader which reads out encrypted data and decryption control information on
decryptability of the encrypted data from an information storage medium;
a coupon storage unit which stores a decryption coupon for the encrypted data;
a decryption information changing unit which changes a condition of the
decryption control information into a decryptable condition by using the
decryption coupon stored in the coupon storage unit if the decryption control in-
formation indicates an undecryptable condition; and
a data decryption unit which decrypts the encrypted data if the decryption control information indicates a decryptable condition.
16. The apparatus according to claim 15, wherein the decryption control in-
formation is established in copy control information.
17. The apparatus according to claim 15, further comprising
a coupon purchasing unit which, if the decryption coupon is not stored in the
coupon storage unit, accesses a decryption coupon selling server, purchases the
decryption coupon, and stores the decryption coupon in the coupon storage unit.
18. The apparatus according to claim 15, further comprising
a coupon input unit which, if the decryption coupon is not stored in the coupon
storage unit, receives a user’s input for the decryption coupon and stores the
decryption coupon in the coupon storage unit.
19. The apparatus according to claim 15, wherein the reader comprises a coupon
reader which, if the decryption coupon is not stored in the coupon storage unit,
reads out the decryption coupon from the information storage medium and stores
the decryption coupon in the coupon storage unit.
20. The apparatus according to claim 15, wherein the encrypted data includes
encrypted digital contents.
21. The apparatus according to claim 15, wherein the decryption coupon is
created by encrypting a copy control information identification uniquely given to
the encrypted data by using a predetermined encryption key.
22. The apparatus according to claim 21, wherein the copy control information
identification is a combination of characters and numbers.
23. The apparatus according to claim 22, wherein a last symbol of the copy
control information identification is a number representing the decryption control
information.
24. The apparatus according to claim 21, wherein the predetermined encryption
key is created by applying an exclusive OR operation for a medium identification uniquely given to the information storage medium, a medium key uniquely given to the information storage medium, and a device identification uniquely given to the decryption device.
25. The apparatus according to claim 21, wherein the predetermined encryption
key is a user’s public key uniquely given to the user.
26. The apparatus according to claim 21, wherein the predetermined encryption
key is created by applying an exclusive OR operation for a device identification uniquely given to the decryption device and a user’s public key uniquely given to the user.
27. The apparatus according to claim 21, wherein the predetermined encryption
key is created by applying an exclusive OR operation for a medium identification uniquely given to the information storage unit, a medium key uniquely given to the information storage medium, and a user’s public key uniquely given
to the user.

28. The apparatus according to claim 15, wherein the decryption information changing unit comprises:
a coupon decryption unit which decrypts the decryption coupon to obtain a copy control information identification; and
a copy control information identification comparator unit which compares the decrypted copy control information identification with a copy control information identification included in the encrypted data and changes a condition of the decryption control information into a decryptable condition if corresponding portions of both the copy control information identifications are the same.

29. A computer readable recording medium which stores a program for implementing:
reading out decryption control information representing decryptability of encrypted data from an information storage medium; and
changing a condition of the decryption control information into a decryptable condition by using a decryption coupon stored in a decryption device if the decryption control information indicates an undecryptable condition.

30. Audio/video (AV) data including copy control information, wherein the AV data comprises:
first copy control information representing an encryption condition and copyability of the AV data; and
second copy control information representing encryptability of the AV data.

31. The audio/video data according to claim 30, wherein the first copy control information represents one of:
a first mode which indicates that the AV data are not encrypted and freely copyable;
a second mode which indicates that the AV data are encrypted and freely copyable;
a third mode which indicates that the AV data are encrypted and one-time copyable; and
a fourth mode which indicates that the AV data are encrypted and uncopiable.

32. The audio/video data according to claim 30, where the second copy control information represents one of:
a first mode in which the AV data are decryptable; and
a second mode in which the AV data are undecryptable.

33. The audio/video data according to claim 32, wherein in the second mode, a device by which the AV data is to be reproduced decrypts the AV data using a predetermined decryption key and a decryption coupon for changing a condition of the second copy control information into the first mode.
FIG. 1

<table>
<thead>
<tr>
<th>COPY CONTROL INFORMATION</th>
<th>DECRYPTION CONDITION</th>
<th>COPYABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>00  COPY FREE</td>
<td>NOT ENCRYPTED</td>
<td>UNRESTRICTEDLY COPYABLE</td>
</tr>
<tr>
<td>01  COPY FREE BUT ENCRYPTED</td>
<td>ENCRYPTED</td>
<td>UNRESTRICTEDLY COPYABLE</td>
</tr>
<tr>
<td>10  COPY ONE GENERATION</td>
<td>ENCRYPTED</td>
<td>ONE-TIME COPYABLE</td>
</tr>
<tr>
<td>11  COPY NEVER (OR NO MORE COPY)</td>
<td>ENCRYPTED</td>
<td>UNCOPYABLE</td>
</tr>
</tbody>
</table>
FIG. 3

