05 AUG 2004

DIGITAL SIGNAL PROCESSING APPARATUS

BACKGROUND OF THE INVENTION

The present invention relates to digital signal processing apparatuses connected to each other for transmitting/receiving content having copyright.

If content is transmitted/received through a digital signal bus, video signals/audio signals, data, etc. can be transmitted/received without deterioration of quality, and this gives a large merit to users. Protection of copyright, however, causes a problem because there is no deterioration in quality. A technique for encrypting the content to be transmitted/received through a digital signal bus is described in NIKKEI Electronics, No. 712, March 23, 1998, pp.47-53. According to this technique, authentication is performed on transmission and reception side apparatuses so that the transmission/reception of content is enabled only between the apparatuses where authentication is established. The process protects copyrighted content from illegal copying.

Not only content but also information for controlling respective apparatuses can be transmitted through the aforementioned digital signal bus. Accordingly, one apparatus can control all the apparatuses connected to the one apparatus through a

digital signal bus.

Although the use of the aforementioned technique makes it possible to protect the copyright of content, both authentication and encryption among apparatuses are so complex and the quantity of information to be processed is so large that a long time is required for processing. Furthermore, as the number of connected apparatuses increases, the quantity of information to be processed increases. Accordingly, there arises a problem in handling property. As described above, when content is to be transmitted/ received through a digital signal bus, both achievement of handling property bearing comparison with that of conventional analog signals and protection of the copyright of the content without users' awareness become a problem to be solved.

Although the use of the aforementioned technique makes it possible for any one of the apparatuses to control all the apparatuses, there are numbers of handling ways for one purpose. Accordingly, there is a possibility that users hardly understand the handling ways.

SUMMARY OF THE INVENTION

An object of the present invention is to solve the aforementioned problem, that is, to provide a digital signal processing apparatus improved both in the connecting way and in the handling property of the

05 AUG 2004

digital signal processing apparatus to protect the copyright of content without user's awareness.

The foregoing object can be achieved by provision of an interface means which performs authentication among all apparatuses connected to a digital signal bus when a power source is turned on.

The object can be further achieved by provision of an interface circuit which performs authentication among all apparatuses connected to a digital signal bus when an apparatus is connected to the digital signal bus.

The object can be further achieved by provision of an interface circuit which performs authentication among all apparatuses connected to a digital signal bus when an input terminal connected to the digital signal bus is selected.

The object can be further achieved by provision of a storage circuit which stores a key used among all apparatuses connected to a digital signal bus.

The object can be further achieved by provision of an interface circuit which changes a transmission channel of a digital signal bus in accordance with copyright control information with content.

The object can be further achieved by provision of a circuit which defines names of all apparatuses connected to a digital signal bus on each apparatus side.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a configuration view of an embodiment for explaining the way of connecting digital signal processing apparatuses according to the present invention;

Fig. 2 is a time chart of a digital signal bus;

Fig. 3 is a flow chart showing authentication;

Fig. 4 is a view showing the configuration of the digital video disk depicted in Fig. 1;

Fig. 5 is a view showing the configuration of the IF circuit depicted in Fig. 4;

Fig. 6 is a flow chart showing authentication among apparatuses;

Fig. 7 is a flow chart showing authentication among apparatuses; and

Fig. 8 is a flow chart showing authentication among apparatuses.

DESCRIPTION OF THE EMBODIMENTS

An embodiment of the present invention will be described below with reference to the drawings.

Fig. 1 shows an example of configuration for explaining an example of the way of connecting digital signal processing apparatuses according to the present invention. In Fig. 1, the reference numeral 100 designates a digital tuner; 102, a digital signal bus; 103 and 104, digital VTRs; 105, a digital video disk;

and 106, a digital display.

First, in each of devices connected to the digital signal bus 102 in Fig. 1, an operation of initializing the digital signal bus 102 is started. In this occasion, an apparatus on a root of the bus is decided on the basis of data transmission/reception among respective interface circuits of apparatuses 100 to 105. The thus decided root apparatus performs management so that signal conflict does not occur in terms of the transmission channel and timing of the bus. The apparatuses other than the root apparatus inquire of the root apparatus about the transmission channel and timing of the bus. When there is no conflict, the other apparatuses are permitted to use the bus.

