

**PLAYBACK MANAGEMENT DEVICE, PLAYBACK MANAGEMENT METHOD,
PLAYBACK MANAGEMENT PROGRAM, CONTENT RECEIVING SYSTEM,
AND CONTENT DISTRIBUTION SYSTEM**

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0001] The present invention relates to a playback management device, a playback management method, a playback management program, a content receiving system, and a content distribution system with a view to effectuating playback management of encoded contents.

DESCRIPTION OF THE PRIOR ART

[0002] It is a current trend to distribute content signals from broadcast stations and then play the content signals with an electronic machine, such as a smartphone, a personal computer, and a TV set. The content signals are encoded and distributed so as to protect distribution-related interests of a content distributor engaged in a paid broadcast service. In this regard, only those users which entered into a contract with the content distributor can decode the content signals and thereby watch the contents.

[0003] In the situation where content signals are encoded and distributed, typical measures taken to increase subscribers involve allowing viewers who have not entered into a contract with the content distributor to watch the contents for a short period of time, that is, see previews of the contents. To effectuate a

preview, it is necessary to output a key which decodes encoded content signals for a specified period of preview time.

Prior Art Document

[Citation Document]

[0004] [Citation 1] Japanese Unexamined Patent Application Publication No. 2011-216941.

[Citation 2] Japanese Unexamined Patent Application Publication No. 11-308595.

SUMMARY OF THE INVENTION

[Problem]

[0005] When a decoding key is output inadvertently, There is a high probability that the decoding key will be improperly used. To perform time management correctly, it is necessary to provide a tamper-resistant time source with a high cost.

[0006] In view of the aforesaid drawback of the prior art, it is the objective of the present invention to provide a playback management device, a playback management method, a playback management program, a content receiving system, and a content distribution system with a view to effectuating a preview with a high degree of security and a low cost.

[Solution]

[0007] The present invention provides, in an embodiment thereof, a playback management device for use with a receiver for receiving a content signal encoded by a key updated in a fixed update period and first control information obtained by encoding information about the key and a playable time for the encoded content

signal, wherein the playback management device comprises: a memory portion for storing the fixed update period in advance; an interface for collecting the first control information from the receiver; a first decoding portion for decoding the first control information and thereby restoring the key and the playable time for the encoded content signal; and a control portion for determining, according to the playable time for the encoded content signal and the fixed update period stored in the memory portion, whether to output the key to the receiver, and outputting the restored key to the receiver when determining to output.

The playable time can be a period of time for which the encoded content signal is played without a contract of playing the encoded content signal. That is the playable time can be a preview time.

[0008] The control portion outputs the key for a number of times corresponding to a ratio of the playable time to the fixed update period.

[0009] The playback management device is an IC chip or an IC card inserted into the receiver.

[0010] The present invention provides, in an embodiment thereof, a content receiving system, comprising: the playback management device; and a receiver for receiving the encoded content signal and the first control information; wherein when the receiver forwards the first control information to the playback management device and collects the key from the playback management device, the receiver uses the key to decode the encoded content signal.

[0011] The present invention provides, in an embodiment thereof, a playback management method, comprising steps performed by a playback management device for use with a receiver, the receiver being adapted to receive a content signal encoded by a key updated in a fixed update period and first control

information obtained by encoding information about the key and a playable time for the encoded content signal, the playback management method comprising the steps of: collecting the first control information from the receiver; decoding the first control information and restoring information about the key and the playable time for the encoded content signal; determining, according to the playable time for the encoded content signal and the fixed update period stored in a memory portion of the playback management device, whether to output the key to the receiver; and outputting the restored key to the receiver when determining to output.

[0012] The present invention provides, in an embodiment thereof, a playback management program, making a playback management device be used with a receiver to function as means described below, the receiver being adapted to receive a content signal encoded by a key updated in a fixed update period and first control information obtained by encoding information about the key and a playable time for the encoded content signal, means for collecting the first control information from the receiver; means for decoding the first control information and restoring information about the key and the playable time for the encoded content signal; means for determining, according to the playable time for the encoded content signal and the fixed update period stored in a memory portion of the playback management device, whether to output the key to the receiver; and means for outputting the restored key to the receiver when determining to output.

