

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
11 October 2007 (11.10.2007)

PCT

(10) International Publication Number
WO 2007/113802 A2

(51) International Patent Classification:
G06F 21/24 (2006.01)

(21) International Application Number:
PCT/IL2007/000387

(22) International Filing Date: 25 March 2007 (25.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
174755 3 April 2006 (03.04.2006) IL
178213 20 September 2006 (20.09.2006) IL

(71) Applicant (for all designated States except US): **NDS LIMITED** [GB/GB]; One Heathrow Boulevard, 286 Bath Road, West Drayton Middlesex UB7 0DQ (GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SHEN-ORR, Chaim** [IL/IL]; 16 Kiryat Sefer Street, 34676 Haifa (IL). **HIBSHOOSH, Eliphaz** [IL/IL]; 5 Sirkin Street, 63562 Tel-aviv (IL). **BELENKY, Yaacov** [IL/IL]; 27/2 Hakinor Street, 98371 Maaleh Adumim (IL). **ICKOWICZ, Gabi** [IL/IL]; 41 HaAchoth Selma Street, Givat Mashua, 96401 Jerusalem (IL).

(74) Agents: **SANFORD T. COLB & CO.** et al.; P.O. Box 2273, 76122 Rehovot (IL).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

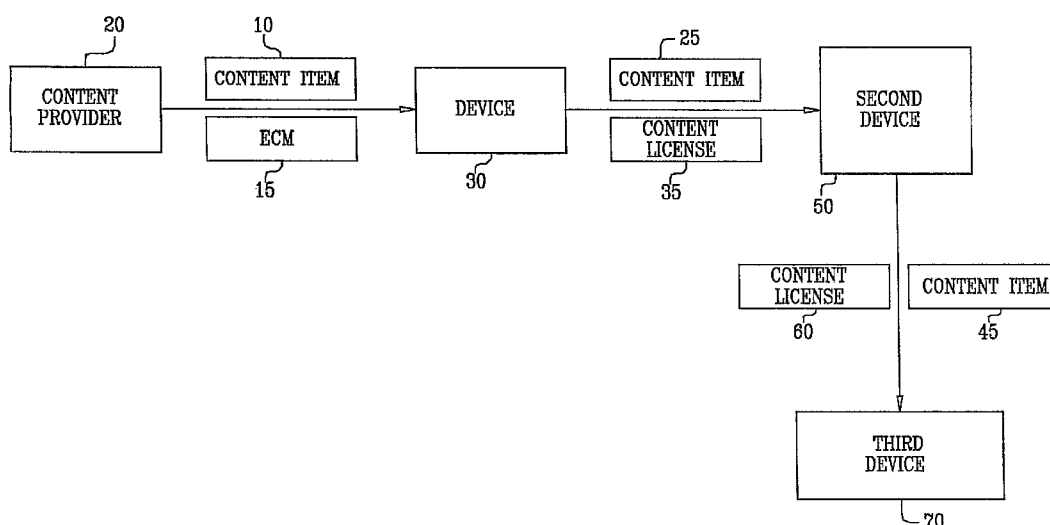
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, 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:

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

(54) Title: KEY MANAGEMENT SYSTEM



(57) Abstract: A key management method including receiving content scrambled with a first scrambling algorithm (FSA), determining whether to descramble the content according to a first rule and producing a first result, only if the first result indicates that the content should be descrambled, descrambling the content according to an FSA control word, determining whether to apply a second scrambling algorithm (SSA) according to a second rule and producing a second result, and only if the second result indicates that the SSA should be applied, applying the SSA, the applying the SSA including re-scrambling according to a SSA control word, wherein the FSA control word changes at an FSA control word change time, and the method also includes changing the SSA control word in lockstep fashion with the FSA control word, such that each change of the FSA control word causes a change of the SSA control word. Related methods and apparatus are also described.

WO 2007/113802 A2

KEY MANAGEMENT SYSTEM

FIELD OF THE INVENTION

The present invention relates to digital rights management and more particularly to a system for causing keys which need to be kept together to be kept together.

BACKGROUND OF THE INVENTION

In broadcast Pay TV system, Audio-Video (A/V) content – a channel or a single program (event) – is typically encrypted (i.e., protected by scrambling) with a set of broadcast keys (also referred to as “Control Words” or CWs), such that all receivers receive identical scrambled content. Access to scrambled content is restricted only to compliant receivers (also referred to as “Set Top Boxes”, STBs) specifically authorized to know the content’s CWs and thus able to descramble the content. The only thing that stands in the way of access to the broadcast protected content is its CWs set. The CW set may be acquired by a user pirating (or “hacking”) a single compromised receiver. Subsequent distribution of pirated keys is accomplished relatively simply via the Internet or other appropriate distribution media. Thus, pirated keys may be made available to receivers which accept the pirated keys and descramble and decode the encrypted content without proper authorization.

