159159

METHOD AND SYSTEM FOR TRANSMISSION OF DECRYPTING INFORMATION

This invention concerns a process and system of decrypting information (data) transmission between a management system and a subscriber's decoder.

The decoders of subscribers of Pay-TV contain a decrypting unit able to treat the arriving signals by cable or by hertz. These signals can be analog or digital.

These signals are of different types, according to whether they contain audio type information, video or of control.

The latter category includes management messages (called EMM messages) that is to say messages containing controls directed to a decoder or to a group of decoders, and control messages (called ECM messages), that is to say containing authorization messages among others, information allowing to decrypt the signals in transmission.

In the present application, we refer to authorization messages (ECM) destined to the decrypting of the audio and video signals.

The offer proposed to subscribers of Pay-TV includes many channels each of which encrypted according to one or more particular keys. This is necessary because of the fact that a subscriber can undertake a subscription for a channel without having the right to take advantage of others channels.

The authorization messages (ECM) are encrypted with a key suitable for the management system. The subscriber's decoder includes a security cryptographic unit able to decrypt these messages. For security reasons, the authorization information allowing the decrypting of the useful signals (video and audio) are changed periodically. The management system transmits these messages (ECM) under encrypted form to the cryptographic unit able to decrypt these messages, manages the authorizations and according to the rights of the subscriber, transmits to the decoder the information necessary for the decrypting of video and audio signals.

G00002

The result of the decrypting by the cryptographic unit is called "control word" abbreviated with "CW". The control-words pilot the decoder and the subscriber can thus have the full advantage of the transmitted information.

As indicated above, these control-words are changed regularly in order to prevent a pirate to calculate this information of control by means of a powerful computer, and benefit free of charge from a paying service. This is why these control-words are changed regularly, the period being typically from 1 to 20 seconds. This period is called crypto-period.

The authorization messages (ECM) are sent with a higher frequency than the crypto-period, for example every 100 milliseconds. This is indispensable on the one hand when starting the decoder service and, on the other hand when changing channels.

In fact, to be able to visualize the desired transmission, the control-words are necessary for the decrypting of the signals. It is not good to wait 5 seconds in front of the screen in order that the image clearly appears.

In the second case, the control-words being for each channel, one should await the end of the crypto-period to receive the authorization message allowing the decrypting of the signals of the new channel. In the same way as previously stated, one cannot accept a delay of several seconds when changing channel.

This is why, in practice, the authorization messages (ECM) are sent to a frequency comprised between 5 and 20 per second.

When changing channel, the time separating the order of the subscriber and the visualization of the desired channel must be the shorter one. According to the usual standards, a duration of about 500 milliseconds is considered as being acceptable.

During this lapse of time, the following operations are carried out:

- placement of the audio, video and control filters on the new channel;

- waiting of the next message (ECM) containing the encrypted control-word for said channel;

- reception of this message (ECM) and transmission to the cryptographic unit for decrypting; and

- execution of the decrypting algorithm by the cryptographic unit and return of the decrypted control-word, transmission of this word to the decoder;

- start of the MPEG decompression and waiting of an image complete of synchronization.

One sees, by the chaining of these operations, that it cannot be carried out in parallel, and thus each of them goes into the determination of the maximum duration in the case of change of channel.

It is known that the more the encrypting algorithm is of high security, the more the operations necessary for the decrypting are long. On the other hand, the decrypting time taking part directly in the calculation of the commutation duration between channels, cannot be lengthened to improve the quality of the encryption. This is why the security of the used algorithms to obtain the control-words is obligingly limited by these constraints of time.

A known method is described in the document EP 0 583 202 and consists in sending, on the active channel, not only the authorization messages (ECM) of the channel concerned, but also the authorization messages of the other channels. These latter are transmitted to a lower frequency so as not to congest the transmission.

This method presents the drawbacks to congest the channel with unnecessary messages and needs the memorization of all authorization messages for a use when changing channel. Another unsolved aspect by this document is the increase of the quality (and thus of the duration) of the decrypting operation which should not increase the commutation time between channels.