[0013] The present invention provides, in an embodiment thereof, a content distribution system, comprising: a broadcast device; a receiver; an IC card inserted into the receiver; and a playback device not having a tuner for processing a broadcast wave from the broadcast device, wherein the broadcast device has: a first encoding portion (11) for encoding a content signal by a first key (Ks) updated

in a fixed update period (T_{ud}) to generate an encoded content signal; a second encoding portion (12) for encoding, by a second key (K_w), the first key (K_s) and information about a playable time (T_{pre}) for the first key (K_s) to generate first control information entitlement control message (ECM); and a third encoding portion (14) for encoding the second key (K_w) by a third key (K_m) intrinsically configured in the IC card to generate second control information entitlement management message (EMM); wherein the encoded content signal, the first control information ECM and the second control information EMM are transmitted to the receiver by a broadcast wave, wherein the receiver has: a tuner (21) for processing the encoded content signal and the first control information ECM; and a first decoding portion (22) for decoding, when the IC card outputs the first key (K_s), the encoded content signal and thereby restoring the content signal; wherein the restored content signal is played by the playback device, wherein the IC card offers more security than the receiver, and the IC card has: a memory portion for storing data about the update period in advance; a second decoding portion (32) for receiving the second control information EMM through the receiver, decoding the second control information EMM by the third key (K_m) of the IC card, and thereby restoring the second key (K_w); a third decoding portion (34) for receiving the first control information ECM through the receiver, decoding the first control information ECM by the restored second key (K_w), and thereby restoring the first key (K_s) and the playable time for the first key (K_s); and a control portion (35) for outputting the first key (K_s) for a number of times corresponding to a ratio of the playable time (T_{pre}) to the update period (T_{ud}) stored in the memory portion in advance.

[Advantage of the Invention]

[0014] The playback management device of the present invention determines whether to output a key, thereby attaining a high degree of security and effectuating a preview at a low cost.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] FIG. 1 is a block diagram of a schematic structure of a content distribution system according to an embodiment of the present invention;

FIG. 2 is a block diagram of an internal structure of a broadcast device 1 according to the embodiment of the present invention;

FIG. 3 is a block diagram of an internal structure of a receiver 2 according to the embodiment of the present invention;

FIG. 4 is a block diagram of an internal structure of an IC card 3 according to the embodiment of the present invention;

FIG. 5 is a schematic view of how to output a key Ks from a control portion 35 of the IC card 3; and

FIG. 6 is a schematic view of the process flow of operation of the content distribution system according to the embodiment of the present invention.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0016] The embodiment of the present invention is hereunder illustrated by drawings and described in detail.

[0017] FIG. 1 is a block diagram of a schematic structure of a content distribution system according to an embodiment of the present invention. The content distribution system comprises a broadcast device 1, a receiver 2, an IC

card (playback management device) 3, and a playback device 4. The diagram shows one receiver 2, one IC card 3, and one playback device 4; however, they are usually provided in a plural number, so is the broadcast device 1. The receiver 2 and the IC card 3 together constitute a content receiving system.

[0018] The broadcast device 1 is, for example, provided in a broadcast station to transmit, by a broadcast wave, an encoded content signal as well as control information ECM (entitlement control message), EMM (entitlement management message) to be described later.

The receiver 2 is operated by a user and receives the content signal and the control information ECM, EMM and forwards the control information ECM, EMM to the IC card 3.

The user inserts the IC card 3 into the receiver 2 to transmit to the receiver 2, when a specified criterion is met, a key Ks (scrambling key) for decoding the encoded content signal. As soon as the receiver 2 receives the key Ks, the encoded content signal is decoded by the key Ks. The decoded content signal is played by the playback device 4.

