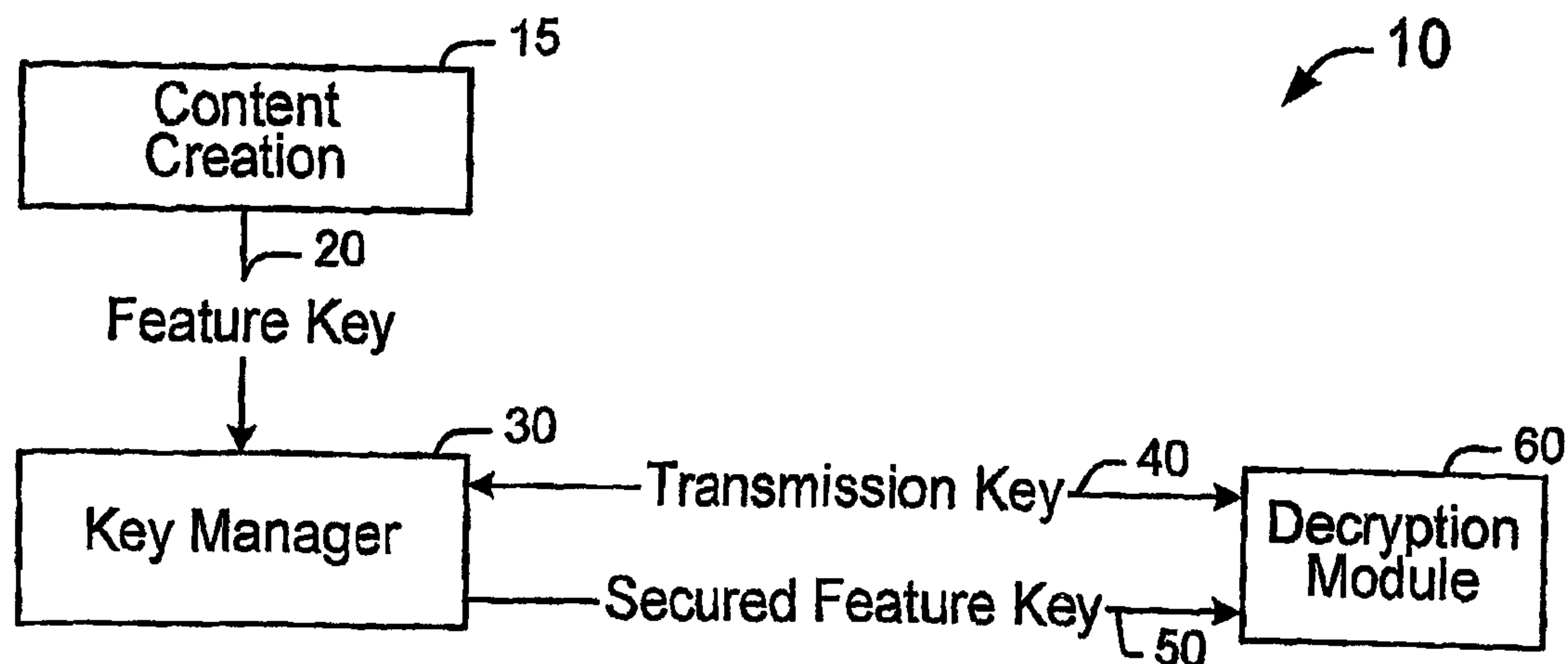




(86) Date de dépôt PCT/PCT Filing Date: 2006/01/18  
(87) Date publication PCT/PCT Publication Date: 2006/08/24  
(45) Date de délivrance/Issue Date: 2016/03/01  
(85) Entrée phase nationale/National Entry: 2007/08/03  
(86) N° demande PCT/PCT Application No.: US 2006/001707  
(87) N° publication PCT/PCT Publication No.: 2006/088596  
(30) Priorité/Priority: 2005/02/15 (US60/653,154)

(51) Cl.Int./Int.Cl. *H04L 9/14* (2006.01),  
*H04N 21/4405* (2011.01)  
(72) Inventeur/Inventor:  
ROBERT, ARNAUD, US  
(73) Propriétaire/Owner:  
THOMSON LICENSING, FR  
(74) Agent: CRAIG WILSON AND COMPANY

(54) Titre : SYSTEME DE GESTION DE CLES POUR CINEMA NUMERIQUE  
(54) Title: KEY MANAGEMENT SYSTEM FOR DIGITAL CINEMA



(57) Abrégé/Abstract:

Key management in a digital cinema system (10, 100 and 1000) occurs by encrypting a feature key associated with encrypted content with a transmission key exchanged with a decryption module (60, 601, 602, 6001, 6002, 6003 and 6004), that serves to decrypt encrypted content. The encrypted feature key undergoes transmission to the decryption module to enable decryption of the encrypted content. In this way, the decryption module will only have the capability of decrypting content based on that module's own key.



