PCT/EP2010/004827 October 10, 2011

DOLBY INTERNATIONAL AB 200114PC WR/JS

Claims

1) A method for encoding a data stream comprising a plurality of data frames, the method comprising

– generating a cryptographic value of a number N of successive data frames and configuration information using a cryptographic hash function; wherein the configuration information comprises information for rendering the data stream;

– inserting the cryptographic value into a frame of the data stream subsequent to the N successive data frames; and

– iteratively generating an intermediate cryptographic value of each of the N successive frames using a starting state; wherein the starting state is the intermediate cryptographic value of the previous iteration; wherein the starting state of the first iteration is an intermediate cryptographic value of the configuration information.

2) The method of claim 1, wherein the method further comprises

– grouping a number N of successive data frames to form a first message; and

– grouping the first message with the configuration information to form a second message;

wherein the cryptographic value is generated of the second message.

3) The method of any previous claim, wherein the cryptographic value is inserted as a data stream element <DSE>; and wherein the data stream element <DSE> is a syntactic element of the frame of the data stream and wherein the data stream is an MPEG4-AAC or MPEG2-AAC stream.

4) The method of any of claims 1 to 3, wherein the number of frames N is greater than one.

5) The method of any of claims 1 to 4, wherein the data frames are video and/or audio frames.

6) The method of any of claims 1 to 5, wherein the data frames are AAC or HE-AAC frames.

7) The method of any of claims 1 to 6, wherein the configuration information comprises at least one of:

- an indication of a sampling rate;
- an indication of a channel configuration of an audio coding system;
- an indication of the number of samples in a data frame.

8) The method of any of claims 1 to 7, wherein the cryptographic value is generated using a key value.

9) The method of claim 8, wherein the step of generating a cryptographic value comprises

- calculating an HMAC-MD5 value of the number N of successive data frames and the configuration information.

10) The method of claim 9, wherein the step of generating a cryptographic value comprises

- truncating the HMAC-MD5 value to yield the cryptographic value.

11) The method of claim 10, wherein the HMAC-MD5 value is truncated to 16, 24, 32, 48, 64, 80, 96 or 112 bits.

12) The method of any of claims 1 to 11, wherein the cryptographic value of N successive data frames is inserted into the next data frame.

13) The method of any of claims 1 to 12, further comprising
– inserting a synchronization indication subsequent to the N successive data frames, wherein the synchronization indication indicates that the cryptographic value has been inserted.

14) The method of any of claims 1 to 13, wherein the data stream element <DSE> is inserted at the end of the frame prior to a <TERM> element.

15) The method of any of claims 1 to 14, wherein the content of the data stream element <DSE> is aligned to a byte boundary of the data stream.

16) The method of any of claims 1 to 15, wherein the steps for generating and inserting the cryptographic value are repeated for a plurality of blocks of N successive data frames.

17) The method of claim 16, wherein the cryptographic value of a block of N successive data frames is generated on the block of N successive data frames comprising the cryptographic value of the previous block of N successive data frames.

18) The method of any of claims 1 to 17, comprising
– selecting N such that the N successive frames cover as close to a pre-determined duration of a corresponding signal as possible when played back with an appropriate configuration.

19) The method of claim 18, comprising
– selecting N such that the pre-determined duration is not exceeded.

20) The method of claims 18 or 19, wherein the pre-determined duration is 0.5 seconds.

21) The method of claim 5, further comprising

– interacting with a video and/or audio encoder of the data stream.

22) The method of claim 21, wherein interacting with the video and/or audio encoder of the data stream comprises

– setting a maximum bit-rate for the video and/or audio encoder such that a bit-rate of the data stream comprising the cryptographic value does not exceed a pre-determined value.