A transmitting operation of the digital signal bus 102 will be described below. Fig. 2 shows the state of transmission of the digital signal bus 102. In Fig. 2, the reference numeral 200 designates a cycle start packet; 201, AV data A; 202, AV data B; and 203, asynchronous transmission data. The terminology "AV data" means audio/video mixed data. Fig. 2 shows an example in which two AV data streams are transmitted. In this manner, two streams are transmitted with different time-derived channels being secured. The asynchronous transmission data 203 are data concerning commands, settings, etc. for respective apparatuses.

The time between adjacent broken lines in Fig. 2 is called "cycle". In the term of one cycle, the bus

is controlled so that transmission bands for the AV data A 201 and the AV data B 202 are secured as sufficiently as possible. The asynchronous transmission data 203 is transmitted after completion of the transmission of the AV data A 201 and the AV data B 202. Specifically, though the transmission of the AV data A 201, the AV data B 202 and the asynchronous transmission data 203 follows the transmission of the cycle start packet 200, waiting is set before the transmission of the asynchronous transmission data 203 when the period of cycle cannot be fulfilled.

Then, authentication is performed among the apparatuses. Authentication is classified into two authentication levels - full and restricted. The two authentication levels are used appropriately in accordance with copyright control information and apparatus content. Full authentication is established only in the case where both transmitter-side and receiver-side apparatuses have public keys respectively. When full authentication is established, any content is enabled to be transmitted even if the content is a copy-prohibited one. Examples of the receiver-side apparatus having a public key include: apparatuses each having no recording device, such as an digital display, etc.; and apparatuses each having any recording device permitted to perform recording for a charge, or the like. Restricted authentication is authentication for apparatuses each having no key but a common key. That

is, restricted authentication is intended for apparatuses each having some recording devices, such as a digital VTR, etc. In restricted authentication, copy-prohibited content is disabled from being transmitted. These operations are shown collectively in Fig. 3.

In step 301 in Fig. 3, the level of authentication is selected in accordance with the authentication level of another apparatus and the copy control information of content to be transmitted. For content that can be copied freely, the authentication process is terminated in step 305 because no authentication or encryption is required for the content. After the authentication level is selected in the step 301, full authentication is established in step 302 or restricted authentication is established in step 303. In step 304, thereafter, an encryption key used to encrypt content is then shared. In step 305, the authentication process is terminated.

The aforementioned process is required to transmit/receive content that cannot be copied freely. The quantity of calculation is, however, so large that a large time is required for the authentication process. Accordingly, when the authentication process should be executed becomes a subject of discussion.

The inside of an apparatus connected to the digital signal bus 102 will be described below. The inside of the digital video disk 105 will be described below as an example with reference to Fig. 4. In Fig.

4, the reference numeral 401 designates a digital signal bus input/output terminal; 402, an analog output terminal; 403, an analog input terminal; 404, an interface (hereinafter referred to as IF) circuit; 405, a decoder; 406, an encoder; 407, a stream conversion circuit; 410, an input switching circuit; 411, an output switching circuit; 412, a recording signal processing circuit; 413, a playback signal processing circuit; 414, a microcomputer; 415, a disk; and 416, a pickup.

Bus control and authentication are processed mainly by the IF circuit 404. First, the basic operations of the apparatus will be described below.

A recording operation is as follows. When the input switching circuit 410 is controlled to select "analog input" on the basis of an input control signal from the microcomputer 414, an analog signal received from the analog input terminal 403 is encoded by the encoder 406 by using a method such as so-called MPEG. In the case of a transport stream from the digital signal bus 102, a desired stream is extracted by the IF circuit 404 to reproduce timing. The transport stream is then converted into a digital disk stream by the stream conversion circuit 407. The digital disk stream is recorded on the disk 415 by use of the recording signal processing circuit 412. In this occasion, the stream being recorded can be monitored because even the stream from the digital signal bus 102 can be decoded by the decoder 405.

A reproducing operation is as follows. Playback data from a signal recorded on the disk 415 are read by the pickup 416. A compressed digital signal is reproduced by the playback signal processing circuit 413. The output switching circuit 411 is controlled on the basis of an output control signal from the microcomputer 414 to select "monitor output" or "playback output" of the input signal. The output of the output switching circuit 411 is sent both to the decoder 405 and to the stream conversion circuit 407. The decoder 405 converts the compressed digital signal into an analog signal and the analog signal is outputted from the analog signal output terminal 402. The stream conversion circuit 407 converts the signal into a transport stream that can be transmitted through the digital signal bus. The transport stream is sent to the IF circuit 404 and then outputted from the digital signal bus input/output terminal 401.