[0019] In an embodiment, the receiver 2 is a dongle, whereas the playback device 4 is a smartphone connected to the dongle. Given the aforesaid structure, even though the smartphone is not equipped with any tuner and thus is unable to process a broadcast wave, the user may still use the smartphone to receive content signals. In an embodiment, the receiver 2 is a set top box, whereas the playback device 4 is a display unit connected to the set top box by an HDMI ® cable. Alternatively, the receiver 2 is built in the playback device 4. Alternatively, a playback management device equivalent to the IC card 3 functions as an IC chip and is mounted inside the receiver 2.

[0020] The IC card 3 must be a high-security module which offers more security than the receiver 2 and thus is effective in stopping improper access from the outside. To this end, the either IC card 3 only needs to be tamper-resistance, or the playback management device equivalent to the IC card 3 is mounted within a tamper-resistance area of a portion of a universal processor.

[0021] The present invention is hereunder described in detail. A contract must be specified in order for the encoded content signal to be played. However, a preview effectuated without a contract is described below.

FIG. 2 is a block diagram of the broadcast device 1 according to the embodiment of the present invention. The broadcast device 1 has a scrambler 11 (encoding portion), an encoding portion 12, a memory portion 13, and an encoding portion 14.

[0022] The scrambler 11 scrambles (encodes) a content signal by a key K_s . The content signal is, for example, a video signal and an audio signal. The encoded content signal thus generated will not be played unless by the key K_s . The key K_s is in the possession of the broadcast device 1. At a receiving end, the receivers 2 are not different and neither are the content signals. The key K_s is updated in a specified update period T_{ud} . Alternatively, the update period T_{ud} is set by the broadcast device 1 or is a predetermined fixed value.

[0023] The encoding portion 12 uses a key K_w (operating key) to encode information about the key K_s and the preview time T_{pre} and thereby generate control information ECM. At the preview time T_{pre} a content signal is played without a contract of playing the content signal, and the preview time T_{pre} is predetermined according to the content signal. Therefore, the control information ECM varies with each content signal.

[0024] The memory portion 13 stores a key K_m (main key) corresponding to each IC card 3. Hence, each IC card 3 has the intrinsically configured key K_m , and the memory portion 13 “remembers” which IC card 3 has which key K_m . The memory portion 13 also stores data about contract information related to the users of the IC cards 3. The contract information shows whether a contract of playing the encoded content signal has been entered into.

[0025] Like the memory portion 13, the encoding portion 14 uses the key K_m of the IC card 3 of a target of transmission to encode the key K_w and the contract information and thereby generate the control information EMM for use by the specific IC card 3.

[0026] The encoded content signal and the control information ECM, EMM are transmitted from the broadcast device 1 to the receiver 2 by a broadcast wave. The encoded content signal and the control information ECM are transmitted together, whereas the control information EMM can be transmitted at any time, for example, at a point in time when the contract information is changed. The control information EMM is for use by the receiver 2 which the specific IC card 3 is inserted into; hence, the control information EMM may also be transmitted by a means for providing communication to therefore save the bandwidth for transmission of the broadcast wave.

[0027] FIG. 3 is a block diagram of the receiver 2 according to the embodiment of the present invention. The receiver 2 has a tuner 21, an interface (IF) 22 in communication with the IC card 3, and a descrambler 23 (decoding portion).

[0028] The tuner 21 receives the encoded content signal and the control information ECM, EMM from the broadcast wave and chooses a channel according to the users' setting. The encoded content signal is supplied to the

descrambler 23, whereas the control information ECM, EMM is supplied to the interface 22.

[0029] The interface 22 forwards to the IC card 3 the control information ECM, EMM received from the broadcast device 1. The interface 22 collects the key Ks output from the IC card 3 and forwards the key Ks to the descrambler 23.

[0030] The descrambler 23 uses the key Ks to descramble (decode) the encoded content signal. That is to say, the descrambler 23 decodes the encoded content signal when the IC card 3 has output the key Ks. However, the descrambler 23 cannot descramble the encoded content signal when the IC card 3 has not output the key Ks. The descrambled content signal is converted into a video signal and/or an audio signal to be output to the playback device 4.

[0031] The receiver 2 will not be required to be capable of communication, provided that the control information EMM is transmitted by a broadcast wave.