23) A method for verifying a data stream at a decoder, the data stream comprising a plurality of data frames and a cryptographic value associated with a number N of preceding successive data frames, the method comprising

– generating a second cryptographic value of the number N of successive data frames and configuration information using a cryptographic hash function; wherein the configuration information comprises information for rendering the data;

– extracting the cryptographic value from a frame of the data stream;

– comparing the cryptographic value with the second cryptographic value; and

– iteratively generating an intermediate second cryptographic value of each of the N successive frames using a starting state; wherein the starting state is the intermediate second cryptographic value of the previous iteration; wherein the starting state of the first iteration is an intermediate second cryptographic value of the configuration information.

24) The method of claim 23, wherein the data stream is an MPEG4-AAC or MPEG2-AAC stream; wherein the cryptographic value is extracted from a data stream element <DSE>; and wherein the data stream element

<DSE> is a syntactic element of the frame of the data stream.

25) The method of claims 23 or 24, further comprising

– extracting the N successive data frames to form a first message;

– grouping the first message with the configuration information to form a second message;

wherein the second cryptographic value is generated of the second message.

26) The method of any of claims 23 to 25, wherein the data stream comprises a plurality of N successive data frames and associated cryptographic values and wherein the method further comprises the step

– determining the number N as the number of frames between two succeeding cryptographic values.

27) The method of any of claims 23 to 26, wherein the cryptographic value has been generated at a corresponding encoder from the N successive data frames and the configuration information, according to a method corresponding to the method used for generating the second cryptographic value.

28) The method of claim 27, wherein

– the cryptographic value and the second cryptographic value are generated using a unique key value and a unique cryptographic hash function.

29) The method of any of claims 23 to 28, further comprising:

– setting a flag, if the cryptographic value corresponds to the second cryptographic value; and

– providing a visual indication if the flag is set.

30) The method of any of claims 23 to 29, further comprising:

– clearing a flag, if the cryptographic value does not correspond to the second cryptographic value or if no cryptographic value can be extracted from the data stream.

31) A data stream comprising a cryptographic value generated and inserted according to the method of any one of claims 1 to 22.

32) An encoder operable to encode a data stream comprising a plurality of data frames, the encoder comprising a processor operable to

– generate a cryptographic value of a number N of successive data frames and configuration information using a cryptographic hash function; wherein the configuration information comprises information for rendering the data stream;

– insert the cryptographic value into a frame of the data stream subsequent to the N successive data frames; and

– iteratively generate an intermediate cryptographic value of each of the N successive frames using a starting state; wherein the starting state is the intermediate cryptographic value of the previous iteration; wherein the starting state of the first iteration is an intermediate cryptographic value of the configuration information.

33) A decoder operable to verify a data stream comprising a plurality of data frames and a cryptographic value associated with a number N of preceding successive data frames, the decoder comprising a processor operable to

– generate a second cryptographic value of the number N of successive data frames and configuration information using a cryptographic hash function; wherein the configuration information comprises information for rendering the data;

– extract the cryptographic value from a frame of the data stream;

– compare the cryptographic value with the second cryptographic value; and

– iteratively generate an intermediate second cryptographic value of each of the N successive frames using a starting state; wherein the starting state is the intermediate second cryptographic value of the previous iteration; wherein the starting state of the first iteration is an intermediate second cryptographic value of the configuration information.

34) A software program adapted for execution on a processor and for performing the method steps of any one of claims 1 to 30 when carried out on a computing device.

35) A storage medium comprising a software program adapted for execution on a processor and for performing the method steps of any one of claims 1 to 30 when carried out on a computing device.

36) A computer program product comprising executable instructions for performing the method of any one of claims 1 to 30 when executed on a computer.

37) A set-top box for decoding a received data stream, comprising an audio signal; the set-top box comprising a decoder according to claim 33 for verifying the received data stream.

38) A portable electronic device for decoding a received data stream, comprising an audio signal; the portable electronic device comprising a decoder according to claim 33 for verifying the received data stream.

39) A computer for decoding a received data stream, comprising an audio signal; the computer comprising a decoder according to claim 33 for verifying the received data stream.

40) A broadcasting system for transmitting a data stream, comprising an audio signal; the broadcasting system comprising an encoder according to claim 32.

