(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 418 756 A2

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
12.05.2004 Bulletin 2004/20

(51) Int Cl.⁷: **H04N 7/167**, H04N 7/16

(21) Application number: **03104017.3**

(22) Date of filing: **29.10.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **29.10.2002 US 284049**

(71) Applicant: **General Instruments, Motorola Inc**
Horsham PA 19044 (US)

(72) Inventors:
- **Chen, Annie On-yee**
  92014, Del Mar (US)
- **Tang, Lawrence W**
  92128, San Diego (US)
- **Murphy, Patrick**
  92123, San Diego (US)
- **Okimoto, John I**
  92128, San Diego (US)
- **Cochran, Keith R.**
  San Diego 92108 (US)
- **Hutchings, George T**
  18901, Doylestown (US)

(74) Representative: **McCormack, Derek James et al**
Motorola
European Intellectual Property Operations
Midpoint
Alencon Link
Basingstoke Hampshire RG21 7PL (GB)

(54) Method and system for encrypting material for distribution

(57) Streaming content is encrypted by segmenting the content into a plurality of crypto periods, and by encrypting the content for each of a plurality of crypto periods with a different cryptographic key. The crypto periods may be based on either (i) fixed time intervals, (ii) a fixed number of packets, (iii) a fixed marker count, or (iv) a pseudo random number of packets. Methods are provided for determining how to record the key changing criteria, and how to convey this information to video on demand (VOD) servers.

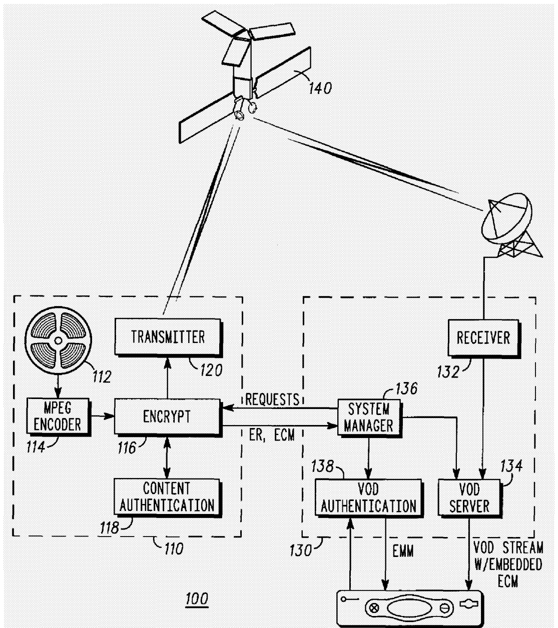

FIG. 1

Description

TECHNICAL FIELD OF THE INVENTION

[0001] The invention relates to a method and a system for encrypting material such as video material for distribution. In particular, it relates conditional access and copy protection techniques, and more particularly to such techniques for interactive, on-demand digital program content such as video-on-demand (VOD) programming distributed via cable and satellite networks.

BACKGROUND

[0002] Recent advances in cable and satellite distribution of subscription and "on-demand" audio, video and other content to subscribers have given rise to a growing number of digital set-top boxes (sometimes referred to as Digital Consumer Terminals or "DCTs") for decoding and delivering digitally broadcast programming. These set-top boxes often include additional circuitry to make them compatible with older analog encoding schemes for audio/video distribution. As the market for digital multimedia content of this type grows and matures, there is a corresponding growth of demand for new, more advanced features.

[0003] Video-on-demand (hereinafter VOD) and audio-on-demand are examples of features made practical by broadband digital broadcasting via cable and satellite. Unlike earlier services where subscribers were granted access to scheduled encrypted broadcasts (e. g., movie channels, special events programming, pay per view purchases, etc.), these on-demand services permit a subscriber to request a desired video, audio or other program at any time and to begin viewing the content at any point therein. Upon receiving the request for programming (and, presumably, authorization to bill the subscriber's account), the service provider then transmits the requested program to the subscriber's set-top box for viewing/listening. The program material is typically "streamed" to the subscriber in MPEG format for immediate viewing/listening, but can also be stored or buffered in the set-top box (typically on a hard-disk drive or "HDD") for subsequent viewing/listening.

[0004] The Motion Picture Association of America (hereinafter MPAA) is a trade association of the American film industry, whose members include the industry's largest content providers (i.e., movie producers, studios). The MPAA requires protection of VOD content from piracy. Without adequate security to protect their content, its member content providers will not release their content (e.g., movies) for VOD distribution. Without up-to-date, high-quality content, the VOD market would become non-viable.