[0032] FIG. 4 is a block diagram of the IC card 3 according to the embodiment of the present invention. The IC card 3 has an interface (IF) 31 in communication with the receiver 2, a decoding portion 32, a memory portion 33, a decoding portion 34, and a control portion 35. The IC card 3 is, for example, inserted into the receiver 2 to receive electric power from the receiver 2 in order to operate.

[0033] The interface 31 collects the control information ECM, EMM from the receiver 2. The interface 31 delivers the key Ks to the receiver 2 under a specified condition.

[0034] The decoding portion 32 decodes the control information EMM with the intrinsically configured key Km of the IC card 3 and thereby restores the key Kw and the contract information. Data about the key Kw and the contract information is stored in the memory portion 33. With the key Km being in the possession of

the IC card 3, the decoding portion 32 can decode the control information EMM within its reach, but cannot decode the control information EMM attributed to the other IC cards 3.

[0035] In addition to the key K_w and the contract information, the memory portion 33 stores data about the update period T_{ud} for the key K_s . When the update period T_{ud} is a fixed value, data about the update period T_{ud} is preconfigured and stored in the memory portion 33.

[0036] The decoding portion 34 decodes the control information ECM with the key K_w and thereby restores the key K_s and the preview time T_{pre} .

[0037] The control portion 35 determines whether to output the key K_s to the receiver 2 according to the contract information, the preview time T_{pre} , and the update period T_{ud} for the key K_s . If the contract information shows that a contract of playing the encoded content signal has been entered into, the control portion 35 will determine that the key K_s has to be output. If the contract information shows that the contract has not been entered into, the control portion 35 will effectuate a preview according to the preview time T_{pre} and the update period T_{ud} . Concretely, the control portion 35 determines that the key K_s has to be output, and the key K_s is output for a number of times equal to a ratio of the preview time T_{pre} to the update period T_{ud} . When the control portion 35 determines that the key K_s has to be output, the control portion 35 outputs the key K_s to the receiver 2 through the interface 31. The judgment made by the control portion 35 in a preview is described in detail below.

[0038] FIG. 5 is a schematic view of how to output the key K_s from the control portion 35 of the IC card 3. Unless otherwise specified, the description below ignores delays caused by decoding and data receiving/transmitting. Referring to

FIG. 5, given a preview time T_{pre} is 90 seconds and the update period T_{ud} for the key K_s is 30 seconds. Hence, the key K_s is updated thrice within the preview time T_{pre} , as $T_{pre}/T_{ud} = 3$. The key K_s to be updated successively are keys K_{s1} , K_{s2} , K_{s3} .

[0039] Referring to FIG. 5, at time t_1 , the receiver 2 received the encoded content signal and the control information ECM, and no key K_s has been output.

[0040] Therefore, at time t_1 , the control portion 35 outputs the key K_{s1} (first output). By this means, for the update period T_{ud} of 30 seconds, which starts from time t_1 and ends at time t_2 , the descrambler 23 of the receiver 2 can use the key K_{s1} to decode the encoded content signal. After time t_2 , since the key K_s has been updated, the descrambler 23 cannot use the key K_{s1} to decode the encoded content signal.

[0041] At time t_2 , the control portion 35 receives the control information ECM obtained by encoding the updated and new key K_{s2} . In consequence, the key K_s has been output only once. Hence, the control portion 35 outputs the key K_s to the receiver 2 (second output). By this means, for the update period T_{ud} of 30 seconds, which starts from time t_2 and ends at time t_3 , the descrambler 23 of the receiver 2 can use the key K_{s2} to decode the encoded content signal. After time t_3 , since the key K_s has been updated, the descrambler 23 cannot use the key K_{s2} to decode the encoded content signal.

[0042] At time t_3 , the control portion 35 receives the control information ECM obtained by encoding the updated and new key K_{s3} . In consequence, the key K_s has been output only twice. Hence, the control portion 35 outputs the key K_s to the receiver 2 (third output). By this means, for the update period T_{ud} of 30 seconds, which starts from time t_3 and ends at time t_4 , the descrambler 23 of the

receiver 2 can use the key Ks3 to decode the encoded content signal. After time t4, since the key Ks has been updated, the descrambler 23 cannot use the key Ks3 to decode the encoded content signal.