The aim of this invention is to propose a method and a transmission system of encrypted information which assures a high security to the destination control-

words of the decoder, without lengthening the duration of treatment of the control-word specific to a channel.

This aim is fully reached by the utilization of a control-word obtained by combination of the decrypting of an authorization message (ECM) for each channel and of the decrypting of an authorization message common to a group of channels.

In the following description, the messages for each channel are called " mono-channel authorization messages (ECM)" and the messages common to a group of channels are called " multi-channel authorization messages (MECM)" (Master ECM).

The algorithm of treating the messages (ECM) is of the fast type and offers thus a limited security. This is imposed by the little time required at the time of the passage from one channel to another.

On the other hand, according to the invention, it is not possible to obtain the control-words (CW) only by the treatment of the mono-channel messages (ECM). The cryptographic unit, to be able to decrypt the mono-channel messages (ECM), must contain the received information in a multi-channel message (MECM). The latter is decrypted by a key called system because it is independent from the different channels.

At the moment of the change or commutation from one channel to another, the information contained in the mono-channel authorization message (ECM) suitable for the new channel is combined with the information contained in the multi-channel authorization message (MECM) already in the cryptographic unit, these latter being common to the two channels. In this way, the decrypting duration of the message (MECM) does not intervene in the calculation of the commutation duration as described above. Therefore, the algorithm to decrypt the messages (MECM) can be stronger and thus need a longer time without therefore penalizing the commutation time. Furthermore, the simple use of a different algorithm increases the security of the system.

The content of the multi-channel messages (MECM) can vary according to al period identical to the message (ECM) (crypto-period), or according to a multiple of this period.

If the time between two mono-channel messages (ECM) is important, since it intervenes directly in the calculation of the maximum time of commutation between two channels, it is not the same for the time between two multi-channel messages (MECM). Since this message is common to a group of channels, it can have a greater time. In fact, its repetition interval intervenes only at the moment of the placing under tension of the decoder. In the case of the figure, one sees that a repetition of 1 to 2 messages per second is sufficient.

The invention will be better understood thanks to the following detailed description which refers to the annexed drawings which are given as an example not limitative, in which:

- Figure 1 represents the transmission of the (ECM) and (MECM) messages on two channels A and B;

- figure 2 represents the security cryptographic unit.

In Figure 1 the messages allowing to decrypt the video and audio signals are represented schematically, on two lines. One can observe at regular intervals, the transmission of the mono-channel messages (ECM) for each channel. On the “A” channel, the "A" mono-channel authorization messages (ECM) are transmitted. On the "B" channel, the "B" mono-channel authorization messages (ECM) are transmitted. The multi-channel messages (MECM) common to channels A and B, are transmitted on the two channels.

In a mode of realization using the analog diffusion, the mono-channel and multi-channel authorization messages are effectively transmitted on each channel, one channel being associated to one frequency. On the other hand, on the numerical diffusion systems, the notion of a channel associated to a frequency does not exist. The multi-channel messages (MECM) can be added in the

messages for this channel or transmitted in a global way to the information flux without it being necessary to repeat it on each channel.

According to this example, the periodicity of the multi-channel messages (MECM) is lower by half to the periodicity of the mono-channel messages (ECM). The periodicity of the messages (MECM) is determined by the acceptable decrypting time at the moment of the first use. In this case, it will be possible to decrypt the signals after having received at least one message (ECM) and one message (MECM). This is why a repetition of approximately one second for the message (MECM) is acceptable and does not encumber the pass-band of the system. Once the message (MECM) is received and treated, it is immediately available when changing channel with the new message (ECM).

Another aspect of the invention is the taking into account of the reductions from the start of the crypto-period according to the channels. In fact, the change of the control-word can be made at different moments according to the channels. Therefore, for example, on the "A" channel, the control-word (CW) changes, from CW-A1 to CW-A2. According to the invention, the control-word is from then obtained due to the multi-channel message (MECM-2). On the other hand, in the hypothesis where the new channel B operates always with the control-word (CW-B1), it will be necessary to use the multi-channel message (MECM-1). This is why each message (MECM) contains the information of several crypto-periods, so allowing to be free of differences of synchronization of the channels.