In this manner, even the signal reproduced from the disk can be transmitted to the digital signal bus because the signal can be converted into a transport stream by the stream conversion circuit 407.

The operation of the IF circuit 404 will be described below with reference to Fig. 5. In Fig. 5, the reference numeral 501 designates a stream input/output terminal; 503, an IF control signal input/output terminal; 504, an encryption circuit; 505, an asynchronous transmission circuit; 506, a microcomputer;

507, an isochronous transmission circuit; 508, a packet processing circuit; 509, a bus control circuit; and 510, a digital signal bus input/output terminal.

The aforementioned bus initializing operation is executed by the bus control circuit 509. Specifically, the initializing operation is executed on the basis of communications among respective bus control circuits of digital apparatuses connected to the digital signal bus. When the initializing operation is completed so that the root apparatus is decided, the microcomputer 506 recognizes information, concerning the connection of respective digital apparatuses, through the packet processing circuit 508. After the recognition of information concerning the connection of respective digital apparatuses, the microcomputer 506 performs connection for apparatuses permitted to be connected and then performs authentication. The processes of connection and authentication are carried out as follows. A command from the microcomputer 506 is converted into a transmission packet by the packet processing circuit 508 through the asynchronous transmission circuit 505. The transmission packet is transmitted/received on the digital signal bus by the bus control circuit 509 through the digital signal bus input/output terminal 510.

After these processes, the information concerning the connection of respective digital apparatuses is transmitted to the microcomputer 414 in

Fig. 4. The microcomputer 414 supplies the connection information to a display not shown. The display indicates the configuration of apparatuses to the user as to whether an apparatus can be connected or not and as to whether data can be transmitted to the apparatus or not. The user utilizes the connection information for selection of connection of apparatuses. In this manner, the connection information is displayed to the user so that the user is prevented from hesitating over which apparatus to connect.

There are some cases where the user can hardly identify apparatuses, for example, because of the presence of two digital VTRs as shown in Fig. 1, the increase of the number of connected apparatuses, and so on. Therefore, the respective names of these apparatuses can be also defined freely by the user. For example, the names of the two digital VTRs 103 and 104 are defined as "DVTR1" and "DVTR2" respectively and the name of the digital tuner 100 is defined as "BS-D" on the basis of its broadcasting service name. This definition makes it possible to provide interfaces that can be understood easily by the user.

After the completion of connection and authentication, a stream is enabled to be transmitted/ received. A stream on the digital signal bus 102 is received as follows. First, a transmission packet is received by the bus control circuit 509. The transmission packet thus received is converted by the

packet processing circuit 508 with the time interval reproduced by the isochronous transmission circuit 507 to reproduce a transport stream. The transport stream is decrypted by the decryption circuit 504 by using the shared key established in authentication. The decrypted stream is outputted from the stream input/output terminal 501. A stream is sent onto the digital signal bus 102 as follows. First, a stream from the stream input/output terminal 501 is encrypted by the encryption circuit 504 by using the shared key established in authentication. The microcomputer 414 in Fig. 4 makes a judgment, on the basis of copy information recorded on the video disk, as to whether the stream should be encrypted by the encryption circuit 504 or not. The microcomputer 414 is communicated with the microcomputer 506 to control the judgment. A time stamp for reproducing the time interval is added to the stream by the isochronous transmission circuit 507 and the stream is converted into a transmission packet by the packet processing circuit 508. The transmission packet is transmitted as a stream output onto the digital signal bus 102 by the bus control circuit 509.

When authentication should be executed and how authentication should be executed will be described below. First, description will be made upon the case where a controller controls all apparatuses, that is, for example, upon the case where electric sources of apparatuses are turned on at the same time in the

condition that the digital display 106 is used as the controller.