41) A method for concatenating a first and a second bitstream, each comprising a plurality of data frames and a cryptographic value associated with a given number of data frames, the method comprising

– generating a concatenated bitstream from the first and second bitstream, wherein the concatenated bitstream comprises at least a portion of the plurality of data frames from the first and second bitstream, and comprises a cryptographic value generated and inserted according to the method of any one of claims 1 to 30.

42) A splicer operable to concatenate a first and a second bitstream, each comprising a plurality of data frames and cryptographic values associated with a given number of data frames, the splicer comprising

– an encoder according to claim 32 for encoding the final frames of the first bitstream and the first frames of the second bitstream.

43) The splicer of claim 42, further comprising

– a forwarding unit for forwarding frames and associated cryptographic values of the first and the second bitstream which are not decoded and encoded.

44) The splicer of claim 42 or 43, further comprising

a decoder according to claim 33 for decoding final frames of the first bitstream, first frames of the second bitstream and the associated cryptographic values to determine the trust status of the first and second bitstream; and

a control unit that enables the encoder to insert cryptographic values into a portion of the bitstream only if the corresponding first or second bitstream is authenticated.

Claims

1) A method for encoding a data stream comprising a plurality of data frames, the method comprising:

generating a cryptographic value of a number N of successive data frames and configuration information using a cryptographic hash function; wherein N is greater than one; wherein the configuration information comprises information for rendering the data stream;

inserting the cryptographic value into a frame of the data stream subsequent to the N successive data frames; and

iteratively generating an intermediate cryptographic value of each of the N successive frames using a starting state for the cryptographic hash function; wherein the starting state for the cryptographic hash function for generating the intermediate cryptographic value of a frame of the N successive frames is the intermediate cryptographic value of a previous frame of the N successive frames; wherein the starting state for the cryptographic hash function for generating the intermediate cryptographic value of the first frame of the N successive frames is an intermediate cryptographic value of the configuration information; wherein the cryptographic value which is inserted into a frame of the data stream subsequent to the N successive data frames is the intermediate cryptographic value of the N^{th} frame; and wherein the intermediate cryptographic values of the first to $(N-1)^{th}$ frame are not inserted into the data stream.

2) The method of claim 1, wherein the method further comprises:

- grouping a number N of successive data frames to form a first message; and
- grouping the first message with the configuration information to form a second message;

wherein the cryptographic value is generated of the second message.

3) The method of claim 1, wherein the cryptographic value is inserted as a data stream element <DSE>; wherein the data stream element <DSE> is a syntactic element of the frame of the data stream and wherein the data stream is an MPEG4-AAC or MPEG2-AAC stream.

4) The method of claim 1, wherein the data frames are AAC or HE-AAC frames.

5) The method of claim 1, wherein the configuration information comprises at least one of:

– an indication of a sampling rate;

– an indication of a channel configuration of an audio coding system;

– an indication of the number of samples in a data frame.

6) The method of claim 1, wherein the cryptographic value is generated using a key value.

7) The method of claim 6, wherein the step of generating a cryptographic value comprises:

– calculating an HMAC-MD5 value of the number N of successive data frames and the configuration information.

8) The method of claim 7, wherein the step of generating a cryptographic value comprises

– truncating the HMAC-MD5 value to yield the cryptographic value.

9) The method of claim 8, wherein the HMAC-MD5 value is truncated to 16, 24, 32, 48, 64, 80, 96 or 112 bits.

10) The method of claim 1, wherein the cryptographic value of N successive data frames is inserted into a next data frame.

11) The method of claim 1, further comprising:

– inserting a synchronization indication subsequent to the N successive data frames, wherein the synchronization indication indicates that the cryptographic value has been inserted.

12) The method of claim 3, wherein a content of the data stream element <DSE> is aligned to a byte boundary of the data stream.

13) The method of claim 1, wherein the steps for generating and inserting the cryptographic value are repeated for a plurality of blocks of N successive data frames.

14) The method of claim 13, wherein the cryptographic value of a block of N successive data frames is generated on the block of N successive data frames comprising the cryptographic value of a previous block of N successive data frames.