## (12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
24 August 2006 (24.08.2006)

PCT

(10) International Publication Number  
**WO 2006/088596 A3**

## (51) International Patent Classification:

*H04N 7/167* (2006.01) *H04N 7/16* (2006.01)

## (21) International Application Number:

PCT/US2006/001707

## (22) International Filing Date: 18 January 2006 (18.01.2006)

## (25) Filing Language:

English

## (26) Publication Language:

English

## (30) Priority Data:

60/653,154 15 February 2005 (15.02.2005) US

(71) Applicant (for all designated States except US): **THOMSON LICENSING** [FR/FR]; 46, Quai A. Le Gallo, F-92100 Boulogne-Billancourt (FR).

## (72) Inventor; and

(75) Inventor/Applicant (for US only): **ROBERT, Arnaud** [CA/US]; 1030 E. Orange Grove, Burbank, California 91501 (US).

(74) Agent: **LAKS, Joseph, J.**; Thomson Licensing LLC, Two Independence Way, Princeton, New Jersey 08540 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AT, AU, AZ, BA, BB, BG, 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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, 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).

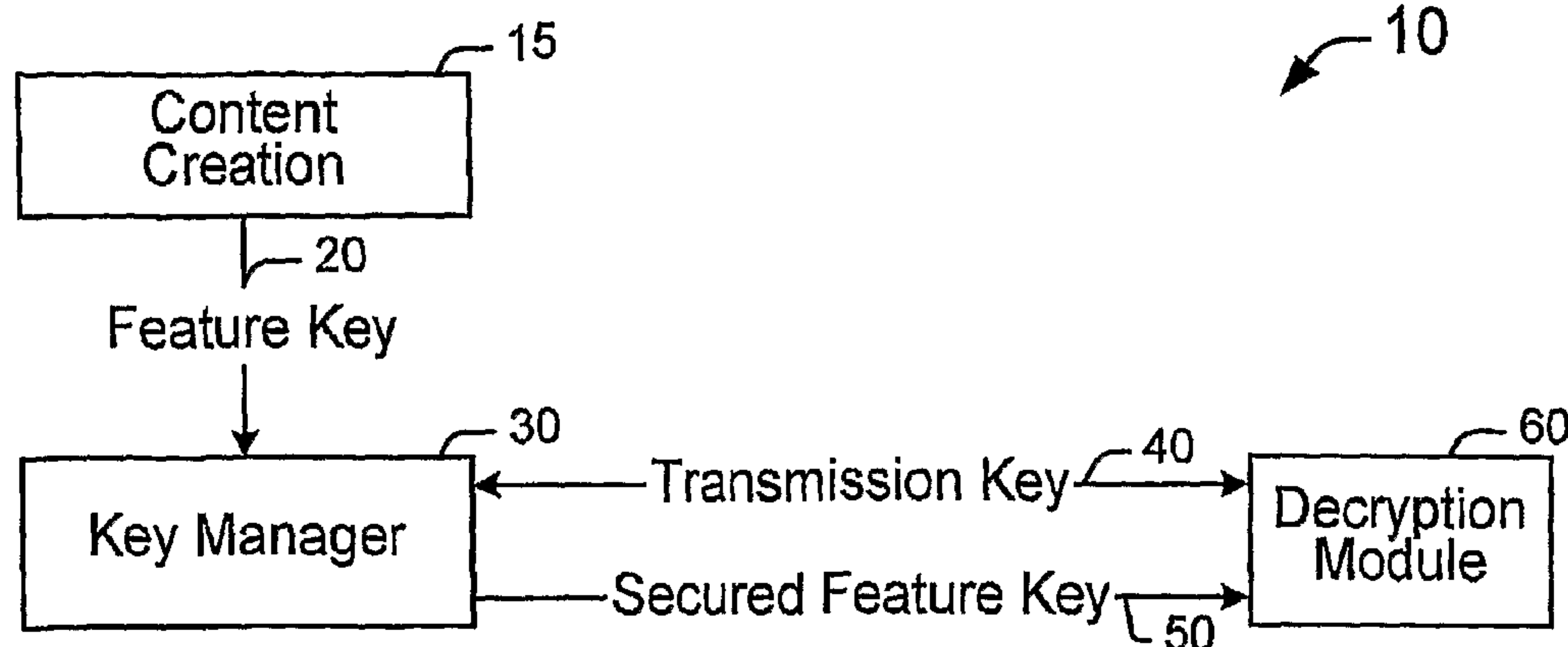
## Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

(88) Date of publication of the international search report:  
7 June 2007

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 FOR DIGITAL CINEMA



(57) Abstract: Key management in a digital cinema system (10, 100 and 1000) occurs by encrypting a feature key associated with encrypted content with a transmission key exchanged with a decryption module (60, 601, 602, 6001, 6002, 6003 and 6004), that serves to decrypt encrypted content. The encrypted feature key undergoes transmission to the decryption module to enable decryption of the encrypted content. In this way, the decryption module will only have the capability of decrypting content based on that module's own key.

