HU000031201T2

(19) **HU**

(11) Lajstromszám: **E 031 201**

(13) **T2**

MAGYARORSZÁG
Szellemi Tulajdon Nemzeti Hivatala

EURÓPAI SZABADALOM
SZÖVEGÉNEK FORDÍTÁSA

(21) Magyar ügyszám: **E 12 713129**
(22) A bejelentés napja: **2012. 04. 02.**

(96) Az európai bejelentés bejelentési száma:
EP 20120713129
(97) Az európai bejelentés közzétételi adatai:
EP 2697979 A1 **2012. 10. 18.**
(97) Az európai szabadalom megadásának meghirdetési adatai:
EP 2697979 B1 **2016. 09. 28.**

(51) Int. Cl.: ***H04N 21/266*** *(2006.01)*
H04N 21/418 *(2006.01)*
H04N 21/45 *(2006.01)*
H04N 21/4623 *(2006.01)*
H04N 21/8358 *(2006.01)*

(86) A nemzetközi (PCT) bejelentési szám:
PCT/EP 12/055938
(87) A nemzetközi közzétételi szám:
WO 12139913

(30) Elsőbbségi adatok:
201161475754 P **2011. 04. 15.** **US**

(72) Feltaláló(k):
KUDELSKI, Henri, CH-1071 Chexbres (CH)

(73) Jogosult(ak):
Nagravision S.A., 1033 Cheseaux-sur-Lausanne (CH)

(74) Képviselő:
Danubia Szabadalmi és Jogi Iroda Kft., Budapest

(54) **Eljárás egy biztonsági modul eredetének azonosítására egy Pay-TV dekóder rendszerben**

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

(11) EP 2 697 979 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
28.09.2016 Bulletin 2016/39

(21) Application number: **12713129.0**

(22) Date of filing: **02.04.2012**

(51) Int Cl.:
H04N 21/266 *(2011.01)* ***H04N 21/418*** *(2011.01)*
H04N 21/4623 *(2011.01)* ***H04N 21/45*** *(2011.01)*
H04N 21/8358 *(2011.01)*

(86) International application number:
PCT/EP2012/055938

(87) International publication number:
WO 2012/139913 (18.10.2012 Gazette 2012/42)

(54) **METHOD TO IDENTIFY THE ORIGIN OF A SECURITY MODULE IN PAY-TV DECODER SYSTEM**

VERFAHREN ZUR IDENTIFIZIERUNG DES URSPRUNGS EINES SICHERHEITSMODULS IN EINEM PAY-TV-DEKODERSYSTEM

PROCÉDÉ POUR IDENTIFIER L'ORIGINE D'UN MODULE DE SÉCURITÉ DANS UN SYSTÈME DÉCODEUR DE TÉLÉVISION PAYANTE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **15.04.2011 US 201161475754 P**

(43) Date of publication of application:
19.02.2014 Bulletin 2014/08

(73) Proprietor: **Nagravision S.A.**
1033 Cheseaux-sur-Lausanne (CH)

(72) Inventor: **KUDELSKI, Henri**
CH-1071 Chexbres (CH)

(74) Representative: **Leman Consulting S.A.**
Chemin de Précossy 31
1260 Nyon (CH)

(56) References cited:
WO-A1-2004/082286
US-A1- 2009 080 689
US-A1- 2009 097 659
US-A1- 2010 169 349

EP 2 697 979 B1

Printed by Jouve, 75001 PARIS (FR)

Description

INTRODUCTION

[0001] The present invention relates to the domain of conditional access systems and more particularly to methods for uncovering the identity of an apparatus used in the practice of unauthorised redistribution of secret encryption keys.

STATE OF THE ART

[0002] One area in which the present invention may be of particular interest is in the domain of pay-TV, where broadcast proprietary audio/video content is offered by an operator at a fee to a plurality of subscribing consumers. Conditional access systems are employed to handle the processing of pay-TV content, with a view to ensuring that only consumers who have subscribed to certain services, usually by payment of a fee to the operator or provider of those services, actually have access to the content provided for those services. According to such conditional access systems, the content is encrypted by the operator under control words, the latter being supplied to the subscribing consumers via security messages, which are either broadcast in a data stream along with the content or may be distributed by some other means. Each subscribing consumer is supplied with an appropriate receiver comprising a security module to allow for the extraction of the control words from the security messages and a descrambling unit for decrypting the broadcast encrypted audio/video content.

[0003] Encrypted audio/video content has value and as such, conditional access systems have been the target for attack by malicious third parties intent on gaining access to the audio/video content without subscribing to the services of the operator and without being in possession of the necessary authorised reception equipment. A practice commonly known as control word sharing, whereby the control words broadcast along with encrypted content are extracted by a malicious third party using valid security modules and re-distributed freely to other malicious third parties, is a particularly significant threat to operators offering pay-TV services since it deprives them of revenue from which they would otherwise have benefited.

[0004] Pay-TV operators therefore have a great interest in being able to trace receiver units which are used in control word sharing activities as this allows the operator to take action against those involved in such activities. United States Patent Application Publication No. 2002/0,133,701A describes a method for tracing traitor receivers in a broadcast encryption system. The method includes using a false key to encode plural subsets representing receivers in the system. The subsets are derived from a tree using a Subset-Cover system, and the traitor receiver is associated with one or more compromised keys that have been obtained by a potentially cloned pirate receiver. Using a clone of the pirate receiver, the identity of the traitor receiver is determined. This system however has the disadvantage that multiple encodings of the same content have to be broadcast, thus having a negative impact on broadcast bandwidth efficiency.