Authentication is started by a receiver-side request. Accordingly, it can be considered that the controller sends a command to a receivable apparatus to execute authentication. In Fig. 1, receivable apparatuses are the digital VTRs 103 and 104, the digital video disk 105 and the digital display 106 whereas transmittable apparatuses are all the apparatuses except the digital display 106. After electric sources of apparatuses are turned on, the digital display 106 used as the controller sends a command to each of the receiver apparatuses to control the receiver apparatus to execute authentication for the respective transmitter apparatuses.

The procedure of processing in this occasion is shown in Fig. 6. In step 601, a transmitter apparatus, for example, the digital tuner 100, is selected. In step 602, full authentication is executed for an apparatus supporting full authentication. For example, in Fig. 1, the apparatus supporting full authentication is the digital display 106. The digital display 106 makes an authentication request to the digital tuner 100. Authentication is then executed, so that a key is stored so as to be shared. In step 603, restricted authentication is executed between the digital tuner 100 and each of receiver apparatuses supporting restricted authentication, that is, each of

the digital display 106, the digital VTRs 103 and 104 and the digital video disk 105. Thus, a key is stored so as to be shared between the digital tuner 100 and each of the digital display 106, the digital VTRs 103 and 104 and the digital video disk 105. In step 604, confirmation is made as to whether authentication is terminated among all transmitter and receiver apparatuses. When authentication is not terminated, the situation of the procedure goes back to the step 601 and another transmitter apparatus, for example, the digital video disk 105, is selected to repeat authentication in the aforementioned manner. Incidentally, apparatuses with no authentication are put out of this processing.

Although the above description has been made upon the case where electric sources are turned on, content transmitted as encrypted content can be received without a break also in the case where authentication is executed when a new apparatus is connected to the digital signal bus 102 or before content is transmitted/received. Further, because the shared key is stored, authentication is not required to be executed newly in the digital display 106 even in the case where the copy control information of content from a transmitter apparatus is changed. Accordingly, the picture is not interrupted. Since the key is shared between the digital tuner 100 and each of the digital display 106, the digital VTRs 103 and 104 and the digital video disk 105, even if content which requires restricted

authentication is transmitted, the content can be received by all the apparatuses. Accordingly, the user does not feel out of place compared with analog signal connection.

Although the above processing has been described in the case where electric sources of apparatuses connected to the digital signal bus 102 are turned on at the same time, the apparatus serving as the controller can detect turned-on apparatuses to perform processing for the apparatuses successively even in the case where the electric sources of the apparatuses are turned on separately.

Even in the case where a main electric source is off, the connection state can be kept so long as an electric source for the IF circuit 404 is supplied in a standby state, or the like. Accordingly, authentication is not required to be executed newly.

It can be further considered that an apparatus is connected to the digital signal bus 102 after an electric source for the apparatus is turned on. Also in this case, the controller detects the connection of the bus to execute authentication so that a key can be shared.

Another apparatus than the controller may detect these newly connected apparatuses so that a series of operations from initialization to re-connection may be performed after the bus is reset.

There is the case where only one encryption key per one transmission channel is used limitatively. In this case, authentication is required again when the copy control information of content is changed. However, the same effect as described above is obtained by preparing transmission channels for each copy control information of content and executing authentication and storing the keys.

The case where no controller is set specifically will be described below. Because a receiver apparatus substantially makes an authentication request, the operation of the receiving apparatus will be described mainly. Processing of the digital VTR 103 as an example of the receiver apparatus in Fig. 1 will be described. First, one transmitter apparatus is retrieved. If there are a plurality of transmitter apparatuses, one transmitter apparatus is selected from the plurality of transmitter apparatuses. In Fig. 1, the digital video disk 105 is selected. Then, authentication is performed between the selected digital video disk 105 and the digital VTR 103. If both restricted authentication and full authentication are permitted, full authentication is used here. Then, confirmation is made as to whether the digital video disk 105 is already connected to another receiver apparatus or not. When, for example, the digital video disk 105 is already connected to the digital display 106, what is meant by the connection is that

authentication is terminated and that a key is already shared. Accordingly, the same key is stored so as to be shared with the digital VTR 103. When the digital video disk 105 is not connected yet, a new key is shared. The aforementioned process is repeated until authentication is terminated among all transmitter apparatuses.

Alternatively, keys serving as seed of encryption key may be shared when authentication is performed. The encryption key is updated successively at regular time intervals by a mutually decided calculation method by using keys as a seed of encryption key.