WO 2006/088596 A3



## KEY MANAGEMENT SYSTEM FOR DIGITAL CINEMA

### FIELD OF THE INVENTION

This invention relates to digital cinema, and more particularly, for a technique for distributing and managing keys that secure content in a digital cinema system.

### BACKGROUND OF THE INVENTION

The term "Digital Cinema" refers generally to the creation and/or distribution of motion pictures in digital form, in contrast to traditional cinema whose content, including the image, sound track and subtitles, exists in an analog form on motion picture film. Digital cinema projection systems now exist and make use of a variety of technical solutions, rather than a single standardized solution embraced by all. Protection against copying remains the major concern of content owners (e.g., the motion picture studios) which has limited wide scale digital cinema deployment. The existence of content in digital form affords the opportunity to make perfect copies of the original content with little effort. For that reason various organizations, such as the Digital Cinema Initiative ("DCI") and the Society for Motion Picture Engineering ("SMPTE") have devoted much effort towards establishing specifications for digital cinema content distribution.

The DCI specification defines preferred solutions in many areas, such as encoding, distribution, and security. The SMPTE has sought to refine the DCI specification from a technical and implementation perspective. Within the area of security, key management plays a significant role. Key management refers to the management of the keys utilized to accomplish encryption of the digital content. The term, "encryption", as used throughout means either encryption or scrambling. Likewise, the term decryption means either



-2-

decryption or descrambling. At the present time, the DCI and SMPTE specifications provide for key management using device certificates and a Trusted Device List ("TDL"). Each Security Entity ("SE"), that is, each device capable of accessing or manipulating the content, will hold a digital certificate provided by the manufacturer of the device; the certificate can be managed by either the manufacturer or an independent entity. The TDL lists trusted devices, e.g., content-receiving devices, such as digital projectors. More specifically, the TDL lists the respective digital certificate of each device that is trusted to manipulate a particular piece of content. A feature encryption key ("KF") undergoes transmission from the content owner, or an agent acting upon its behalf such as a distributor, to a Security Module ("SM") located in a theater authorized to display the content. The SM has the responsibility for making sure that only devices explicitly referenced in the TDL access or learn of the KF.

This scheme has several disadvantages. First, no link necessarily exists between the issuer of the TDL and the issuer of the certificate(s), which introduces a security weakness. Conceivably, an outsider could manage to issue certificates to uncertified devices, and could manage to have such uncertified devices listed in a TDL. Second, the Security Module (SM), which typically resides outside the control of the content rights owner and the exhibitor, serves as the sole entity responsible for ensuring that the feature keys only get distributed to trusted devices. Under such circumstances, a hacker could manipulate the SM in such a way to permit transmission of feature keys to devices outside the TDL. Third, with the SM responsible for the KF management in a theater, a hacker could manipulate the SM to get access to the KF. Since the content resides in digital form, access to KF would allow the hacker to access the content and redistribute it virtually free of losses

Thus, a need exists for a key management process that maintains the feature key confidential to those devices that actually perform decryption of the content.

## SUMMARY OF THE INVENTION

Brief in accordance with the present principles, there is provided a technique for key management, and in practice, key management for digital cinema content. The method commences by encrypting a feature key associated with encrypted content with a transmission key exchanged with a decryption module. Typically, although not necessarily, the decryption module resides at a theater or similar facility at which encrypted content undergoes decryption



-3-

in accordance with a key for subsequent presentation. The encrypted feature key undergoes transmission to the decryption module to enable decryption of the encrypted content. In this way, the decryption module will only have the capability of decrypting content based on that module's own key.

5

## BRIEF SUMMARY OF THE DRAWINGS

FIGURE 1 depicts a simplified block diagram of a system for practicing the key management technique of the present principles for a single decryption module in a single exhibition facility;

10

FIGURE 2 depicts a simplified block diagram of a system for practicing the key management technique of the present principles for multiple of decryption modules in a single exhibition facility; and

FIGURE 3 depicts a simplified block diagram of a system for practicing the key management technique of the present principles for a multiple decryption modules in multiple exhibition facilities.

15

## DETAILED DISCLOSURE

FIGURE 1 depicts a block schematic diagram of a system 10 for providing key management in accordance with a first embodiment of the present principles. At the outset of the key management process, a content creator, such as a movie studio, engages in content creation, represented by block 15 in FIG 1. The created content resides in digital form, whether as a result of initial creation using digital capture devices or the result of conversion into digital of images initially captured on film. The content creator or its agent will encrypt the content in digital form using any one of a number of well known techniques that require the use of a key, depicted in FIG. 1 as feature key 20, to decrypt the content.