[0005] The document US 2009/0097659 describes a solution to trace a rogue receiver by encrypting at least some packets of the transmitted stream by different group keys. Each receiver belongs to a group and receives the keys necessary to decrypt the packet pertaining to said group.

[0006] When one of said group keys are found to an illegitimate person, this is the proof that one receiver of said group is not longer trustworthy. The group is then divided into smaller groups in order to point toward the rogue receiver by iterating steps.

[0007] The document US 2009/0080689 describes a solution for watermarking a content. A pre-processing unit generates one or more alternate values for an original value of the content. The alternate values are added to the content as metadata. On the recipient side, the metadata are processed and one alternate value (or the original value) is selected according to an internal parameter such as an identifier uniquely identifying the recipient. The selected alternate value is used to update the content to produce a watermarked content.

[0008] The document US 2010/0169349 describes a similar solution as the previous document. The content is analysed to produce Metada according to a watermarking scheme. At the reception, the Metadata and a payload, which could the serial number of the player, are used to introduce modification into the original content. The final result is a watermarked content comprising information allowing to later recover the payload.

[0009] The document WO 2004/082286 describes a conditional access system in which the content is encrypted by control words. The control word is then embedded into an ECM and encrypted by a service key. Said service key is then as well embedded into an EMM which comprises as well unique or group addresses of the intended receivers. The aim of this document is to reduce the harm caused by the leak of a service key. For that purpose, the same control word is encrypted by two different service keys and sent in two distinct ECM. The first service key is sent via an EMM to a first set of decoders and the second service key is sent to a second set of receivers. In case that one set of compromised, this set is divided into a smaller group and the keys are to be changed to grant access only the participants of the group.

Brief description of the invention

[0010] This invention proposes a solution to identify the origin of a security module in pay-ty system according to the following method :

[0011] Method to identify the origin of a security module

in pay-tv decoder system this method comprising the steps of :

- receiving by the pay-tv decoder system a service comprising at least a first stream, a second stream and a control word stream, the second stream being a duplicate of the first stream, said first stream being encrypted by a first control word (CW1) and said second stream being encrypted by a second control word stream (CW2),
- extracting from the control word stream, entitlement messages containing at least one main control word (CW) allowing to retrieve the first and the second control words, and access conditions,
- transferring the control word stream to the security module,
- extracting the entitlement messages from the control word stream and checking the access conditions,
- if the access conditions are met, determining the first and second control words from the main control word in the entitlement message,
- determining an internal parameter of the security module, this internal parameter being unique per security module,

characterized in that, it further comprises the steps of :

- selecting a current control word from the first or the second control word based on part of the internal parameter, corresponding to the first or the second stream,
- transmitting the current control word to the pay-tv decoder,
- selecting a current stream from the first or the second stream in accordance with the selection of the first or the second control word,
- decrypting the current stream with the current control word.

Brief description of the figures

[0012] This invention will be better understood thanks to the attached figures in which :

- the figure 1 illustrates the devices of the invention, namely a pay-tv decoder system,
- the figure 2 illustrates the resulting stream.

Description of the invention

[0013] The present invention proposes to duplicate at least one of the elementary streams of a service and to encrypt this supplemental stream by a particular control word. A service comprises several elementary streams assembled together to form a service, such as a video stream, an audio stream and data stream (for carrying the control messages ECM).

[0014] These elementary streams are described in the PMT (Program Map Table). The Program Map Tables (PMTs) contain information about services. For each service, there is one PMT. The PMTs provide information on each service present in the transport stream, including the program_number, and list the elementary streams that comprise the described MPEG-2 program. There are also locations for optional descriptors that describe the entire MPEG-2 program, as well as an optional descriptor for each elementary stream. Each elementary stream is labeled with a stream_type value.

[0015] The present invention will describe as an example the duplication of an audio stream. However, the same method can be applied with a video stream in case that the bandwidth is not an issue.

[0016] As it is well known from the man skilled in the art, the security module can essentially be realised according to four distinct forms. One of these forms is a microprocessor card, a smart card, or more generally an electronic module (taking the form of key, a badge,...). Such a module is generally removable and connectable to the decoder.

[0017] The form with electric contacts is the most widely used, but a connection without contact for example of the type ISO 14443 is not excluded.

[0018] A second known form is that of an integrated circuit box, generally placed definitively and irremovably in the decoder. An alternative is made up of a circuit mounted on a base or connector such as a SIM module connector.

[0019] In a third form, the security module is integrated into an integrated circuit box also having another function, for example in a descrambling module of the decoder or in the microprocessor of the decoder.

[0020] In a fourth embodiment, the security module is not realised in hardware, but its function is implemented only in software form. Given that in the four cases, the function is identical although the security level differs, we can talk about a security module regardless of the way in which its function is carried out or the form that this module may take.

[0021] The audio stream is duplicated, each audio stream is then encrypted by a different key or control word.

[0022] Both encrypted streams (audio1, audio2) are then assembled with the other streams to form the service. The various streams are identified in the PMT and the keys for the first and the second audio stream are included in the data stream.