<table>
<thead>
<tr>
<th>DECRYPT NEVER CCI</th>
<th>ENCRYPTION KEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>DECRYPT FREE</td>
</tr>
<tr>
<td>01</td>
<td>DECRYPT NEVER</td>
</tr>
<tr>
<td></td>
<td>ONLY ENCRYPTION KEY</td>
</tr>
<tr>
<td></td>
<td>ENCRYPTION KEY AND DECRIPTION COUPON</td>
</tr>
</tbody>
</table>

FIG. 4

START

READ "DECRYPT NEVER CCI" S100

DECRIPTABLE? S110

YES

NO

OBTAIN DECRIPTION COUPON S120

DECRIPT DECRIPTION COUPON S130

DECRIPTED CCI ID = CCI ID INCLUDED IN DATA? S140

YES

CHANGE "DECRYPT NEVER CCI" S150

NO

DECRIPT ENCRYPTED DATA S160

END
### FIG. 5

<table>
<thead>
<tr>
<th>AV CONTENTS</th>
<th>&quot;DECRYPT NEVER CCI&quot; CODE</th>
<th>CCI ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;THE LORD OF THE RINGS&quot; PART 1 DVD</td>
<td>00 DECRIPT FREE</td>
<td>4c4c5c00-fe1e-11d0-ad87-010</td>
</tr>
<tr>
<td></td>
<td>01 DECRIPT NEVER</td>
<td>4c4c5c00-fe1e-11d0-ad87-011</td>
</tr>
<tr>
<td>&quot;THE LORD OF THE RINGS&quot; PART 2 DVD</td>
<td>00 DECRIPT FREE</td>
<td>7c3c56d0-fe1e-11d0-ad87-020</td>
</tr>
<tr>
<td></td>
<td>01 DECRIPT NEVER</td>
<td>7c3c56d0-fe1e-11d0-ad87-021</td>
</tr>
<tr>
<td>&quot;THE LORD OF THE RINGS&quot; PART 3 DVD</td>
<td>00 DECRIPT FREE</td>
<td>4c4c5c00-fe1e-11d0-ad87-030</td>
</tr>
<tr>
<td></td>
<td>01 DECRIPT NEVER</td>
<td>4c4c5c00-fe1e-11d0-ad87-031</td>
</tr>
<tr>
<td>&quot;THE LORD OF THE RINGS&quot; PART 4 DVD</td>
<td>00 DECRIPT FREE</td>
<td>7c3c56d0-fe1e-11d0-ad87-040</td>
</tr>
<tr>
<td></td>
<td>01 DECRIPT NEVER</td>
<td>7c3c56d0-fe1e-11d0-ad87-041</td>
</tr>
</tbody>
</table>

### FIG. 6

ENCRYPT CCI ID BY APPLYING XOR OPERATION FOR DISC ID, DISC KEY, DEVICE ID, AND USER'S PUBLIC KEY (S200)
FIG. 7

CONTENTS SHOP

ENCRYPT CCI ID BY APPLYING XOR OPERATION FOR DISC ID, DISC KEY, AND USER'S PUBLIC KEY (S210)

DISC ID

CCI COUPON

USER

FIG. 8

CONTENTS SHOP

ENCRYPT CCI ID BY APPLYING XOR OPERATION FOR DEVICE ID AND USER'S PUBLIC KEY (S220)

DEVICE ID

CCI COUPON

USER
INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2004/003202

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L 9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7 G06F 13/00, G11B 20/00, H04L 9/00 32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

search terms: copy control Information, encryption, decryption, public key, coupon

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>US 20020169973 A 14 Nov. 2002 (LG Electronics Inc.) claims 1-12</td>
<td>1, 15, 19</td>
</tr>
<tr>
<td>Y</td>
<td>EP 1067540 A2 10 Jan. 2001 (Pioneer Corp.) claims 1, 4</td>
<td>1, 15, 19</td>
</tr>
<tr>
<td>A</td>
<td>EP 1365339 A2 26 Nov. 2003 (NTT DoCoMo Inc.) claims 1-3, 20, 25, 26</td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>JP 2001-351519 A 21 Dec. 2001 (Pioneer Corp.) claims 1, 4, 11, 15</td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>EP 1126453 A2 22 Aug. 2001 (Matsushita Electric Industrial Co.) claims 1, 5</td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>A JP 1999-176091 A 2 July 1999 (Hitachi Ltd.) claims 1, 14, 24, 34</td>
<td>1</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.

[T] later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

[X] document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

[Y] document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

[&] document member of the same patent family

Date of the actual completion of the international search

25 FEBRUARY 2005 (25.02.2005)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701
Republic of Korea

Facsimile No. 82-42-472-7140

Date of mailing of the international search report

25 FEBRUARY 2005 (25.02.2005)

Authorized officer

JEONG, Jae Woo

Telephone No. 82-42-481-5718

Form PCT/ISA/210 (second sheet) (January 2004)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>JP 2003 337894 A</td>
<td>26 Nov. 2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 20040153422 A1</td>
<td>5 Aug. 2004</td>
</tr>
</tbody>
</table>