20

25

A key manager 30 receives the feature key 20. It further agrees to a transmission key 40 with a decryption module 60 typically associated with a digital cinema projector located at an exhibition facility such as a movie theater or the like (not shown). Either the key manager or decryption module will initiate the exchange of the transmission key 40. Typically, the key manager 30 takes the form of a programmed digital computer, or dedicated logic having

30



-4-

the ability to encrypt and/or decrypt one type of key using another key. The key manager 30 encrypts the feature key 20 with the transmission key 40, yielding a secure feature key 50 which is sent to the decryption module 60. The decryption module 60 utilizes the negotiated transmission key 40 to derive the feature key 20, and further decrypt encrypted content to permit display.

The key management technique practiced by the system 10 described above affords the advantage of increased security. The process of encrypting the content feature key 20 with the transmission key 40 from the decryption module 60 makes the feature key 20 more difficult to intercept. Moreover, the secure feature key 50 utilized by the decryption module 60 remains uniquely associated with the decryption module, greatly reducing the likelihood that secure feature key, even if hacked, would enable another decryption module to properly decrypt a piece of encrypted content.

FIGURE 2 depicts a block schematic diagram of a system 100 for providing key management in accordance with a second embodiment of the present principles. At the outset of the key management process, a content creator, such as a movie studio, engages in content creation, represented by block 150 in FIG 2. The created content resides in digital form, whether as a result of initial creation using digital capture devices or the result of conversion into digital of images initially captured on film. The content creator or its agent will encrypt the content in digital form using any one of a number of well known techniques that require the use of a key, depicted in FIG. 2 as feature key 200 to decrypt the content.

A key manager 300 receives the feature key 200 from the content creator. The key manager 300 of FIG. 2 will exchange transmission keys 401 and 402 with each of decryption modules 601 and 601, both located at the same exhibition facility, but each module associated with a different digital cinema projector (not shown). Either the key manager or each decryption module will initiate the exchange. . Like the key manager 30 of FIG. 1, the key manager 300 takes the form of a programmed digital computer, or dedicated logic having the ability to encrypt one type of key using another key. The key manager 300 of FIG. 2 encrypts the feature key 200 separately with each of the transmission keys 401 and 402 from the decryption modules 601 and 602, respectively, to yield secure feature keys 501 and 502, respectively. Each of the decryption modules 601 and 602 utilizes its corresponding one of transmission keys 401 and 402, respectively, to access the feature key 200 and further decrypt encrypted content to permit display.



In comparison to the key management system 10 of FIG. 1 which performs encryption of the feature key 20 with the transmission 40 associated with the single decryption module 60, the key manager 300 of FIG. 2 separately encrypts the feature key 200 with the transmission key of the different decryption modules 601 and 602 to yield the separate secured feature keys 501 and 502, respectively. Each of the separate secured feature keys 501 and 502 will only function with a corresponding one of the decryption modules 601 and 602. With the key management system 100 of FIG. 2, a theater operator cannot use the same secure feature key with more than one decryption module to violate established security safeguards.

The key manager 300 of FIG. 2 can also exchange different feature keys (such as the key feature 200) with each of the decryption modules 601 and 602. In such a case, the key manager 300 would utilize the transmission key 401 to encrypt a feature key 201 (not shown) yielding in a secured feature key (not shown) in place of the secured feature key 501) and send it to the decryption module 601; the later would use its transmission key 401 to decrypt this secured feature key, obtain the feature key 201, and decrypt encrypted content to permit display. Similarly, the key manager 300 would encrypt a second feature key 202 (not shown) using the transmission key 402 yielding a secure feature key (not shown) in place of key the secured feature key 502). The key manager 300 would send this secured feature key to the decryption module 602 who would use its transmission key 402 to decrypt the secured feature key 504, obtain the feature key 202, and decrypt encrypted content to permit display.

FIGURE 3 depicts a block schematic diagram of a system 1000 for providing key management in accordance with a third embodiment of the present principles. At the outset of the key management process, a content creator, such as a movie studio, engages in content creation, represented by block 1500 in FIG 3. The created content resides in digital form, whether as a result of initial creation using digital capture devices or the result of conversion into digital of images initially captured on film. The content creator or its agent will encrypt the content in digital form using any one of a number of well known techniques that require the use of a key, depicted in FIG. 3 as feature key 2000 to decrypt the content.