It is, therefore, a basic security guideline that broadcast content in a user domain storage or home network is always locally scrambled – encrypted by the user STB with a key generated locally, for example and without limiting the generality of the foregoing, by the user STB.

Preferably, a single local key is not used as the CW for an unlimited amount of time, nor for a large number of content items, as theft of the CW would therefore result in a very large reward. For example and without limiting the generality of the foregoing, if all content on a storage disk is always encrypted with a single constant local CW, theft of the local CW is highly attractive. Access to the local CW gives unlimited access to all of the content stored on the storage disk. Accordingly, another basic security guideline is postulated, such that the

applicability of the local CW is preferably restricted to a controlled set of finite content items.

Typically, a broadcast content item may be divided into more than one crypto-period, each crypto-period comprising a CW. Moreover, content usage rights such as access to the content item, and transfer and storage of the content (i.e. copy control rights, such as copy-freely or copy-never) are assigned to the content item. In general, the rights associated with the content item are synchronous with and have a maximum granularity of one crypto-period; i.e. the rights may at most change every crypto-period.

Typically, multiple content items are often concurrently processed for rights enforcements. It is thus crucial to preclude the possibility of swapping the rights assigned, for instance, to one movie with another. For example, a copy-never content right for movie-A should not be replaced with copy-free right of movie-B.

PCT patent application IL/03/00969, published in the English language on 21 October 2004 as WO 2004/091132 of NDS Ltd., describes a method for protecting digital content. The method includes receiving compressed encrypted digital content, determining an output format, based, at least in part, on all of the following: received control information; and a rule determining whether a clear compressed output format is allowed; and producing output from the compressed digital content based on a result of the determining, wherein, if the rule does not allow clear compressed output format, the compressed encrypted digital content is provided in a form which prevents production of clear compressed output in the producing step.

The disclosures of all references mentioned above and throughout the present specification, as well as the disclosures of all references mentioned in those references, are hereby incorporated herein by reference.

SUMMARY OF THE INVENTION

The present invention seeks to provide an improved method and system for a lock-step mechanism wherein local control words are changed every time when external control words, e.g., broadcast, are changed, in one indivisible atomic action.

Scrambled broadcast content is typically descrambled using its broadcast key and preferably immediately re-encrypted with a locally generated key by the receiver, in one atomic indivisible step. Thus, a user wishing to share decrypted content is forced to send both the locally-scrambled content and the set of local encryption keys (Local-CWs). Such high bandwidth transfer of A/V content is time-consuming, inconvenient and serves as an impediment to illegal content sharing.

Throughout the present specification and claims, a broadcast scrambling algorithm is referred to as an "External Scrambling Algorithm", ESA, and a local scrambling algorithm is referred to as a "Local Scrambling Algorithm", LSA. The ESA is also referred to herein as a First Scrambling Algorithm, FSA, and the LSA is also referred to herein as a Second Scrambling Algorithm, SSA. CWs corresponding to the ESA comprise ESA-CWs and CWs corresponding to the LSA comprise LSA-CWs. It is appreciated that external scrambling is typically "universal" scrambling; externally scrambled content reaches a plurality of devices with the same scrambling at each one of the plurality of devices. On the other hand, local scrambling varies, and is typically and preferably different at each one of the plurality of devices.

A particular ESA-CW is preferably securely bound to a LSA-CW for a given content item. Thus, the LSA-CW is preferably for a finite duration (the same duration as the ESA-CW). In preferred embodiments of the present invention, rights to use the content item, the ESA-CW and the LSA-CW are preferably bound together in a secure environment, thereby ensuring that the rights, the ESA-CW, and the LSA-CW stay together. Furthermore, swapping rights among different users is preferably more difficult according to the present invention in preferred embodiments thereof. It is also appreciated that changes in rights, as explained below, also preferably occur only in the secure environment.

When a content item initially arrives at the user's STB, the content item has its ESA-CWs and associated content usage rights. Arrival of a new ESA-CW typically is accompanied with a new set of ESA-CWs specifying a new set of content usage rights. Thus the change in ESA-CW may be used as secure signaling of an end of an event. The signal of the end of an event helps ensuring that a single LSA-CW is restricted to a single content item by a lock-step mechanism combining any change in ESA-CW with a corresponding LSA-CW change.

To prevent exchange of content rights among multiple content items, the ESA-CW and rights associated thereto are preferably bound to its corresponding LSA-CW and derived-rights. Absent such mechanism a pirate may be able to replace a highly restrictive set of rights with a more lenient set of rights.