[0023] The keys, also named Control-Words are embedded into Entitlement Control Messages which comprises also the right requirements for having access to the encrypted content. In general, a message contain the current control-word and the next control-word i.e. the control word that applies on the future data when after a key change.

[0024] According to a first embodiment, the message comprises four control-words, two by streams (current and next). According to another embodiment, two messages are provided to the security module, each message being dedicated to only one stream.

[0025] Since the service comprises several streams, and only one is duplicated, the method of the invention is preferably based on the use of three control words. One (CW1) for the first stream, one (CW2) for the duplicated first stream, and one (CW3) for the other streams. As far as the decoder is concerned, only two control words will be provided at a time, i.e. CW1 and CW3 or CW2 and CW3 by the security module.

[0026] The security module process the received message, i.e. decrypt the same with a transmission key pertaining to the broadcasting system and extract the access conditions as well as the control-words.

[0027] The security module verifies that the access conditions are met, i.e. the memory of the security module contains the rights referred by the access conditions. These rights are loaded into the security module preferably by messages uniquely addressed to said security module and encrypted by a personal key of this security module.

[0028] Each security module (SM) in a collection of security modules (SM) managed by the operator (OP) is uniquely identifiable by an internal setting (UA) which is particular to the security module (SM). Each security module (SM) is instructed to select one of the control words (CW) according to its unique internal setting (UA). The internal setting (UA) could be for example the value of a register representing the security module's unique address. Preferably, the security module (SM) is instructed to select the control word (CW) according to the value of the nth bit of its unique address for example.

[0029] For the sake of understanding the control word for the first steam will be named first control word CW1, the control word for the duplicated steam (second stream) will be named second control word CW2, and the control word for the other stream (or streams) will be named third control word CW3.

[0030] As a consequence, based on an internal parameter, the security module selects the first of the second control-word and returns it to the decoder. The control words used for the decryption of the streams are not necessarily extracted for the ECM. The security module can extract one main control word from the ECM and produce the first and the second words with a cryptographic function from the third control word. This function will be preferably initialized by a parameter known by all security modules. Of course, any one of the control word can be used as initial control word to produce the other control words.

[0031] It is important that the decoder selects the correct stream with the corresponding control word. This can be done by different means i.e. by an instruction of the security module or by the decoder itself.

[0032] In the same way that the security module sends instructions to the decoder DEC, the security module informs the decoder of the stream to be processed. It is worth noting that the decoder has set the filter FI of the elementary to both streams. Only one among the first or second stream is selected to be passed to the descrambler DSC. The information received from the security module will be used to select the proper stream among the streams, preferably when the control word changes. The decoder stores temporary the stream selection and analyses the current stream. When a control-word change is detected, the new stream selection is applied so that the descrambler receives the correct stream matching the control-word received previously.

[0033] In case that the decoder can decide itself on which stream is to the processed, the decoder is aware of the internal parameter used for the selection and applies the same selection. The unique address UA of the security module is known by the decoder.

[0034] In a particular embodiment of the present invention, an initialised sweep register (CNTR) is used to point to a particular bit in the unique address of the security module. When initialised, the sweep register points to the first bit of the unique address and the state of that bit is used to select one from the two control words. When the selection has been made the sweep register increments and the next bit of the unique address is used to select one of the first or second control words. This process is continued until all of the bits of the unique address have been used, whereupon the sweep register is reinitialised. The control words from the security messages may be processed as and when they arrive or they may be stored in a control word table (CWT) and processed on demand or according to a time-based regime.

[0035] The figure 2 illustrates the result of the streams after the selection of the first (ST1) or second (ST2) stream according to the state of the corresponding bit of the internal parameter UA.

[0036] According to another embodiment of the present invention, rather than the command driven processing described above, a more automated method may be used. In this embodiment the security message (ECM) or the management message (EMM) further comprises information related to time - time of day for example. This information may be used to further indicate at what time the selection of the control word should be made. It is then possible to send a command to a group of security modules to determine if a member of that group is used fraudulently. In the positive event, the size of the group can be reduced until the proper security module is located.

[0037] The advantage of the turning on or off this dual

control word method is to select the time when a duplicate stream is present. It is not necessary to duplicate a stream at all time, the method can be started for a short period, thus reducing the impact on the bandwidth.

[0038] Furthermore, a hash function performed on the time-related information yields a value which may be used to point to a particular bit of the unique address to use in selecting one from the pair of control words. For example, for a 32-bit unique address, a modulo-32 of the result of the hash of the time-related information would point to one of the 32 bits from the unique address.

[0039] According to another aspect of the invention, the duplicate stream is not a copy of the first stream. The second stream contains some modification such as watermarking in a way that the modifications are visually undetectable by the end user. As a consequence, the resulting output of the descrambler will alternatively contain the first and the second stream, the change from the first to the second being dictate by the internal parameter of the descrambler.