A key manager 3000 receives the feature key 2000 from the content creator. The key manager 3000 of FIG. 3 exchange transmission keys 4001-4004 with decryption modules 6001-6004, respectively. In the illustrated embodiment of FIG. 3, the decryption modules 6001 and 6002 reside at a first exhibition facility (Theater A) whereas the decryption modules 6003 and 6004 reside at a second exhibition facility (Theater B). Alternatively, each of the



-6-

decryption modules 6001-6004 could reside at separate exhibition facilities. The number of exhibition facilities and the number decryption modules at each such facility can vary without adversely affecting the key management technique of the present principles. Either the key manager or decryption module will initiate the exchange. If the key manager initiates the exchange, the key manager system typically will send to each decryption module a unique identifier of at least one expected decryption recipient.

Like the key manager 300 of FIG. 2, the key manager 3000 of FIG. 3 takes the form of a programmed digital computer, or dedicated logic having the ability to encrypt one type of key using another key. The key manager 3000 of FIG. 3 encrypts the feature key 2000 separately with each of the transmission keys 4001-4004 from the decryption modules 6001-6004, respectively, to yield secure feature keys 5001-5004, respectively. Each of the decryption modules 6001-6004 uses its corresponding one of secured feature keys 5001-5004, respectively, to decrypt encrypted content to permit display.

Just as the key manager 300 of FIG. 2 separately encrypts the feature key 200 with the transmission keys 401 and 402 to yield the separate secure feature keys 501 and 502, respectively, the key manager 3000 of FIG. 3 encrypts the feature key 2000 separately with each of the transmission keys 4001-4004, respectively, to yield secure feature keys 5001-5004, respectively. In each instance, each decryption module receives a secure feature key unique to that module. Thus, the key management system 1000 of FIG. 3, like the key management system 100 of FIG. 2 prevents a theater operator from using the same secure feature key with more than one decryption module to violate established security safeguards.

In the event that two or more decryption modules serve to decrypt the same feature, a key manager, such as key manager 300 of FIG. 2 or key manager 3000 of FIG. 3 could provide the same feature key, provided that such decryption modules each provide the key manager with a common transmission key. Otherwise, the key manager will provide a separate secure feature key to each decryption module.

In each of key management systems 10, 100 and 1000 of FIGS. 1-3, respectively, transmission of the feature key to the key manager occurs in a secure manner. As discussed, each key manager creates individual secured feature key(s) by encrypting the feature key with the transmission key associated with each decryption module destined to eventually decrypt content, including any spare or back-up decryption module.



-7-

In practice, the feature keys, 20, 200 and 2000 each comprise a single symmetrical key. The feature key exchange between the feature creation system and key manager typically occurs using a cryptographic symmetrical algorithm based on a shared secret. The feature key exchange between the feature creation system and the key manager can also be  
5 secured using an asymmetrical cryptographic algorithm based on the secret/public key pair of the key manager, or using a secured authenticated channel or a private modem line.

Similarly, the feature key exchange between the key manager and the decryption module(s) typically occurs using a cryptographic symmetrical algorithm based on a shared secret, provided the key manager and the decryption module were able to mutually  
10 authenticate each other in a cryptographic sense. The feature key exchange between the key manager and the decryption module can be secured using an asymmetrical cryptographic algorithm based on the secret/public key pair of the decryption module, provided the key manager was able to securely authenticate the decryption module.

Various alternatives exist for encrypting content, such as using a digital envelope or  
15 asymmetrical keys. Moreover, content encryption can occur using multiple keys, rather than a single key, with each key typically, although not necessarily, associated with a temporal segment of the feature. Various methods exist for segmenting the content to enable the use of multiple keys, such as segmenting the feature into N consecutive segment, where N is greater than one. If multiple feature encryption keys are utilized, the system described at Figure 1 can  
20 be modified to optimize operations, both at the system and the feature decryption levels. For example, as illustrated in Figure 1, the key management system 30 could first encrypt the feature keys with a master key, encrypt the master key with the transmission key 40 (the transmission key could be the public key of the decryption module or a symmetrical key exchanged between the key manager and the decryption module), and send both results to the  
25 decryption module 60. Content encryption also can occur using asymmetrical scrambling or encryption algorithms. Further, the content can undergo super-scrambling or super-encrypted using an additional key, e.g. the feature is first encrypted by the feature key, and then by the additional key (or vice versa). Content encryption can also occur using a key that is derived from the feature key and other information, such as but not limited to, the identity of the key  
30 management system, the decryption module, the time, the date, and/or any combination thereof.



-8-

In a preferred embodiment, the transmission key comprises the public key of the decryption module as provided by an asymmetrical cryptography key pair. The transmission key can change periodically, randomly, or on-demand.

Each decryption module sends its public key to the key manager. Such transmission  
5 can occur individually (i.e. each decryption module has a direct connection to the key manager). Alternatively, a group of decryption modules, e.g. all decryption modules at a single exhibition facility, could send their respective public keys within a single message to the key management system. The communication link could comprise a wireless or wired channel. Alternatives to the asymmetrical approach for the transmission key could include  
10 using a pre-agreed upon symmetrical key, a MAC-based method, and so on. The key management technique of the present principles affords the advantage of securing the features encryption key in such a way the latter is only accessible the decryption module level and by no other intermediary modules.