Furthermore, when a locally scrambled content item (possibly a stored locally scrambled content item) is to be copied or transferred, the locally scrambled content item preferably undergoes re-encryption with LSA and a new locally generated key. In the case of copying or transferring a locally scrambled content item a coupling is accordingly established between LSA-CW1 and LSA-CW2.

There is thus provided in accordance with a preferred embodiment of the present invention a key management method including receiving content scrambled with a first scrambling algorithm (FSA), determining whether to descramble the content according to a first rule and producing a first result, only if the first result indicates that the content should be descrambled, descrambling the content according to an FSA control word, determining whether to apply a second scrambling algorithm (SSA) according to a second rule and producing a second result, and only if the second result indicates that the SSA should be applied, applying the SSA, the applying the SSA including re-scrambling according to a SSA control word, wherein the FSA control word changes at an FSA control word change time, and the method also includes changing the SSA control word in lockstep fashion with the FSA control word, such that each change of the FSA control word causes a change of the SSA control word.

Further in accordance with a preferred embodiment of the present invention the first rule includes an instruction to descramble the content according to the FSA control word.

5 Still further in accordance with a preferred embodiment of the present invention the first rule includes an instruction to not descramble the content.

Additionally in accordance with a preferred embodiment of the present invention the second rule includes an instruction to descramble the content according to the SSA control word.

10 Moreover in accordance with a preferred embodiment of the present invention and wherein the second rule includes an instruction to not descramble the content.

Further in accordance with a preferred embodiment of the present invention the changing of the SSA control word occurs in hardware.

15 Still further in accordance with a preferred embodiment of the present invention re-encrypted content is locally stored.

Additionally in accordance with a preferred embodiment of the present invention the first rule is included in a content license.

20 Moreover in accordance with a preferred embodiment of the present invention the second rule is included in a content license.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

5 Fig. 1 is a simplified block diagram illustration of a content item being transferred from a content provider to a content receiving device, from the content receiving device to a second content receiving device, and from the second content receiving device to a third content receiving device, the system of Fig. 1 being constructed and operative in accordance with a preferred embodiment of the
10 present invention;

 Fig. 2 is a simplified block diagram illustration of the content item of the system of Fig. 1, depicting the relationship between the content item and an external scrambling algorithm control word and a local scrambling algorithm control word;

15 Fig. 3 is a simplified block diagram illustration of a scrambled broadcast content item arriving at a device descrambler / scrambler module, and being locally scrambled, in an atomic, indivisible action; and

 Fig. 4 is a simplified flowchart illustration of a preferred method of operation of the system of Fig. 1, in accordance with preferred embodiments
20 thereof.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Reference is now made to Fig. 1, which is a simplified block diagram illustration of a content item 10 being transferred:

from a content provider 20 to a content receiving device 30;

5 from the content receiving device 30 to a second content receiving device 50; and

from the second content receiving device 50 to a third content receiving device 70, the system of Fig. 1 being constructed and operative in accordance with a preferred embodiment of the present invention.

10 The system of Fig. 1 comprises a plurality of devices, depicted as the content receiving device 30, the second content receiving device 50, and the third content receiving device 70. Additionally, the system of Fig. 1 also comprises a content item in various states, depicted as being transferred between the devices 30, 50, 70 comprising the plurality of devices. The relationship
15 between the different states of the content item is described below. The system of Fig. 1 further comprises an entitlement control message (ECM) 15, a first content license 35, and a second content license 60.

The content item in various states mentioned above, depicted as the content item 10, the content item 25 and the content item 45 typically comprises
20 the same content. However, as the content item 10, the content item 25 and the content item 45 are typically in various different states of encryption, or are in the clear. Therefore, it is likely that the content item 10, the content item 25 and the content item 45 comprise different strings of bits. Accordingly, the content item 10, the content item 25 and the content item 45, are depicted differently.

25 It is appreciated that different portions of the system of Fig. 1 comprise various sub-systems upon which the system and method of the present invention may apply. Specifically:

transferring the content item 10 and the ECM 15 from the content provider 20 to the content receiving device 30;

30 transferring the content item 25 and the first content license 35 from the content receiving device 30 to the second content receiving device 50; and

transferring the content item 45 and the second content license 45 from the second content receiving device 50 to the third content receiving device 70.

5 The operation of Fig. 1 is now explained, with reference to the discussions, below, of Fig. 2 and Fig. 3.

Reference is now made to Fig. 2, which is a simplified block diagram illustration of the content item 10, 25, 45 of the system of Fig. 1, depicting the relationship between the content item 10, 25, 45 and an external scrambling algorithm control word (ESA-CW) and a local scrambling algorithm control word (LSA-CW). Fig. 2 depicts the content item 10, 25, 45 comprised of a multiplicity of transport packets 110. The multiplicity of transport packets 110 is preferably subdivided over time into key periods, or crypto-periods, CP1, CP2, CP3, ..., CPn. Each key period CP1, CP2, CP3, ..., CPn preferably comprises a plurality of transport packets 110. Each key period CP1, CP2, CP3, ..., CPn is depicted as comprising an ESA-CW and a LSA-CW. Each one of the plurality of transport packets 110 are preferably thereby associated with both an ESA-CW and a LSA-CW. It is appreciated that each time the ESA-CW changes, the LSA-CW changes as well, in lock-step fashion.