[0043] At time t4, the control portion 35 receives control information obtained by encoding the updated and new key Ks. Since, by time t4, the control portion 35 has output the key Ks thrice, the control portion 35 will no longer transmit the key Ks to the receiver 2. Therefore, after time t4, the descrambler 23 cannot decode the encoded content signal.

[0044] Accordingly, the encoded content signal is decoded and played for the 90 second preview time Tpre.

[0045] FIG. 6 is a schematic view of the process flow of operation of the content distribution system according to the embodiment of the present invention. The control information EMM has been transmitted to the receiver 2, and the memory portion 33 stores data about the key Kw. No contract of playing the encoded content signal was entered into.

[0046] The broadcast device 1 transmits the encoded content signal and the control information ECM to the receiver 2 by a broadcast wave (step S1). The control information ECM includes information about the encoded key Ks and the preview time Tpre.

The receiver 2 receives the encoded content signal and the control information ECM (step S11) and forwards the control information ECM to the IC card 3 (step S12).

[0047] The IC card 3 receives the control information ECM (step S21). Afterward, the decoding portion 34 of the IC card 3 uses the key Kw to decode the control information ECM (step S22) and thereby restore the key Ks and the

preview time T_{pre} . Then, the control portion 35 calculates the number N of times the key K_s is output according to the restored preview time T_{pre} and the update period T_{ud} stored in the memory portion 33 (step S23). The control portion 35 sees T_{pre}/T_{ud} as the number N of times. Afterward, the control portion 35 effectuates the first output of the key K_s (step S24).

[0048] The control portion 35 outputs the key K_s to the receiver 2 the number N of times and those outputs are done once every the update period T_{ud} (step S21~S25). That is to say that when the actual number of times of outputting the key K_s has not reached N ("No" in step S25), the decoding portion 34 receives the control information ECM after lapse of the update period T_{ud} from reception of a specific key K_s (for example, the key K_{s1} of FIG. 5) (step S21), and the decoding portion 34 decodes the control information ECM including the updated key K_s (for example, the key K_{s2} of FIG. 5) (step S22). Afterward, the control portion 35 outputs the restored key K_s to the receiver 2 (step S24).

[0049] When the descrambler 23 of the receiver 2 receives the key K_s (step S13), the descrambler 23 descrambles the encoded content signal (step S14). Before the key K_s is updated, that is, before lapse of the update period T_{ud} , the descrambler 23 can descramble the encoded content signal ("No" in step S15).

[0050] In case the key K_s has been updated after lapse of the update period T_{ud} ("Yes" in step S15), if the descrambler 23 receives the updated key K_s from the IC card 3 ("Yes" in step S13), the descrambler 23 will keep descrambling the encoded content signal (step S14). the key K_s is updated and If the updated key K_s is not transmitted from the IC card 3 ("No" in step S13), the descrambler 23 cannot descramble the encoded content signal.

[0051] In this embodiment, the IC card 3 is well informed of the update period T_{ud} , and thus the high-security IC card 3 is able to determine whether to output the key K_s . Afterward, the IC card 3 will output the key K_s to the receiver 2 only if the key K_s is determined to be output, thereby enhancing security. Hence, the manufacturing cost of the receiver 2 is reduced because the receiver 2 neither needs a high degree of security nor needs to manage a preview time.

[0052] In this embodiment, the update period T_{ud} is a fixed value, and the update period T_{ud} is stored in the memory portion 33 in advance. However, this embodiment will also work, provided that the IC card 3 is well informed of the update period T_{ud} . In addition to the fixed update period T_{ud} , considerations are given to variant embodiments.

[0053] For instance, the encoding portion 14 of FIG. 2 may encode the key K_w and information about the update period T_{ud} to generate the control information EMM. In this case, the decoding portion 32 of FIG. 4 may decode the control information EMM and thereby restore the update period T_{ud} . The restored update period T_{ud} is then stored in the memory portion 33.