Each of decryption modules 60, 601-602 and 6001-6004 has an association with a  
15 physical device at the exhibition facility, for example but not limited to, a Security Module (not shown), a projector(not shown), a content processing device (not shown), and so on. The actual location of the decryption module has no bearing on the key management technique of the present principles. What remains necessary is that each decryption module has its identity known to the key manager and both must have the ability to exchange transmission keys with  
20 each other. Although depicted separately, the key management system could exist as part of a physical device in the theater (as described above) or could exist as part of the content creation system.

The decryption module need not possess a direct communication link to the key manager. In such a case, a relay entity, for example the Theater Management System or the  
25 Security Module (not shown), as described in the DCI and SMPTE documents (incorporated by reference herein), could capture the messages from the key manager, and relay them to the appropriate decryption module.

The foregoing describes a technique for managing keys in connection with decryption of encrypted content.



PU050025

- 9 -

What is claimed is:

1. A key management method, comprising the steps of:  
encrypting a feature key associated with encrypted content with each of a plurality of transmission keys collectively received as single message from corresponding decryption modules at a key manager that performs the encryption, to yield a plurality of secured feature keys; and  
providing a separate one of the plurality of secured feature keys to a corresponding one of the decryption modules to enable decryption of the encrypted content.
2. The method according to claim 1 wherein the providing step further comprises the step of providing the secure feature keys over secure transmission channels.
3. The method according to claim 1 wherein the providing step further comprises the step of providing the secure feature keys over secure wireless transmission channels.
4. A key manager system for receiving a feature key from a feature creation system and for distributing secure feature keys to decryption modules, comprising,  
a key manager, in the form of a digital computer, for (1) encrypting a feature key from the feature creation system with each of a plurality of transmission keys collectively received as single message from corresponding decryption modules to yield a plurality of secure feature keys and (2) providing a separate one of the plurality of secured feature keys to a corresponding one of decryption module to enable decryption of the encrypted content.
5. The system of claim 4 wherein the feature creation system and the key manager exist as a single entity.
6. The system of claim 4 wherein the key manager and the device decryption modules exist as a single entity.



PU050025

- 10 -

7. The system of claim 4 wherein the content is encrypted using one of an asymmetrical or a symmetrical scrambling or encryption algorithm.
8. The system of claim 4 wherein the key manager system sends to the decryption module a unique identifier of at least one expected decryption recipient.
9. The system of claim 4 wherein the feature key is secured using a symmetrical encryption or scrambling algorithm utilizing a key shared between the key manager and the decryption module.
10. The system of claim 4 wherein the feature key is secured using an asymmetrical encryption algorithm based on the secret/public key of the key manager.
11. The system of claim 4 wherein the feature key is secured using an asymmetrical encryption algorithm based on a secret/public key of the decryption module.
12. The system of claim 4 wherein the feature key is secured using an asymmetrical cryptographic based secret/public key pair generated in accordance with the transmission key and other information.
13. The system of claim 4 wherein distribution of the secured feature key occurs over a secured channel.