It is also appreciated that in some embodiments of the present invention, either one of the ESA or the LSA may not always be applied during a given crypto-period on a given device. Typically, the content item 10, being delivered from an external content provider content provider 20 is ESA scrambled, and not LSA scrambled. Also typically, the content item 25, being delivered from the content receiving device content receiving device 30, is at least LSA scrambled, and may be either ESA scrambled or not, as will be described below. Nonetheless, as will be explained below in greater detail, rights to use the content, for example and without limiting the generality of the foregoing, unlimited consumption, limited consumption (such as: play once, play three times, etc.), time limited consumption (such as: play for one week, play for two weeks, etc.), and copying rights (such as: do not copy, copy once, unlimited copy, etc.) do not change from a less permissive state to a more permissive state as the content item content item 10, 25, and 45 is passed from the content provider 20 to the content

receiving device 30; from the content receiving device 30 to the second content receiving device 50; and from the second content receiving device 50 to the third content receiving device 70. For example and without limiting the generality of the foregoing, copying content which comprises a "copy once" right from a first device to a second device results in a change of rights from a more permissive state (copy once) to a less permissive state (do not copy).

Furthermore, as mentioned above, in cases where both the ESA and the LSA are applied together, either in a case of re-encryption, or in a case of super-encryption, the ESA-CW and the LSA-CW change at the same time, in lock-step fashion.

When the ESA-CW is sent from a content provider 20 (Fig. 1) to a receiving device 30 (Fig. 1), the ECM 15 preferably comprises information to generate the ESA-CW and also comprises content licensing and rights information. For example and without limiting the generality of the foregoing, content usage rights such as access to the content item, and transfer and storage of the content (i.e. copy control rights, such as copy-freely or copy-never) are assigned to the content item. In general, the rights associated with the content item are synchronous with and have maximum granularity of the crypto-periods; i.e., the rights may only change every crypto period.

When content is transferred from the content receiving device 30 (Fig. 1) to the second content receiving device 50 (Fig. 1), the content receiving device 30 (Fig. 1) preferably transfers the transport packets 110 (Fig. 2) of each key period comprising the content item 25 along with the first content license 35 comprising the LSA-CW associated with the key period comprising the transferred transport packets 110. It is further appreciated that the first content license 35 also comprises information controlling content usage rights in the receiving device 50 (Fig. 1). It is further appreciated that if external scrambling is also applied to the content item 25, in the case of super-encryption (discussed at length below), then the EAS_Cw is also preferably comprised in the first content license 35.

Reference is now made to Fig. 3, which is a simplified block diagram illustration of a scrambled broadcast content item 310 (corresponding to the content item 10 of Fig. 1) arriving at a device descrambler / scrambler module

320, and being locally scrambled, in an atomic, indivisible action. The scrambled broadcast content item 310 preferably arrives at the receiving device 30, 50, 70 (Fig. 1), and is preferably transferred to the descrambler / scrambler module 320 comprised therein. The descrambler / scrambler module 320 preferably is comprised in a single chip, so that it is preferably difficult to intercept data from inside the single chip. As is well known in the art, comprising the descrambler / scrambler module 320 in a single chip has the effect of making data comprised therein more secure than if actions on the data comprised therein were effected in several independent chips. The descrambler / scrambler module 320 preferably comprises a broadcast descrambler 330 and a local scrambler 350.

The scrambled broadcast content item 310 is preferably input into the broadcast descrambler 330. The broadcast descrambler 330 preferably utilizes the ESA-CW 340 in order to descramble the scrambled broadcast content item 310, thereby producing a descrambled broadcast content item. The descrambled broadcast content item is preferably input into the local scrambler 350. The local scrambler 350 preferably utilizes the LSA-CW 360 in order to scramble the descrambled broadcast content item, thereby producing a locally scrambled broadcast content item 370. The locally scrambled broadcast content item 370 may then preferably be sent to a local storage unit 380.

It is appreciated that in some preferred embodiment of the present invention, it is preferable for the descrambler / scrambler module 320 to also comprise a local descrambler (not depicted). For example and without limiting the generality of the foregoing, in cases where the content item 10 is transferred from one of:

the content receiving device 30 to a second content receiving device 50; and

the second content receiving device 50 to a third content receiving device 70,

the content item 10 may preferably be received at the second content receiving device 50 and the third content receiving device 70 scrambled according to the LSA. Accordingly, the only way such LSA scrambled content is useable would be if the LSA scrambled content item were to be descrambled.