Figure 2 illustrates the functionality of these data transmitted in the multi-channel message (MECM). The mono-channel message (ECM) contains the control-word (CW) under encrypted form and is transmitted to the cryptographic unit (CU) able to decrypt this information. For this, it disposes of parameters P1, P2 to Pn which define the rights associated to the system in general, and to this channel in particular. This unit calculates, thanks to these parameters, the control-word (CW). According to the invention, the data transmitted by the message (MECM), once decrypted, can modify the parameters upstream of the cryptographic unit (CU), or downstream of this unit.

According to a particular form of the invention, the final control-word (CW) is obtained by a logic operation between the information contained in the message (MECM) and the message (ECM), such that addition, subtraction, or exclusive or multiplication.

According to a particular form of the invention, the information contained in the message (MECM) is used as secondary key to decrypt the content of the mono-channel messages (ECM).

CLAIMS

1. A multi-channel transmission system of encrypted information for Pay-TV, comprising a management centre and at least one subscriber unit, the management centre transmitting encrypted signals and mono-channel authorization messages (ECM) encrypted for each channel, characterized in that it includes multi-channel authorization messages (MECM) common to a group of channels, these messages being combined with the mono-channel authorization messages (ECM) for the channel currently received in order to decrypt the same.

2. A multi-channel transmission system according to claim 1, characterized in that the multi-channel authorization messages (MECM) are encrypted by an algorithm different to the algorithm used to encrypt the mono-channel authorization messages (ECM).

3. A multi-channel transmission system according to claims 1 and 2, characterized in that the multi-channel authorization messages (MECM) are modified according to a period different to the period of the mono-channel authorization messages (ECM).

4. A multi-channel transmission system according to claims 1 to 3, characterized in that the information contained in the multi-channel authorization messages (MECM) is combined with the information contained in the mono-channel authorization messages (ECM) by operations such as addition, subtraction, or exclusive (XOR), multiplication or coding.

5. A multi-channel transmission system according to claims 1 to 3, characterized in that the subscriber unit includes a cryptographic unit (CU) determining control-words (CW) from mono-channel authorization messages (ECM), allowing the subscriber unit to decrypt the encrypted signals, the content of the multi-channel authorization messages (MECM) being combined with the parameters (P1, P2 ... Pn) of cryptographic calculation of the cryptographic unit (CU).

6. A transmission method of multi-channel encrypted signals for Pay-TV consisting of:

- transmitting multi-channel encrypted signals to the subscriber unit,

- transmitting mono-channel authorization messages (ECM) encrypted for each channel,

- decrypting the authorization messages (ECM) for the channel currently received by a cryptographic unit (CU), the decrypted information representing control-words (CW) necessary to decrypt the signals suitable for the channel currently received,

characterized in that it consists in:

- transmitting multi-channel authorization messages (MECM) common to a group of channels,

- decrypting these multi-channel authorization messages (MECM) and combining the decrypted information with the information necessary for the obtainment of the control-words (CW).

7. A transmission method of multi-channel encrypted signals according to claim 6, characterized in that the combination is done on the entry parameters (P1, P2,.. Pn) of the cryptographic unit (CU).

8. A transmission method of multi-channel encrypted signals according to claim 6, characterized in that the combination is done on the results obtained by the cryptographic unit (CU).

9. A transmission method of multi-channel encrypted signals according to claims 6 to 8, characterized in that it consists in modifying the multi-channel authorization messages (MECM) according to a period different to the modification period of the mono-channel authorization messages (ECM).

10. A transmission method of multi-channel encrypted signals according to claims 6 to 9, characterized in that it consists in encrypting the multi-channel

authorization messages (MECM) according to an algorithm different to the algorithm used to encrypt the mono-channel authorization messages (ECM).