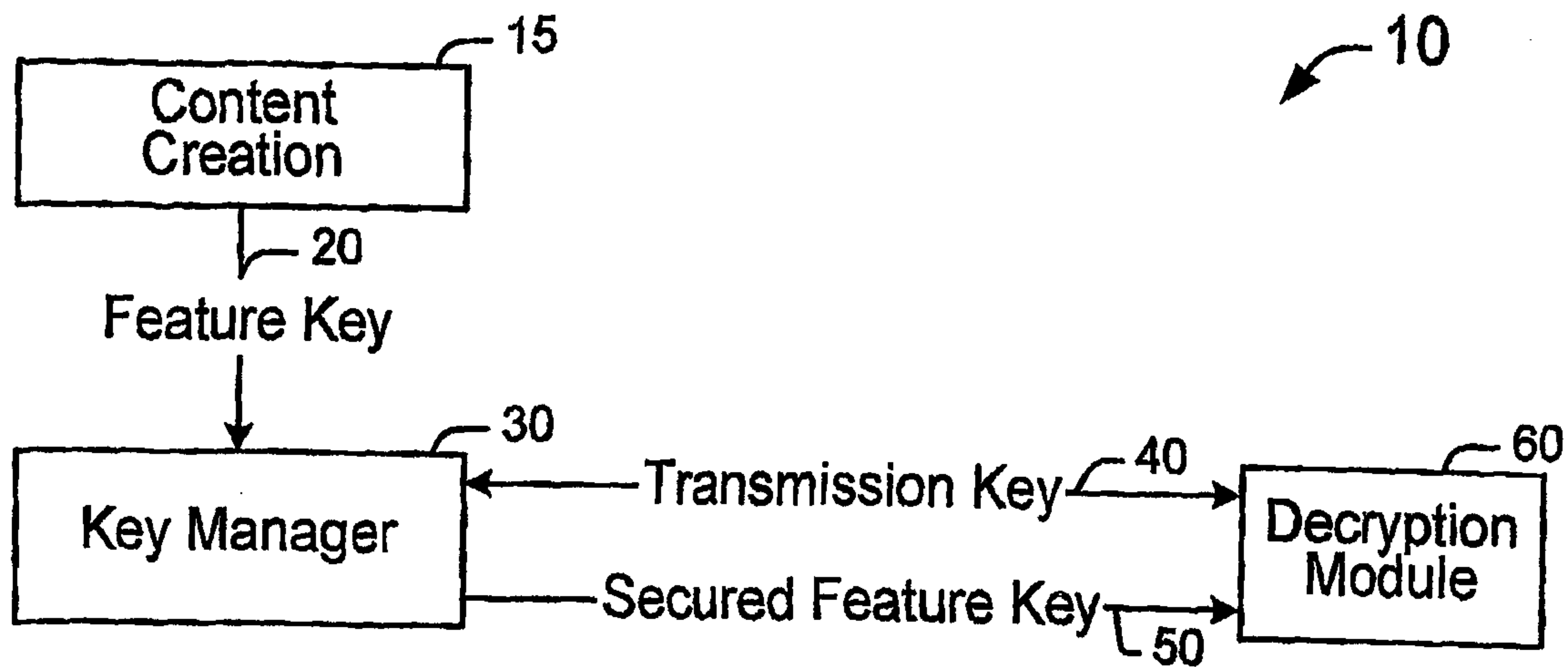


FIG. 1

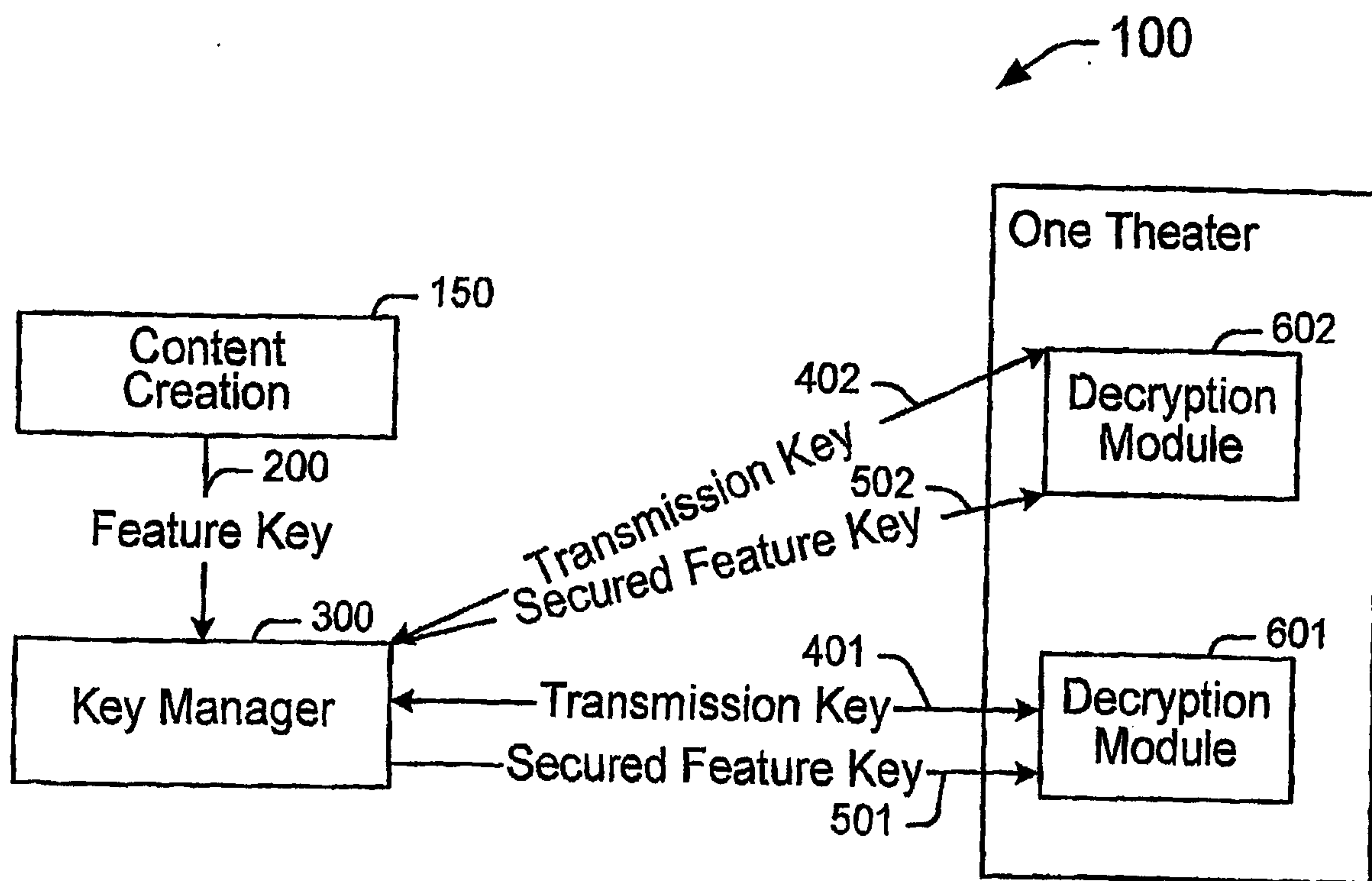