Generation of the LSA-CW is now discussed. In advance of the start of a new key period CP1, CP2, CP3, ..., CPn (Fig. 2), the ECM 15 (Fig. 1) arrives at the content receiving device 30. Alternatively, the first content license 35 (Fig. 1) preferably arrives at the second content receiving device 50 along with the content item 25 (Fig. 1). An appropriate mechanism comprised in the content receiving device 30 such as, but not limited to a smart card, translates the ECM 15 (Fig. 1) into a content license comprising a content sequence license (CSL) and a base line ECM (BL-ECM).

The CSL preferably comprises rights and usage rules for content associated with the ECM 15 (Fig. 1). Examples of rights and usage rules were provided above. The CSL also comprises rules concerning applying LSA and ESA, described below as LSA-CW On/Off and ESA-CW On/Off.

The BL-ECM preferably comprises the LSA-CW and the ESA-CW. It is appreciated that where LSA or ESA are not applied, the BL-ECM preferably comprises filler bits in place of a valid LSA-CW or ESA-CW.

Appropriate software comprised in the content receiving device 30, the second content receiving device 50, and the third content receiving device 70 (Fig. 1) preferably delivers the ECM 15 to a processor, preferably a secure processor. The processor, based at least on information comprised in the CSL preferably determines what action the device 30, 50, 70 (Fig. 1) should take.

If the processor determines that the device 30, 50, 70 (Fig. 1) should render the content item 10, 25, 45, the device 30, 50, 70 (Fig. 1) then preferably renders the plurality of transport packets 110 (Fig. 2) comprising the content item 10, 25, 45 (Fig. 1), and preferably deletes each of the plurality of transport packets 110 (Fig. 2) after rendering.

If the processor determines that the device 30, 50, 70 (Fig. 1) should store the content item 10, 25, 45, the device 30, 50, 70 (Fig. 1) then preferably removes the ESA scrambling and re-encrypts the content with LSA scrambling. Alternatively, the device 30, 50, 70 (Fig. 1) then preferably super-encrypts the content, applying LSA scrambling to the already ESA scrambled content.

In the event of ESA descrambling and re-encryption of the content with LSA scrambling, the CSL and BL-ECM preferably together comprise the following information:

LSA-CW On/Off	LSA-CW	ESA-CW On/Off	ESA-CW
0	Filler Bits	1	ESA-CW

where:

- 5 LSA-CW On/Off indicates that the LSA-CW comprised in the BL-ECM does not comprise a valid control word, but rather comprises filler bits; and
 ESA-CW On/Off indicates that the ESA-CW comprised in the BL-ECM comprises a valid control word.

- 10 In such a case, a random number generator comprised in the processor preferably provides a new LSA-CW, thereby generating a new content license comprising the following information:

LSA-CW On/Off	LSA-CW	ESA-CW On/Off	ESA-CW
1	LSA-CW	0	Filler Bits

where:

- LSA-CW On/Off indicates that the LSA-CW comprised in the BL-ECM comprises a valid control word; and
 15 ESA-CW On/Off indicates that the ESA-CW comprised in the BL-ECM does not comprise a valid control word, but rather comprises filler bits. Thus, the processor preferably thereby generates the LSA-CW.

Additionally, the device preferably comprises a key table slot preferably comprising the following information:

LSA Decryption On/Off	LSA-CW	ESA Decryption On/Off	ESA-CW	LSA Encryption On/Off	LSA-CW

- 20 Thus, in the re-encryption case described above, the key table slot preferably comprises the following information:

LSA Decryption	LSA-CW	ESA Decryption	ESA-CW	LSA Encryption	LSA-CW

On/Off		On/Off		On/Off	
0	Filler Bits	1	ESA-CW	1	LSA-CW

Thereby enabling the device to reverse the re-encryption process, as needed.

It is appreciated that in certain preferred embodiments of the present invention, the different variations of the above table may be applied. For example and without limiting the generality of the foregoing, in the content receiving device 30 and the second content receiving device 50, the key table slot, in the re-encryption case may preferably comprise the following information:

LSA Decryption On/Off	LSA-CW	ESA Decryption On/Off	ESA-CW	LSA Encryption On/Off	LSA-CW
1	LSA-CW	1	ESA-CW	0	Filler Bits

In the event of super-encryption of the content with LSA scrambling, the CSL and BL-ECM preferably together comprise the following information:

LSA-CW On/Off	LSA-CW	ESA-CW On/Off	ESA-CW
0	Filler Bits	1	ESA-CW

10 where:

LSA-CW On/Off indicates that the LSA-CW comprised in the BL-ECM does not comprise a valid control word, but rather comprises filler bits; and
ESA-CW On/Off indicates that the ESA-CW comprised in the BL-ECM comprises a valid control word.