[0005] Access control methods, which may include encryption, are continually evolving to keep pace with the challenges of video-on-demand (VOD) and other consumer-driven interactive services. With VOD, head-end-based sessions are necessarily becoming more personalized. In this scenario, video streams are individually encrypted and have their own set of unique keys.

[0006] One key area of concern, especially for direct content providers and movie companies, is VOD copy protection. The method by which content is produced and delivered to consumers is constantly changing. Under the newest scenarios, content delivery can occur over data backbones, satellite networks and the Internet, increasing the potential for hackers to get digitally perfect copies of the VOD content. As the VOD industry develops and adapts to the piracy threat by providing more sophisticated encryption schemes, piracy becomes more difficult, but the potential gain to the video "pirate" for achieving successful encryption breaches (successful content copying) remains a considerable attraction to hackers.

[0007] Assuming that physical security and network security measures are adequate at the movie company, the VOD encoding company and at the MSO (Multiple System Operator) or satellite operator's facilities, the primary points of VOD vulnerability to piracy occur when VOD content is transmitted over widely accessible communication networks such as a satellite channel, the Internet or a cable system. Such transmissions can occur between the movie company and the VOD encoder, between the VOD encoder and the MSO or satellite operator, and between the MSO or satellite operator and the VOD customer. Because of the ease with which such transmissions can be intercepted, these are the points where the risk of piracy is the greatest.

SUMMARY OF THE INVENTION

[0008] According to the invention, techniques are provided to pre-encrypt VOD material with a changing cryptographic key and to convey this information to VOD servers so that the VOD servers can send out the corresponding ECMs (Entitlement Control Messages) when the encrypted content is delivered to a consumer's digital set top.

[0009] Further according to the invention, multiple encryption keys are added when pre-encrypting VOD material. More specifically, methods are provided for determining when to change encryption keys; how to record the key changing criteria, and how to convey this information to the VOD servers.

[0010] Further according to the invention, streaming content is encrypted by segmenting the content into a plurality of crypto periods, and encrypting the content for each of a plurality of crypto periods with a different cryptographic key. The crypto periods may be established as follows:

1) <u>Fixed crypto period:</u> Define a crypto time interval and change the key each time the crypto time-interval passes.

2) Fixed number of packets: Determine a number of content packets "n" corresponding to a suitable time interval and change the cryptographic key every "n" packets.

3) Fixed "marker" count: Using a suitable MPEG-II field type as a "marker", such as an I-frame header, change the cryptographic key every time "n" markers have passed in the stream, where "n" is selected to produce a suitable crypto period. The MPEG-II I-frame header is one example of a suitable "marker." Alternatively, any other suitable, recurring MPEG-II encoding element could be used as a stream "marker" to delimit segments of the MPEG-II stream.

4) Random crypto period: Change the crypto-period randomly within upper and lower constraints on the crypto period, using a pseudo-random algorithm. Calculate a number of packets for each crypto period and change the key after that number of packets. Generate an index file indicating at which packet numbers the encryption key should be changed.

[0011] The invention is particularly useful for generating rapidly changing encryption keys, and for methods of communicating how and when to change the keys in the context of, for example, the MediaCipher-II conditional access (CA) system available from the Broadband Communications Sector of Motorola, Inc., Horsham, Pennsylvania, USA. Motorola's MediaCipher-II system is capable of changing keys at rates (crypto periods) which are measured in fractions of a second, rather than several seconds.

GLOSSARY

[0012] Unless otherwise noted, or as may be evident from the context of their usage, any terms, abbreviations, acronyms or scientific symbols and notations used herein are to be given their ordinary meaning in the technical discipline to which the invention most nearly pertains. The following glossary of terms is intended to lend clarity and consistency to the various descriptions contained herein, as well as in prior art documents:

CA Conditional Access. A means by which access to content is granted only if certain prerequisite conditions are met (e.g., payment of a subscription fee, time-dependent license, etc.)

CAS Conditional Access System. A means of allowing system users to access only those services that are authorized to them, comprises a combination of authentication and encryption to prevent unauthorized reception

CP Crypto Period. A period covering a portion of an encrypted stream during which a specific encryption key is valid.

ECM Entitlement Control Message. Entitlement Control Messages are private conditional access information which specify control words and possibly other, typically stream-specific, scrambling and and/or control parameters.

EMM Entitlement Management Message. Conditional access messages used to convey entitlements or keys or other parameters to users, or to invalidate or delete entitlements or keys. For example, an EMM can be used in combination with an ECM to determine an encryption key. Without the EMM, the key cannot be derived. The following categories of EMM are possible:

EMM-G: EMM for the whole audience
EMM-S: Shared EMM between the elements of a group.
EMM-U: EMM for a single client.

ER Encryption Record. Contains information about how specific program content is encrypted, and rules for decoding.