15) A method for verifying a data stream at a decoder, the data stream comprising a plurality of data frames and a cryptographic value associated with a number N of preceding successive data frames, wherein N is greater than one, the method comprising:

– generating a second cryptographic value of the number N of successive data frames and configuration information using a cryptographic hash function; wherein the configuration information comprises information for rendering the data stream;

– extracting the cryptographic value from a frame of the data stream;

– comparing the cryptographic value with the second cryptographic value; and

– iteratively generating an intermediate second cryptographic value of each of the N successive frames using a starting state for the cryptographic hash function; wherein the starting state for the cryptographic hash function for generating the intermediate second cryptographic value of a frame of the N successive frames is the intermediate second cryptographic value

of a previous frame of the N successive frames; wherein the starting state for the cryptographic hash function for generating the intermediate second cryptographic value of the first frame of the N successive frames is an intermediate second cryptographic value of the configuration information; wherein the second cryptographic value is the intermediate second cryptographic value of the N^{th} frame.

16) The method of claim 15, wherein the data stream is an MPEG4-AAC or MPEG2-AAC stream; wherein the cryptographic value is extracted from a data stream element <DSE>; and wherein the data stream element <DSE> is a syntactic element of the frame of the data stream.

17) The method of claim 15, further comprising:

– extracting the N successive data frames to form a first message; and

– grouping the first message with the configuration information to form a second message;

wherein the second cryptographic value is generated of the second message.

18) The method of claim 15, wherein the data stream comprises a plurality of N successive data frames and associated cryptographic values and wherein the method further comprises:

– determining the number N as the number of frames between two succeeding cryptographic values.

19) An encoder operable to encode a data stream comprising a plurality of data frames, the encoder comprising:

a hardware processor operable to:

generate a cryptographic value of a number N of successive data frames, wherein N is greater than one, and configuration information using a cryptographic hash function; wherein the configuration information comprises information for rendering the data stream;

insert the cryptographic value into a frame of the data stream subsequent to the N successive data frames; and

iteratively generate an intermediate cryptographic value of each of the N successive frames using a starting state for the cryptographic hash function; wherein the starting state for the cryptographic hash function for generating the intermediate cryptographic value of a frame of the N successive frames is the intermediate cryptographic value of a previous frame of the N successive frames; wherein the starting state for the cryptographic hash function for generating the intermediate cryptographic value of the first frame of the N successive frames is an intermediate cryptographic value of the configuration information; wherein the cryptographic value which is inserted into a frame of the data stream subsequent to the N successive data frames is the intermediate cryptographic value of the N^{th} frame; and wherein the intermediate cryptographic values of the first to $(N-1)^{th}$ frame are not inserted into the data stream.

20) A decoder operable to verify a data stream comprising a plurality of data frames and a cryptographic value associated with a number N of preceding successive data frames, wherein N is greater than one, the decoder comprising:

a hardware processor operable to:

generate a second cryptographic value of the number N of successive data frames and configuration information using a cryptographic hash function; wherein the configuration information comprises information for rendering the data stream;

extract the cryptographic value from a frame of the data stream;

compare the cryptographic value with the second cryptographic value; and

iteratively generate an intermediate second cryptographic value of each of the N successive frames using a starting state for the cryptographic hash function; wherein the starting state for the cryptographic hash function for generating the intermediate second cryptographic value of a frame of the N successive frames is the intermediate second cryptographic value of a previous frame of the N successive frames; wherein the starting state for the cryptographic hash function for generating the intermediate second cryptographic value of the first frame of the N successive frames is an intermediate second cryptographic value of the configuration information; wherein the second cryptographic value is the intermediate second cryptographic value of the N^{th} frame.

21) A non-transitory storage medium having a software program stored thereon, the software program being adapted for execution on a processor and for performing the method steps of claim 1 when carried out on a computing device.

22) A non-transitory storage medium having a software program stored thereon, the software program being adapted for execution on a processor and for performing the method steps of claim 15 when carried out on a computing device.