15 In such a case, a random number generator comprised in the processor preferably provides a new LSA-CW, thereby generating a new content license comprising the following information:

LSA-CW On/Off	LSA-CW	ESA-CW On/Off	ESA-CW
1	LSA-CW	1	ESA-CW

where:

LSA-CW On/Off indicates that the LSA-CW comprised in the BL-ECM
20 comprises a valid control word; and

ESA-CW On/Off indicates that the ESA-CW comprised in the BL-ECM comprises a valid control word. Thus, the processor preferably thereby generates the LSA-CW.

Thus, in the super-encryption case described above, the key table slot preferably comprises the following information:

LSA Decryption On/Off	LSA-CW	ESA Decryption On/Off	ESA-CW	LSA Encryption On/Off	LSA-CW
0	Filler Bits	0	Filler Bits	1	LSA-CW

Thereby enabling the device to reverse the super-encryption process, as needed.

It is appreciated that software components of the present invention may, if desired, be implemented in ROM (read only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques.

Reference is now made to Fig. 4, which is a simplified flowchart illustration of a preferred method of operation of the system of Fig. 1, in accordance with preferred embodiments thereof. The method of Fig. 4 is believed to be self explanatory with reference to the above discussion.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only by the claims which follow:

What is claimed is:

CLAIMS

1. A key management method comprising:
5 receiving content scrambled with a first scrambling algorithm (FSA);
determining whether to descramble the content according to a first rule and producing a first result;
only if the first result indicates that the content should be
10 descrambled, descrambling the content according to an FSA control word;
determining whether to apply a second scrambling algorithm (SSA) according to a second rule and producing a second result; and
only if the second result indicates that the SSA should be applied, applying the SSA, the applying the SSA comprising re-scrambling according to a
15 SSA control word,
wherein the FSA control word changes at an FSA control word change time, and the method also comprises:
changing the SSA control word in lockstep fashion with the FSA control word, such that each change of the FSA control word causes a change of
20 the SSA control word.
2. The method according to claim 1 and wherein the first rule comprises an instruction to descramble the content according to the FSA control word.
25
3. The method according to claim 1 and wherein the first rule comprises an instruction to not descramble the content.
4. The method according to any of claims 1 - 3 and wherein the second
30 rule comprises an instruction to descramble the content according to the SSA control word.

5. The method according to any of claims 1 - 3 and wherein the second rule comprises an instruction to not descramble the content.

6. The method according to any of claims 1 - 5, and wherein the
5 changing of the SSA control word occurs in hardware.

7. The method according to any of claims 1 - 6 and wherein the re-encrypted content is locally stored.

10 8. The method according to any of claims 1 - 7 and wherein the first rule is comprised in a content license.

9. The method according to any of claims 1 - 8 and wherein the second rule is comprised in a content license.

15

10. Apparatus substantially as described hereinabove.

11. Apparatus substantially as shown in the drawings.

20 12. A method according to any of claims 1 - 9 and substantially as described hereinabove.