The aforementioned procedure is shown in Fig. 7. In step 701 in Fig. 7, first, a transmitter apparatus is selected by retrieval. In step 702, authentication is performed between the selected transmitter apparatus and a receiver apparatus serving as the controller. In step 703, confirmation is made as to whether the selected transmitter apparatus is already connected to another receiver apparatus. When the selected transmitter apparatus is already connected, what is meant by the connection is that authentication is terminated and that a key is already shared. Accordingly, when the selected transmitter apparatus is already connected, the same key as used in the connected receiver apparatus is shared in step 704. When the selected transmitter apparatus is not connected yet, a new key is shared in step 706. The aforementioned

process is repeated until authentication is terminated among all transmitter apparatuses in step 706.

The process in Fig. 7 can be also used in the aforementioned manner when a new receiver apparatus is connected or powered on. Even in the case where a new transmitter apparatus is connected or powered on, authentication can be performed in the aforementioned manner on the basis of detection of the transmitter apparatus. Further, even in the case where the selected transmitter apparatus is already connected to another receiver apparatus and is transmitting content to the already connected receiver apparatus, authentication can be performed in the aforementioned manner.

As described above, the aforementioned process is performed by each of receiver apparatuses so that a key is stored in accordance with the copy control information, even in the case where no controller is set specifically. Accordingly, even in the case where the copy control information of content from transmitter apparatuses is changed, the picture is not interrupted because authentication is not required. Further, a key per a transmitter apparatus can be shared to respective receiver apparatuses. Accordingly, even in the case where content requiring restricted authentication is transmitted, the content can be received by all the receiver apparatuses. The user does not feel out of place compared with analog signal connection.

Although the embodiment has been described

upon the case where both connection and authentication are performed for all apparatuses, the same effect as described above can be also obtained when both connection and authentication are performed only for apparatuses registered in advance or subjected to data transmission in the past in the case where the processing time becomes noticeably large because of connection of an extremely large number of apparatuses, or the like.

There is a further case where a plurality of systems each having the connection form as shown in Fig. 1 are connected through bridges. In this case, authentication is performed for apparatuses connected in a bridge. The same effect as described above is obtained when authentication is performed whenever content is transmitted in the case where apparatuses are connected through a bridge.

The case where authentication is performed when the input is switched will be described below. The digital video disk 105 has both an analog input and a digital input. Accordingly, the digital video disk 105 may be designed so that authentication is performed when the digital input is selected. In this case, a certain processing time is required for switching the input. The burden imposed on processing, however, becomes light because connection is performed only in the case of necessity.

Processing in this occasion is shown in Fig. 8. In step 801, a transmitter apparatus which is transmitting content is retrieved to select a target transmitter apparatus. In step 802, authentication is performed. In step 803, confirmation is made as to whether the selected transmitter apparatus is already connected to another apparatus. If the selected transmitter apparatus is already connected, the same key as used in the already connected apparatus is shared in step 804. If the selected transmitter apparatus is not connected yet, a new key is shared in step 805. As described above, the burden imposed on processing is light because connection is performed only in the case of necessity. Although this embodiment has been described upon an apparatus having both an analog input and a digital input, the same effect as described above is obtained also in the case where the apparatus has two or more digital inputs. Although the above description has been made upon the digital video disk, the same processing as described above is performed upon another digital apparatus.

The aforementioned authentication can be performed in the same manner as described above in the case where it is applied to other information than copy information and copyright information.

In the digital signal processing apparatus according to the present invention, authentication is

performed for management of copyright among apparatuses connected to a digital signal bus, when the apparatuses are powered on or connected to the digital signal bus. Accordingly, even in the case where content requiring restricted authentication is transmitted, the content can be received immediately.

Further, authentication is performed for management of copyright among apparatuses connected to a digital signal bus, when an input terminal connected to the digital signal bus is selected. Accordingly, the burden imposed on processing is light because connection is performed only in the case of necessity.

Further, a key used among apparatuses connected to a digital signal bus is stored. Accordingly, even in the case where the copy control information of content from a transmitter apparatus is changed, authentication is not required so that the picture is not interrupted because the key is stored.

Further, the transmission channel of the digital signal bus is changed in accordance with the copyright control information attendant on content. Accordingly, even in the case where only one key can be established for one transmission channel, authentication is not required so that the picture is not interrupted because the key is stored though the copy control information of content from a transmitter apparatus is changed.