ERS Encryption Renewal System. A system by which a conditional access license is renewed.

Internet The Internet (upper case "I") is the vast collection of inter-connected networks that all use the TCP/IP protocols. The Internet now connects many independent networks into a vast global internet. Any time two or more networks are connected together, this results in an internet (lower case "i"; as in international or inter-state).

MPAA Motion Picture Association of America

MPEG Moving Pictures Experts Group

MPEG-II MPEG-2 is the standard for digital television (officially designated as ISO/IEC 13818, in 9 parts).

MSO Multiple System Operator. A company that owns multiple cable systems.

PCR Program Clock Reference. PCR information is embedded into MPEG-II streams to accurately synchronize a program clock on the receiving system to the MPEG-II stream.

VOD Video-On-Demand. The service of providing content through subscriber selection off a large menu of options, available to a viewer at any time.

[0013] Embodiments of the present invention will now be described by way of example with reference to the accompanying drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] **Figure 1** is a block diagram of a system for delivering pre-encrypted video content, in accordance with the invention.

[0015] **Figure 2A** is a diagram showing a changing-key encryption scheme for pre-encrypted content using a fixed crypto period, in accordance with the invention.

[0016] **Figure 2B** is a diagram showing a changing-key encryption scheme for pre-encrypted content using a crypto period based on a fixed number of packets, in accordance with the invention.

[0017] **Figure 2C** is a diagram showing a changing-key encryption scheme for pre-encrypted content using a crypto period delimited by a fixed number of MPEG-II I-frames, in accordance with the invention.

[0018] **Figure 2D** is a diagram showing a changing-key encryption scheme for pre-encrypted content using a "random" crypto period, in accordance with the invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0019] The invention relates to conditional access and copy protection techniques and more particularly to such techniques for interactive, on-demand digital program content such as video-on-demand (VOD) programming distributed via cable and satellite networks.

[0020] In order to protect against interception and copying of digital program content, a pre-encryption procedure is employed whereby server-based VOD content is stored in an encrypted form, then delivered directly to viewers without further encryption processing. The VOD content is encrypted at the point where it is encoded, and is distributed to content resellers (e.g., MSO's, satellite operators, etc.) in encrypted form. Content encoders generally do not distribute directly to end-users (viewers). Typically, encryption is accomplished separately and uniquely for each reseller.

[0021] **Figure 1** is a block schematic diagram of a system 100 for delivery of pre-encrypted program content, within which an embodiment of the present invention can be incorporated. The system 100 is suitably a conditional access system (CAS) which is a system for granting conditional access to certain digital content (movies, etc.), the "conditions" being licensing conditions (fee paid, access granted starting on date xx/xx/xx at xx:xx until yy/yy/yy at yy:yy, etc.). It is noted that although the entire system 100 is not typically included in one CAS, it could be.

[0022] At a content encoder's location 110, master content 112 (e.g., movies and other program content) is encoded into digital form via a suitable (e.g., MPEG-II) encoder 114. This content is then encrypted in an encryption system 116, to be "encrypted content." A content authorization system 118 is used to, e.g., manage, renew and verify valid licensing for the encrypted content. This can permit, for example, encryption by the encryption system 116 only if valid licensing exists for any particular destination. At a minimum, system 118 will control whether encryption can occur, independently of content destination. The encryption system 116 can generate a "personalized" encryption for each destination content reseller (e.g., MSO). Such a feature is not, however, required. Instead, the same encryption process could be used for a plurality of different MSOs. The encrypted content is transmitted via a transmitter (XMIT) 120 over a suitable transmission medium 140 to a receiver 132 at a reseller's location 130. The transmission medium is shown as being a satellite, but it can be the Internet, a cable network, or any other suitable delivery mechanism.

[0023] The receiver 132 receives the encrypted content and stores it in a VOD server 134 from which it can be re-transmitted to end-users. A system manager 136 (e.g., computer system that controls operation of a reseller's various transmission and communications resources) communicates with the encryption system 116 to make requests for program content, and to receive encryption records (ER) defining how the requested program content is encrypted/encoded and to receive entitlement control messages (ECMs) associated with the encryption of the program content. Typically, the encryption system 116 and the system manager 136 are parts of an ECM Renewal System (ERS) by which authorizations to distribute/decode program content are managed and renewed. It should be appreciated, however, that the ECM renewal can be separate from the other functions included in encryption system 116. As an example, a centralized ERS can be provided. It is also noted that the System Manager 136 would typically be provided by the VOD vendor, although it may be provided by others.