13. A method according to any of claims 1 - 9 and substantially as shown in the drawings.

25

14. A system substantially as described hereinabove.

15. A system substantially as shown in the drawings.

30

FIG. 1

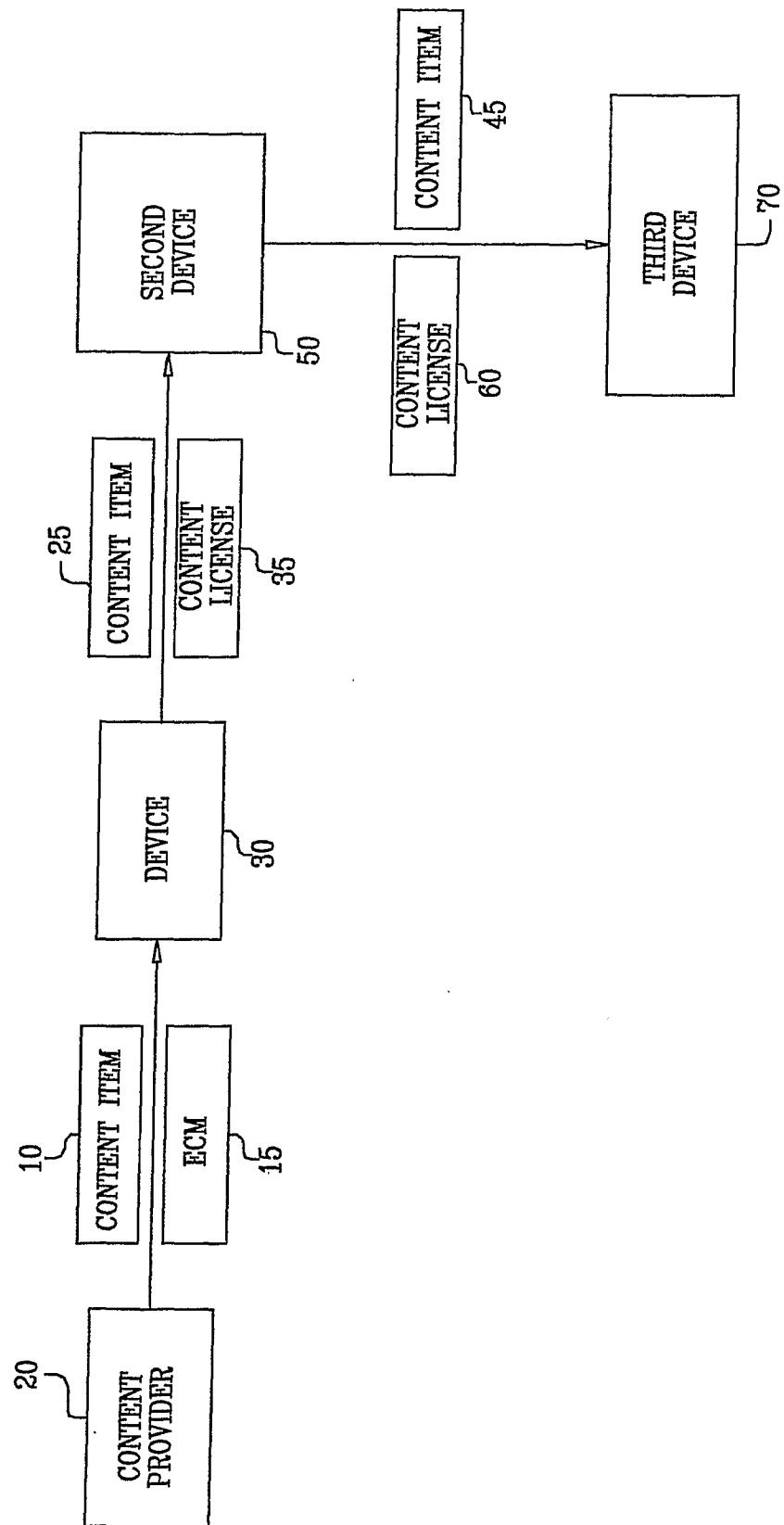
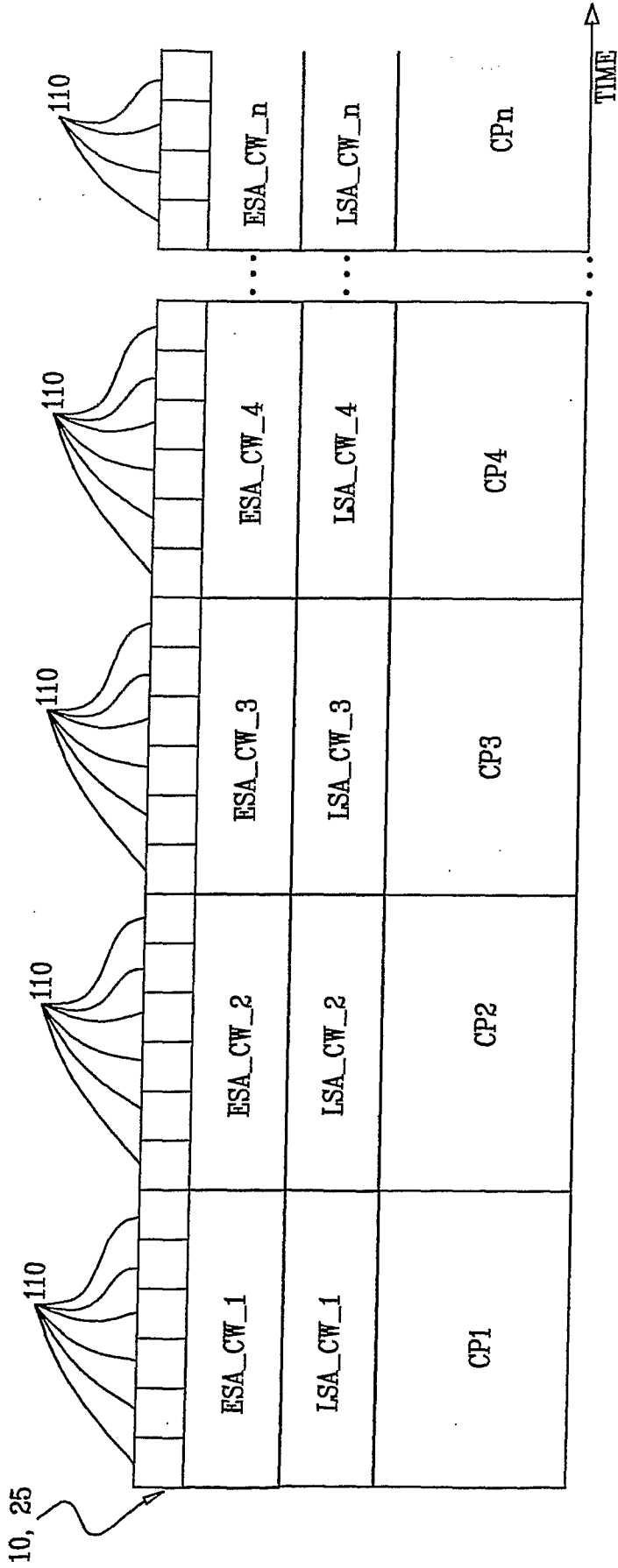