Claims

1. A method to identify the origin of a security module in pay-tv decoder system this method comprising the steps of :

   - receiving by the pay-tv decoder system a service comprising at least a first stream, a second stream and a control word stream, the second stream being a duplicate of the first stream, said first stream being encrypted by a first control word (CW1) and said second stream being encrypted by a second control word (CW2),
   - extracting from the control word stream, entitlement messages containing at least one main control word (CW) allowing to retrieve the first and the second control words, and access conditions,
   - transferring the control word stream to the security module,
   - extracting the entitlement messages from the control word stream and checking the access conditions,
   - if the access conditions are met, determining the first and second control words from the main control word in the entitlement message,
   - determining an internal parameter of the security module, this internal parameter being unique per security module,
   - selecting a current control word from the first or the second control word based on part of the internal parameter, corresponding to the first or the second stream,
   - transmitting the current control word to the pay-tv decoder,
   - selecting a current stream from the first or the second stream in accordance with the selection of the first or the second control word,
   - decrypting the current stream with the current control word,

   characterized in that, the internal parameter is a unique address of the security module and having a plurality of bits, and the method comprises the steps of :

   a. initializing a sweep register (CNTR) pointing to the first bit of the unique address,
   b. using the sweep register to point to a bit of the unique address,
   c. using the state of said bit to select the current control word,
   d. incrementing the sweep register to point to the next bit of the unique address each time the selection of a current control word from the first or the second control word is performed,
   e. repeating the steps b to d until all of the bits of the unique address have been used, and reinitializing the sweep register.

2. Method of claim 1, wherein the entitlement message comprises the first and the second control words.

3. Method of claim 1, wherein the first and the second control word are calculated from the main control word using a cryptographic function.

4. Method of claim 3, wherein the cryptographic function is initialized by a parameter common to all security modules.

5. Method of any of the claim 1 to 4, wherein the selection of the current stream by the pay-tv decoder is triggered by an instruction received from the security module.

6. Method of any of the claim 1 to 4, wherein the selection of the current stream by the pay-tv decoder is triggered by the selection of the same part of the internal parameter by the pay-tv decoder.

7. Method of any of the claims 1 to 6, wherein the first and the second stream are streams carrying the same audio or video information.

8. Method of any of the claims 1 to 6, wherein at least the first stream comprises a mark allowing to distinguishing said first stream from said second stream.

9. Method according to claim 8, wherein the first stream is an audio stream and the mark is an unperceived audio mark.

10. Method according to claim 8, wherein the first stream

is a video stream and the mark is an unperceived video mark.

11. A pay-tv decoder system (DEC) comprising a security module (SM) to identify the origin of a security module in pay-tv decoder system, the pay-tv decoder system being configured to :

- receives a service comprising at least a first stream, a second stream and a control word stream, the second stream being a duplicate of the first stream, said first stream being encrypted by a first control word (CW1) and said second stream being encrypted by a second control word (CW2),
- extracts from the control word stream, entitlement messages containing at least one main control word (CW) allowing to retrieve the first and the second control words, and access conditions,
- transfers the control word stream to the security module,
- selects a current stream from the first or the second stream in accordance with the selection of the first or the second control word,
- decrypts the current stream with a current control word,

said security module being configured to :

- determines an internal parameter of the security module, this internal parameter being unique per security module,
- extracts the entitlement messages from the control word stream and checks the access conditions,
- if the access conditions are met, determines the first and second control words from the main control word in the entitlement message,
- selects the current control word from the first or the second control word based on part of the internal parameter, corresponding to the first or the second stream,
- transmits the current control word to the pay-tv decoder (DEC),

characterized in that, the internal parameter is a unique address of the security module and having a plurality of bits, said security module (SC) being further configured to :

a. initialize a sweep register (CNTR) thus pointing to the first bit of the unique address,
b. use the sweep register to point to a bit of the unique address,
c. use the state of said bit to select the current control word,
d. increment the sweep register to point to the next bit of the unique address each time the selection of a current control word from the first or the second control word is performed,
e. repeat the steps b to d until all of the bits of the unique address have been used, and reinitialize the sweep register.

Patentansprüche

1. Verfahren, um die Herkunft eines Sicherheitsmoduls in einem Pay-TV-Decodersystem zu identifizieren, mit folgenden Phasen:

- Empfang, durch das Pay-TV-Decodersystem, eines Dienstes mit mindestens einem ersten Strom, einem zweiten Strom und einem Kontrollwortstrom, wobei der zweite Strom ein Duplikat des ersten Stromes ist, wobei besagter erster Strom durch ein erstes Kontrollwort (CW1) verschlüsselt wird und der zweite Strom durch ein zweites Kontrollwort (CW2) verschlüsselt wird,
- Extrahieren, aus dem Kontrollwortstrom, von Zugriffsmeldungen, die mindestens ein Hauptkontrollwort (CW) enthalten, das es gestattet, das erste und das zweite Kontrollwort und Zugangsbedingungen abzurufen,
- Übertragung des Kontrollwortstroms an das Sicherheitsmodul,
- Extrahieren der Zugriffsmeldungen aus dem Kontrollwortstrom und Kontrolle der Zugangsbedingungen,
- wenn die Zugangsbedingungen erfüllt sind, Bestimmung des ersten und zweiten Kontrollworts aus dem Hauptkontrollwort in der Zugriffsmeldung,
- Ermittlung eines internen Parameters des Sicherheitsmoduls, wobei dieser interne Parameter für jedes Sicherheitsmodul eindeutig ist,
- Auswahl eines aktuellen Kontrollworts aus dem ersten oder dem zweite Kontrollwort auf der Grundlage eines Teils des internen Parameters, entsprechend dem ersten oder dem zweiten Strom,
- Übertragung des aktuellen Kontrollworts an den Pay-TV-Decoder,
- Auswahl eines aktuellen Stroms aus dem ersten oder dem zweiten Strom in Übereinstimmung mit der Auswahl des ersten oder des zweiten Kontrollworts,
- Entschlüsselung des aktuellen Stroms mit dem aktuellen Kontrollwort, **gekennzeichnet dadurch, dass** der interne Parameter eine eindeutige Adresse des Sicherheitsmoduls ist und eine Vielzahl von Bits umfasst, wobei das Verfahren folgende Phasen umfasst:

a. Initialisieren eines Sweep-Registers (CNTR), das auf das erste Bit der eindeutigen Adresse weist,
b. Verwendung der Sweep-Registers, um auf ein Bit der eindeutigen Adresse zu weisen,
c. Verwendung des Zustandes des besagten Bits, um das aktuelle Kontrollwort auszuwählen,
d. Erhöhen des Sweep-Registers, um auf das nächste Bit der eindeutigen Adresse zu weisen, jedes Mal wenn die Auswahl eines aktuellen Kontrollworts aus dem ersten oder dem zweiten Kontrollwort durchgeführt wird,
e. Wiederholung der Phasen b bis d, bis alle Bits der eindeutigen Adresse verwendet wurden, und Neuinitialisierung des Sweep-Registers.

2. Verfahren nach Anspruch 1, wobei die Zugriffsmeldung das erste und das zweite Kontrollwort umfasst.

3. Verfahren nach Anspruch 1, wobei das erste und das zweite Kontrollwort aus dem Hauptkontrollwort unter Verwendung einer kryptographischen Funktion berechnet werden.

4. Verfahren nach Anspruch 3, wobei die kryptographische Funktion von einem Parameter initialisiert wird, der allen Sicherheitsmodulen gemein ist.

5. Verfahren nach einem beliebigen der Ansprüche 1 bis 4, wobei die Auswahl des aktuellen Stroms durch den Pay-TV-Decoder durch eine Anweisung ausgelöst wird, die von dem Sicherheitsmodul empfangen wird.

6. Verfahren nach einem beliebigen der Ansprüche 1 bis 4, wobei die Auswahl des aktuellen Stroms durch der Pay-TV-Decoder durch die Auswahl desselben Teils des internen Parameters durch den Pay-TV-Decoder ausgelöst wird.

7. Verfahren nach einem beliebigen der Ansprüche 1 bis 6, wobei der erste und der zweite Strom dieselben Audio- oder Video-Informationen enthalten.

8. Verfahren nach einem beliebigen der Ansprüche 1 bis 6, wobei mindestens der erste Strom eine Markierung umfasst, durch die man den ersten Strom vom zweiten Strom unterscheiden kann.

9. Verfahren nach Anspruch 8, wobei der erste Strom ein Audiostrom ist und die Markierung eine unbemerkte Audiomarkierung ist.

10. Verfahren nach Anspruch 8, wobei der erste Strom ein Videostrom ist und die Markierung eine unbemerkte Videomarkierung ist.

11. Pay-TV-Decodersystem (DEC) mit einem Sicherheitsmodul (SM), um die Herkunft eines Sicherheitsmoduls in einem Pay-TV-Decodersystem zu identifizieren, wobei das Pay-TV-Decodersystem wie folgt konfiguriert ist:

- es empfängt einen Dienst mit mindestens einem ersten Strom, einem zweiten Strom und einem Kontrollwortstrom, wobei der zweite Strom ein Duplikat des ersten Stroms ist, wobei besagter erster Strom von einem ersten Kontrollwort (CW1) verschlüsselt wird und der zweite Strom durch ein zweites Kontrollwort (CW2) verschlüsselt wird,
- es extrahiert aus dem Kontrollwortstrom Zugriffsmeldungen, die mindestens ein Hauptkontrollwort (CW) enthalten, das es gestattet, das erste und das zweite Kontrollwort und Zugangsbedingungen abzurufen,
- es überträgt den Kontrollwortstrom an das Sicherheitsmodul,
- es wählt einen aktuellen Strom aus dem ersten oder dem zweiten Strom in Übereinstimmung mit der Auswahl des ersten oder des zweiten Kontrollworts aus,
- es entschlüsselt den aktuellen Strom mit einem aktuellen Kontrollwort,

wobei das Sicherheitsmodul wie folgt konfiguriert ist:

- es bestimmt einen internen Parameter des Sicherheitsmoduls, wobei dieser interne Parameter für jedes Sicherheitsmodul eindeutig ist,
- es extrahiert die Zugriffsmeldungen aus dem Kontrollwortstrom und kontrolliert die Zugangsbedingungen,
- wenn die Zugangsbedingungen erfüllt sind, bestimmt es das erste und das zweite Kontrollwort aus dem Hauptkontrollwort in der Zugriffsmeldung,
- es wählt das aktuelle Kontrollwort aus dem ersten oder dem zweiten Kontrollwort auf der Grundlage eines Teils des internen Parameters aus, entsprechend dem ersten oder dem zweiten Strom,
- es überträgt das aktuelle Kontrollwort an den Pay-TV-Decoder (DEC), **gekennzeichnet dadurch, dass** der interne Parameter eine eindeutige Adresse des Sicherheitsmoduls ist und eine Vielzahl von Bits umfasst, wobei das Sicherheitsmodul (SC) des Weiteren wie folgt konfiguriert ist:

a. es initialisiert ein Sweep-Register (CNTR), das so auf das erste Bit der eindeutigen

Adresse weist,
b. es verwendet das Sweep-Register, um auf ein Bit der eindeutigen Adresse zu weisen,
c. es verwendet den Zustand dieses Bits, um das aktuelle Kontrollwort auszuwählen,
d. es erhöht das Sweep-Register, um auf das nächste Bit der eindeutigen Adresse zu weisen, jedes Mal wenn die Auswahl eines aktuellen Kontrollworts aus dem ersten oder zweiten Kontrollwort durchgeführt wird,
e. es wiederholt die Phasen b bis d, bis alle Bits der eindeutigen Adresse verwendet wurden, und initialisiert das Sweep-Register neu.