[0054] For instance, the encoding portion 12 of FIG. 2 may encode information about the key K_s and preview time T_{pre} and information about the update period T_{ud} to generate the control information ECM. In this case the decoding portion 34 of FIG. 4 may decode the control information ECM and thereby restores the update period T_{ud} . The restored update period T_{ud} is then stored in the memory portion 33.

[0055] For instance, the encoding portion 12 of FIG. 2 may encode information about the key K_s and preview time T_{pre} and time information to generate the control information ECM. The time information is, for example, about the time at

which new key K_s is output from the broadcast device 1. Referring to FIG. 5, the encoding portion 12 generates control information ECM1 inclusive of key K_{s1} and time information t_1 . Afterward, the encoding portion 12 generates control information ECM2 inclusive of key K_{s2} and time information t_2 . In this case, the decoding portion 32 of FIG. 4 uses the time difference ($t_2 - t_1$) between the time information t_1 restored from the control information ECM1 and the time information t_2 restored from the control information ECM2 as the update period T_{ud} . Additionally, the decoding portion 32 of FIG. 4 stores the update period T_{ud} in the memory portion 33.

[0056] At least a portion of the content distribution system in the aforesaid embodiments may be hardware or software. If it is software, a program executable to perform a function of at least a portion of the content distribution system can be stored in a record medium, such as a floppy disk or CD-ROM, so as to be read and executed by a computer. The record medium is not restricted to a magnetic disk or an optical disc, which is removable and replaceable, but may also include a fixed record medium, such as a hard disk drive device or memory.

[0057] Moreover, the program executable to perform a function of at least a portion of the content distribution system can be distributed by a communication network (including a wireless network), such as the Internet. Furthermore, The program may also be encoded, modulated, or compressed and be distributed by a wireless network or a wired network, such as the Internet, or by being stored in a record medium.

[0058] Given the above description, persons skilled in the art may think of a supplemental effect or various variations of the present invention. However, the present invention is not restricted to the aforesaid embodiments. Various

supplements, changes, and partial deletions can be made to the present invention without departing from the scope and conceptual thoughts derived from technical features, and equivalents thereof, recited in the claims.

CLAIMS

1. A playback management device for use with a receiver for receiving a content signal encoded by a key updated in a fixed update period and first control information obtained by encoding information about the key and a playable time for the encoded content signal, wherein the playback management device comprises:
 - a memory portion for storing the fixed update period in advance;
 - an interface for collecting the first control information from the receiver;
 - a first decoding portion for decoding the first control information and thereby restoring the key and the playable time for the encoded content signal, wherein the playable time is a time period for which the encoded content signal is played without a contract of playing the encoded content signal; and
 - a control portion for determining, according to the playable time for the encoded content signal and the fixed update period stored in the memory portion, whether to output the key to the receiver, and outputting the restored key to the receiver when determining to output, wherein the control portion outputs the key for a number of times corresponding to a ratio of the playable time to the fixed update period.
2. The playback management device of claim 1, wherein a security of the playback management device is higher than a security of the receiver.
3. The playback management device of claim 1, wherein the playback management device is an IC chip or an IC card inserted into the receiver.
4. A content receiving system, comprising:

the playback management device of claim 1; and
a receiver for receiving the encoded content signal and the first control information;
wherein when the receiver forwards the first control information to the playback management device and collects the key from the playback management device, the receiver uses the key to decode the encoded content signal.

5. A playback management method, comprising steps performed by a playback management device for use with a receiver, the receiver being adapted to receive a content signal encoded by a key updated in a fixed update period and first control information obtained by encoding information about the key and a playable time for the encoded content signal, the playback management method comprising the steps of:

collecting the first control information from the receiver;

decoding the first control information and restoring information about the key and the playable time for the encoded content signal, wherein the playable time is a time period for which the encoded content signal is played without a contract of playing the encoded content signal;

determining, by a control portion according to the playable time for the encoded content signal and the fixed update period stored in a memory portion of the playback management device, whether to output the key to the receiver; and

outputting the restored key to the receiver when determining to output,

wherein the control portion outputs the key for a number of times corresponding to a ratio of the playable time to the fixed update period.