FIG. 2



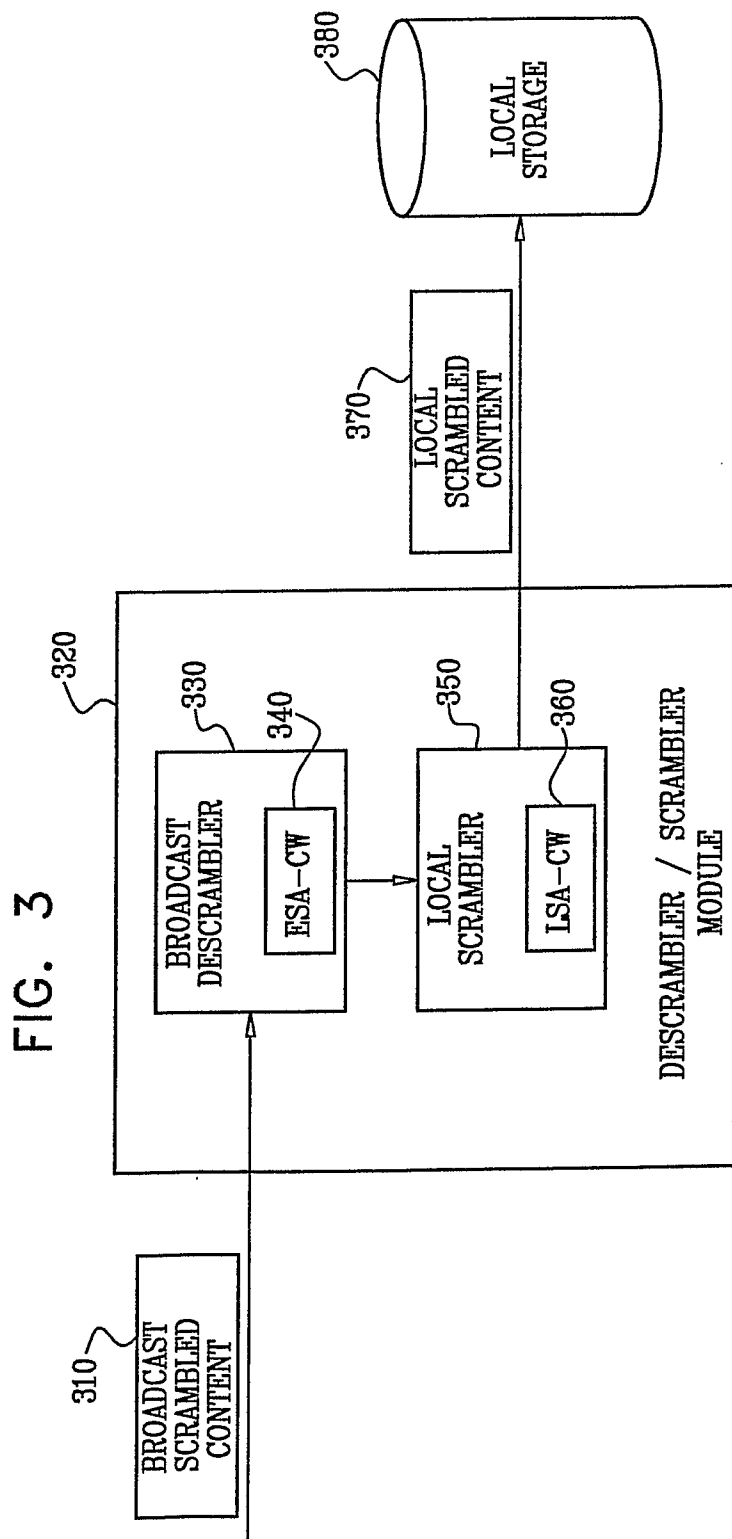


FIG. 4