05 AUG 2004

Further, an apparatus defines the respective names of apparatuses connected to the digital signal bus. Accordingly, an interface understood easily by the user can be provided.

WHAT IS CLAIMED IS :

1. A digital signal processing apparatus connected to other digital signal processing apparatuses by means of a digital signal bus to transmit/ receive a digital signal, wherein said digital signal processing apparatus comprises an interface circuit so that when said digital signal processing apparatus is powered on, said interface circuit performs authentication between said digital signal processing apparatus and [any of] said other digital signal processing apparatuses powered on simultaneously with or before power-on of said digital signal processing apparatus, and wherein key information is shared by performing an authentication processing between said digital signal processing apparatus and said other digital signal processing apparatuses, and the digital signal is encrypted or decrypted on the basis of said key information.

2. A digital signal processing apparatus connected to other digital signal processing apparatuses by means of a digital signal bus to transmit/ receive a digital signal, wherein said digital signal processing apparatus comprises an interface circuit so that when powering-on of said other digital signal processing apparatuses is detected, said interface curcuit performs authentication between said digital signal processing apparatus and [any of] said other digital signal processing apparatuses, and wherein key information is shared by performing an authentication processing between said digital signal processing apparatus and said other digital signal processing apparatuses, and the digital signal is encrypted or decrypted on the basis of said key information.

3. A digital signal processing apparatus connected to other digital signal processing apparatuses by means of a digital signal bus to transmit/ receive a digital signal, wherein said digital signal processing apparatus comprises an interface circuit which performs authentication between said digital signal processing apparatus and said other digital signal processing apparatuses when said interface circuit is connected to said digital signal bus, and wherein key information is shared by performing an authentication processing between said digital signal processing apparatus and said other digital signal processing apparatuses, and the digital signal is encrypted or decrypted on the basis of said key information.

4. A digital signal processing apparatus connected to other digital signal processing apparatuses by means of a digital signal bus to transmit/ receive a digital signal, wherein said digital signal processing apparatus comprises an interface circuit which performs authentication between said digital signal processing apparatus and said other digital signal processing apparatuses when connection of said other digital signal processing apparatuses to said digital signal bus is detected, and wherein key information is shared by performing an authentication processing between said digital signal processing apparatus and said other digital signal processing apparatuses, and the digital signal is encrypted or decrypted on the basis of said key information.

5. A digital signal processing apparatus provided with a plurality of input terminals including an input terminal from a digital signal bus and connected to other digital signal processing apparatuses by means of said

digital signal bus to transmit/ receive a digital signal, wherein said digital signal processing apparatus comprises:

a switching circuit for selecting said plurality of input terminals; and

an interface circuit which performs authentication between said digital signal processing apparatus and said other digital signal processing apparatuses when said input terminal connected to said digital signal bus is selected by said switching circuit,

wherein key information is shared by performing an authentication processing between said digital signal processing apparatus and said other digital signal processing apparatuses, and the digital signal is encrypted or decrypted on the basis of said key information.

6. A digital signal processing apparatus connected to other digital signal processing apparatuses by means of a digital signal bus to encrypt a digital signal and transmit/ receive said encrypted digital signal, wherein key information is shared by performing an authentication processing between said digital signal processing apparatus and said other digital signal processing apparatuses, and the digital signal is encrypted or decrypted on the basis of said key information, and said digital signal processing apparatus comprises a storage circuit for storing said key information used in transmission/ reception of signals between said digital signal processing apparatus and said other digital signal processing apparatuses.

7. A digital signal processing apparatus connected to other digital signal processing apparatuses by means of a digital signal bus having a plurality of transmission channels to thereby encrypt a digital signal in

accordance with copyright control information of said digital signal and perform transmission/ reception of said encrypted digital signal, wherein said digital signal processing apparatus comprises an interface circuit which changes said transmission channels of said digital signal bus in accordance with said copyright control information when said digital signal is to be transmitted.

8. A digital signal processing apparatus connected to other digital signal processing apparatuses by means of a digital signal bus to exchange a digital signal, wherein said digital signal processing apparatus comprises a circuit for defining a name of said digital signal processing apparatus and names of said other digital signal processing apparatuses connected to said digital signal bus.