[0024] At the reseller's (e.g., MSO's) location, a user authorization system 138 ("VOD Auth.") receives requests from end users for program content, and verifies that appropriate authorizations are in place for the end user to view the requested content. If the appropriate authorizations are in place, then the user authorization system 138 instructs the VOD server 134 to deliver the requested (encrypted) content to the user's VOD playback device 150 (e.g., set-top box) and generates an Entitlement Management Message (EMM) for the requested content for delivery to the VOD playback device 150, along with the requested content. In an alternate embodiment, the EMM is sent well in advance, e.g., from the CAS.

[0025] An ECM contains encryption information specific to the program content which, in combination with a valid EMM, can be used to derive a decryption key for decrypting the content. ECMs are typically embedded within the program content, and due to the encryption mechanisms employed cannot be used to derive valid encryption keys absent a valid EMM for the content. EMMs may also include conditional access information, such as information about when, how many times, and under what conditions the content may be viewed/ played.

[0026] Those skilled in the art will appreciate that when the inventive concepts are used with pre-encrypted content, ECM authorizations will change over time. Thus, ECM data embedded in the content will need to be updated with "renewed" ECMs, or ECMs with authorizations based on subscriber specific rights (for example to copy one or more times). With multiple key changes in the content, the server (which "plays out" the content with the ECMs) must know when to switch ECM sets from one crypto period to the next. Several methods to accomplish this synchronization are disclosed herein. It should also be appreciated that the decoder will decrypt (if it has the proper ECMs) by looking at the transport scrambling control bits in the MPEG packet headers.

[0027] A technique that can be used to improve the security of encrypted streaming content such as VOD content is to change the cryptographic keys (encryption keys) at a plurality of points within the content. In order to make it more difficult for "pirates" to steal these keys, it is desirable to use as many different cryptographic keys as possible to encrypt one item of content. However, this creates a number of new issues:

1) Determining the number of sets of cryptographic keys that should be employed to encrypt one item of content, and determining an upper limit on how frequently keys can be changed.

2) Determining how and where, within the program content, to effect the cryptographic key changes, and how to encode those key changes.

3) Determining how to communicate the cryptographic key sets to VOD servers.

4) Determining how to synchronize cryptographic key changes with the corresponding ECMs when the content is streamed to the consumer at time of purchase..

5) Determining how to handle the ECM renewal process.

[0028] The inventive technique addresses these issues by defining a cryptographic key change methodology that permits rapid key changes with straightforward, simple key change synchronization at the time of decryption. This is accomplished, in part, by taking advantage of the MPEG-II data stream structure.

[0029] Present encryption schemes employ a simple, conventional two-key encryption technique to encrypt VOD content. Both keys taken together are essentially a single "cryptographic key set" used to encrypt the entire content. For example, symmetric (i.e., private) keys can be used for encryption. In an alternate implementation, one of the keys can comprise a "public key", and be delivered with the content. The other key is required in combination with the public key to decrypt the content, and is delivered as part of a successful authorization or licensing process. Neither key is useful absent the other key. Although a public key implementation is possible, a private key approach is currently the preferred implementation.

[0030] A problem with encrypting the VOD content with a single set of keys is that an aggressive "attack" using exhaustive cryptographic "cracking" techniques (e.g., a "brute force" approach) could discover a set of keys that will decode the content. Once broken, the content can be reproduced "in the clear" (i.e., unencrypted), thereby completely thwarting the security offered by the encryption scheme. As is well known in the art, key size is a factor in minimizing the likelihood of a successful brute force attack.

[0031] For highest security and greatest protection against cryptographic "cracking" attacks by "pirates", it is highly desirable to increase the number of separate cryptographic keys used by changing the keys at numerous points during the encryption process. The greater the number of "crypto periods" (separately encrypted segments of the content), the more difficult it becomes to "crack" the encryption scheme. If, for example, cryptographic keys were to be changed every 0.5 seconds within a VOD stream (i.e., a crypto period of 0.5 seconds), then the would-be "pirate" would be forced to crack the encryption scheme for each and every 0.5 seconds of content. Each successful breach of encryption security would only produce 0.5 seconds of "clear" (unencrypted) content. For a 90 minute movie, this would require 10,800 separate successful breaches of the encryption scheme. Given the time and effort required to accomplish each breach, this presents a formidable barrier to piracy.

[0032] The inventive technique maintains all cryptographic keys separate from the encoded/encrypted content. A set of ECMs (Entitlement Control Messages) conveying information about a set of keys is multiplexed into the VOD stream by the VOD server when delivering the VOD content to an end user's VOD playback device (e.g. set-top box). A separate EMM (Entitlement Management Message) from an authorization system is delivered to the VOD playback device. The EMM contains the remaining information required to decode/decrypt the VOD content.

[0033] There are two points in the streaming VOD de-

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.