Revendications

1. Méthode pour identifier l'origine d'un module de sécurité dans un système de décodeur de télévision à péage, cette méthode comprenant les étapes de:

   - recevoir par le système de décodeur de télévision à péage un service comprenant au moins un premier flux, un deuxième flux et un flux de mot de contrôle, le deuxième flux étant un double du premier flux, ledit premier flux étant crypté par un premier mot de contrôle (CW1) et ledit deuxième flux étant crypté par un deuxième mot de contrôle (CW2),
   - extraire à partir du flux de mot de contrôle, des messages de droit d'accès contenant au moins un mot de contrôle principal (CW) permettant de récupérer le premier et le deuxième mot de contrôle, et des conditions d'accès,
   - transférer le flux de mot de contrôle au module de sécurité,
   - extraire des messages de droits d'accès du flux de mot de contrôle et vérifier les conditions d'accès,
   - si les conditions d'accès sont remplies, déterminer le premier et le deuxième mot de contrôle à partir du mot de contrôle principal dans le message de droit d'accès,
   - déterminer un paramètre interne du module de sécurité, ce paramètre interne étant unique pour chaque module de sécurité,
   - sélectionner un mot de contrôle actuel à partir du premier ou du deuxième mot de contrôle en fonction d'une partie du paramètre interne, qui correspond au premier ou au deuxième flux,
   - transmettre le mot de contrôle actuel au décodeur de télévision à péage,
   - sélectionner un flux actuel à partir du premier ou du deuxième flux selon la sélection du premier ou du deuxième mot de contrôle,
   - décrypter le flux actuel avec le mot de contrôle actuel,

   caractérisée en ce que le paramètre interne est une adresse unique du module de sécurité et ayant une pluralité de bits, et la méthode comprend les étapes de:

   a. initialiser un registre de balayage (CNTR) pointant vers le premier bit de l'adresse unique,
   b. utiliser le registre de balayage pour pointer vers un bit de l'adresse unique,
   c. utiliser l'état dudit bit pour sélectionner le mot de contrôle actuel,
   d. augmenter le registre de balayage pour pointer vers le bit suivant de l'adresse unique à chaque fois que la sélection d'un mot de contrôle actuel à partir du premier ou du deuxième mot de contrôle est effectuée,
   e. répéter les étapes b à d jusqu'à ce que tous les bits de l'adresse unique aient été utilisés, et réinitialiser le registre de balayage.

2. Méthode selon la revendication 1, où le message de droit d'accès comprend le premier et le deuxième mot de contrôle.

3. Méthode selon la revendication 1, où le premier et le deuxième mot de contrôle sont calculés à partir du mot de contrôle principal utilisant une fonction cryptographique.

4. Méthode selon la revendication 3, où la fonction cryptographique est initialisée par un paramètre commun à tous les modules de sécurité.

5. Méthode selon l'une quelconque des revendications 1 à 4, où la sélection du flux actuel par le décodeur de télévision à péage est déclenchée par une instruction reçue du module de sécurité.

6. Méthode selon l'une quelconque des revendications 1 à 4, où la sélection du flux actuel par le décodeur de télévision à péage est déclenchée par la sélection de la même partie du paramètre interne par le décodeur de télévision à péage.

7. Méthode selon l'une quelconque des revendications 1 à 6, où le premier et le deuxième flux sont les flux portant les mêmes informations audio ou vidéo.

8. Méthode selon l'une quelconque des revendications 1 à 6, où au moins le premier flux comprend une marque permettant de distinguer ledit premier flux dudit deuxième flux.

9. Méthode selon la revendication 8, où le premier flux est un flux audio et la marque est une marque audio

inaperçue.

10. Méthode selon la revendication 8, où le premier flux est un flux vidéo et la marque est une marque vidéo inaperçue.

11. Système de décodeur de télévision à péage (DEC) comprenant un module de sécurité (SM) pour identifier l'origine d'un module de sécurité dans un système de décodeur de télévision à péage, le système de décodeur de télévision à péage étant configuré pour:

- recevoir un service comprenant au moins un premier flux, un deuxième flux et un flux de mot de contrôle, le deuxième flux étant un double du premier flux, ledit premier flux étant crypté par un premier mot de contrôle (CW1) et ledit deuxième flux étant crypté par un deuxième mot de contrôle (CW2),
- extraire du flux de mot de contrôle, des messages de droit d'accès contenant au moins un mot de contrôle principal (CW) permettant de récupérer le premier et le deuxième mot de contrôle, et des conditions d'accès,
- transférer le flux de mot de contrôle au module de sécurité,
- sélectionner un flux actuel à partir du premier ou du deuxième flux selon la sélection du premier ou du deuxième mot de contrôle,
- décrypter le flux actuel avec un mot de contrôle actuel,

ledit module de sécurité étant configuré pour:

- déterminer un paramètre interne du module de sécurité, ce paramètre interne étant unique pour chaque module de sécurité,
- extraire les messages de droit d'accès du flux de mot de contrôle et vérifier les conditions d'accès,
- si les conditions d'accès sont remplies, déterminer le premier et deuxième mot de contrôle à partir du mot de contrôle principal dans le message de droit d'accès,
- sélectionner le mot de contrôle actuel à partir du premier ou du deuxième mot de contrôle en fonction d'une partie du paramètre interne, qui correspond au premier ou au deuxième flux,
- transmettre le mot de contrôle actuel au décodeur de télévision à péage (DEC), **caractérisé en ce que** le paramètre interne est une adresse unique du module de sécurité et ayant une pluralité de bits, ledit module de sécurité (SC) étant configuré en outre pour:

a. initialiser un registre de balayage (CNTR) ainsi pointant vers le premier bit de l'adresse unique,
b. utiliser le registre de balayage pour pointer vers un bit de l'adresse unique,
c. utiliser l'état dudit bit pour sélectionner le mot de contrôle actuel,
d. augmenter le registre de balayage pour pointer vers le bit suivant de l'adresse unique à chaque fois que la sélection d'un mot de contrôle actuel à partir du premier ou du deuxième mot de contrôle est effectuée,
e. répéter les étapes b à d jusqu'à ce que tous les bits de l'adresse unique aient été utilisés, et réinitialiser le registre de balayage.

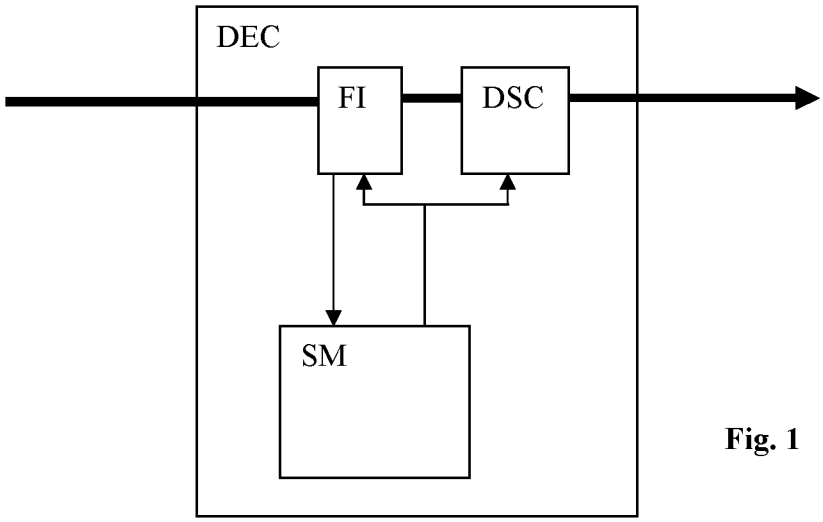

Fig. 1

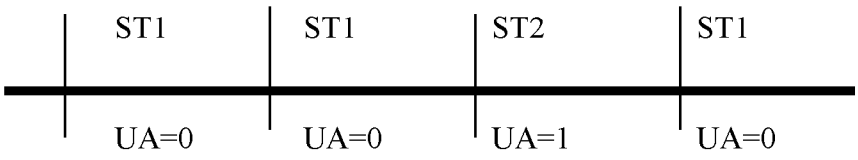

Fig. 2

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20020133701 A **[0004]**
- US 20090097659 A **[0005]**
- US 20090080689 A **[0007]**
- US 20100169349 A **[0008]**
- WO 2004082286 A **[0009]**

Eljárás egy biztonsági modul eredetének azonosítására egy Pay-TV dekóder rendszerben

Szabadalmi igénypontok

1. Eljárás egy biztonsági modul eredetének azonosítására PayTV dekóder rendszerben, az eljárás a következő lépéseket tartalmazza:

– a Pay-TV dekóder rendszerrel egy szolgáltatás vétele, amely legalább egy első folyamot, egy második folyamot és egy vezérlőszó folyamot tartalmaz, ahol a második folyam az első folyam kétszerese, az említett első folyamot egy első vezérlőszó (CW1) és az említett második folyamot egy második vezérlőszó (CW2) kódolja,

– a vezérlőszó folyamból jogosultság üzenetek kivonása, amelyek legalább egy olyan fő vezérlőszót (CW) tartalmaznak, amely lehetővé teszi az első és a második vezérlőszó, és hozzáférési feltételek visszakeresését,

– a vezérlőszó folyam átvitele a biztonsági modulhoz,

– a jogosultság üzenetek kivonása a vezérlőszó folyamból és a hozzáférési feltételek ellenőrzése,

– ha a hozzáférési feltételek teljesültek, az első és második vezérlőszó meghatározása a jogosultság üzenetben lévő fő vezérlőszóból,

– a biztonsági modul egy belső paraméterének meghatározása, ez a belső paraméter biztonsági modulonként egyedi,

– egy aktuális vezérlőszó kiválasztása az első vagy a második vezérlőszóból, az első vagy a második folyam szerinti belső paraméter egy része alapján,