FIG. 2



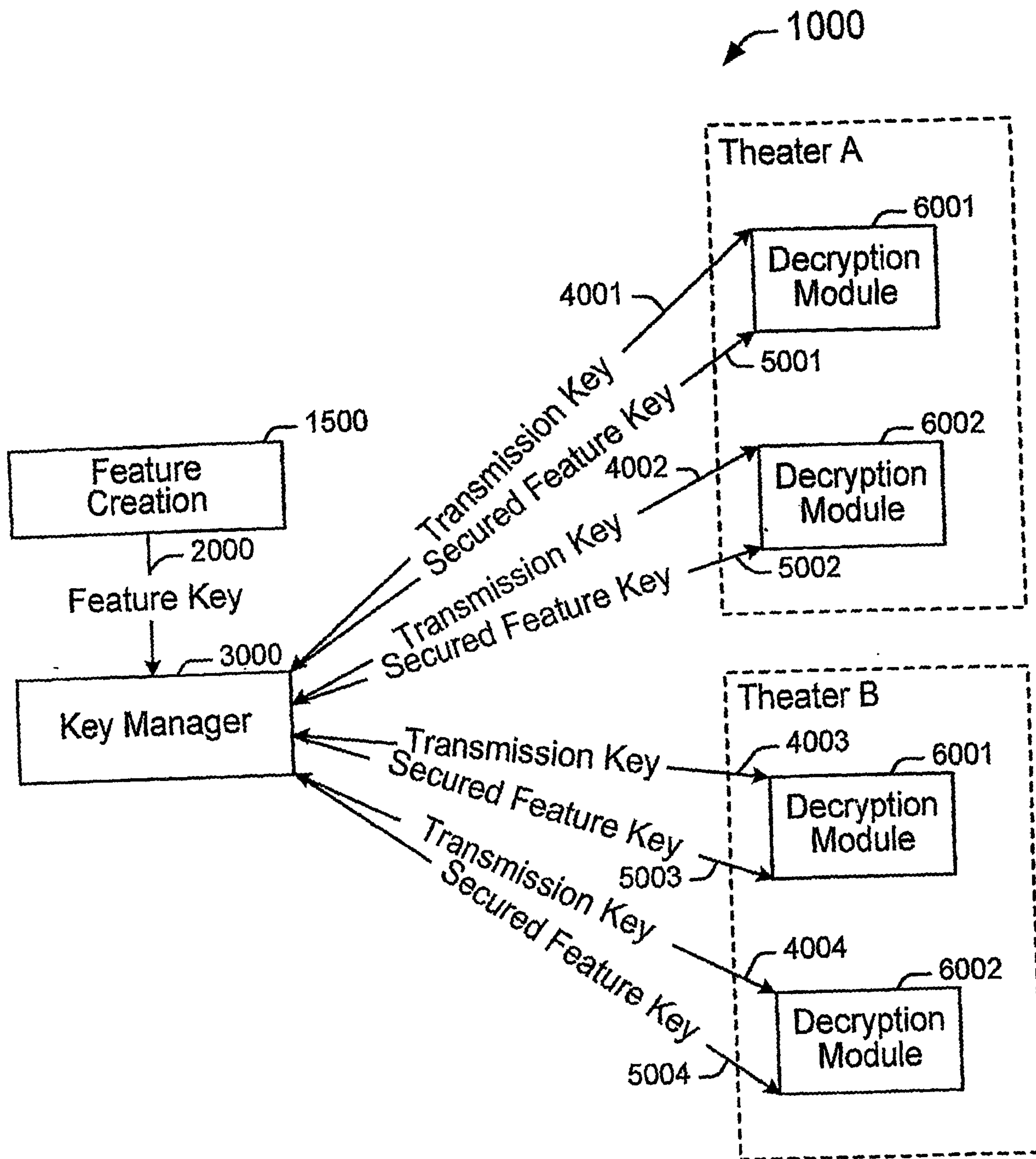


FIG. 3