– az aktuális vezérlőszó átvitele a Pay-TV dekóderhez,

– egy aktuális folyam kiválasztása az első vagy a második folyamból az első vagy a második vezérlőszó kiválasztásával összhangban,

– az aktuális folyam dekódolása az aktuális vezérlőszóval,

azzal jellemezve, hogy a belső paraméter a biztonsági modul egy egyedi címe, és több bitet tartalmaz, és az eljárás tartalmazza a következő lépéseket:

a. az egyedi cím első bitjére mutató pásztázási regiszter (CMTR) inicializálása,

b. a pásztázási regiszter használata az egyedi cím egy bitjére mutatására,

c. az említett bit állapotának használata az aktuális vezérlőszó kiválasztásához,

d. a pásztázási regiszter értékének növelése, hogy az egyedi cím egy következő bitjére mutasson, minden esetben, amikor egy aktuális vezérlőszó kiválasztását végezzük az első vagy a második vezérlőszó közül,

e. a b-d. lépések ismétlése, amíg az egyedi cím összes bitjét felhasználjuk, és a pásztázási regiszter újbóli inicializálása.

2. Az 1. igénypont szerinti eljárás, ahol a jogosultság üzenet tartalmazza az első és a második vezérlőszót.

3. Az 1. igénypont szerinti eljárás, ahol az első és második vezérlőszót a fő vezérlőszóból számítjuk ki rejtjelező

függvény használatával.

4. A 3. igénypont szerinti eljárás, ahol a rejtjelező függvényt az összes biztonsági modulra közös paraméterrel inicializáljuk.

5. Az 1-4. igénypontok bármelyike szerinti eljárás, ahol az aktuális folyam Pay-TV dekóderrel történő kiválasztását a biztonsági modultól kapott utasítással váltjuk ki.

6. Az 1-4. igénypontok bármelyike szerinti eljárás, ahol az aktuális folyam Pay-TV dekóderrel történő kiválasztását a belső paraméter azonos részének a Pay-TV dekóder általi kiválasztása útján váltjuk ki.

7. Az 1-6. igénypontok bármelyike szerinti eljárás, ahol az első és a második folyam ugyanazt az audió vagy videó információt hordozó folyam.

8. Az 1-6. igénypontok bármelyike szerinti eljárás, ahol legalább az első folyam egy jelölést tartalmaz, amely lehetővé teszi az említett első folyam megkülönböztetését az említett második folyamtól.

9. A 8. igénypont szerinti eljárás, ahol az első folyam egy audió folyam és a jelölés egy nem észlelt audió jelölés.

10. A 8. igénypont szerinti eljárás, ahol az első folyam egy videó folyam és a jelölés egy nem észlelt videó jelölés.

11. Pay-TV dekóder rendszer (DEC), amely egy biztonsági modult (SM) tartalmaz egy Pay-TV dekóder rendszerben lévő biztonsági modul eredetének azonosítására, a Pay-TV dekóder rendszer úgy van konfigurálva, hogy:

– vegyen egy szolgáltatást, amely legalább egy első folyamot, egy második folyamot és egy vezérlőszó folyamot tartalmaz, ahol a második folyam az első folyam kétszerese, az említett első folyamot egy első vezérlőszó (CW1) és az említett második folyamot egy második vezérlőszó (CW2) kódolja,

– a vezérlőszó folyamból jogosultság üzeneteket vonjon ki, amelyek legalább egy olyan fő vezérlőszót (CW) tartalmaznak, amely lehetővé teszi az első és a második vezérlőszó, és hozzáférési feltételek visszakeresését,

– a vezérlőszó folyamot átvigye a biztonsági modulhoz,

– kiválasszon egy aktuális folyamot az első vagy a második folyamból az első vagy a második vezérlőszó kiválasztásával összhangban,

– dekódolja az aktuális folyamot egy aktuális vezérlőszóval,

az említett biztonsági modul úgy van konfigurálva, hogy:

– meghatározza a biztonsági modul egy belső paraméterét, ez a belső paraméter biztonsági modulonként egyedi,

– kivonja a jogosultság üzeneteket a vezérlőszó folyamból és ellenőrizze a hozzáférési feltételeket,

– ha a hozzáférési feltételek teljesültek, meghatározza az első és második vezérlőszót a jogosultság üzenetben lévő fő vezérlőszóból,

– kiválassza az aktuális vezérlőszót az első vagy a második vezérlőszóból, az első vagy második folyam szerinti belső paraméter része alapján,

– átvigye az aktuális vezérlőszót a Pay-TV dekóderhez (DEC),

azzal jellemezve, hogy a belső paraméter a biztonsági modul egy egyedi címe, és több bitet tartalmaz, az említett biztonsági modul (SC) úgy van továbbá konfigurálva, hogy:

a. inicializálja az egyedi cím első bitjére mutató pásztázási regisztert (CMTR),

b. a pásztázási regisztert használja az egyedi cím egy bitjére mutatására,

c. az említett bit állapotát használja az aktuális vezérlőszó kiválasztásához,

d. a pásztázási regiszter értékét növelje, hogy az egyedi cím egy következő bitjére mutasson, minden esetben, amikor egy aktuális vezérlőszó kiválasztása történik az első vagy a második vezérlőszó közül,

e. a b-d. lépéseket ismételje az egyedi cím összes bitjének felhasználásáig, és a pásztázási regisztert újból inicializálja.