РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2012 107 995** (13) **A**

(51) МПК
H04L 9/32 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2012107995/08, 06.08.2010**

Приоритет(ы):
(30) Конвенционный приоритет:
07.08.2009 US 61/232,295

(43) Дата публикации заявки: **20.09.2013** Бюл. № **26**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **07.03.2012**

(86) Заявка PCT:
EP 2010/004827 (06.08.2010)

(87) Публикация заявки PCT:
WO 2011/015369 (10.02.2011)

Адрес для переписки:
123242, Москва, Кудринская площадь, 1, а/я 35, "Михайлюк, Сороколат и партнеры-патентные поверенные"

(71) Заявитель(и):
ДОЛБИ ИНТЕРНЕШНЛ АБ (NL)

(72) Автор(ы):
БЁМ Рейнхольд (DE),
ГРЁШЕЛЬ Александер (DE),
ХЁРИХ Хольгер (DE),
ХОММ Даниль (DE),
ШИЛЬДБАХ Вольфганг А. (DE),
ШУГ Михель (DE),
ВАЦКЕ Оливер (DE),
ВОЛЬТЕРС Мартин (DE),
ЦИГЛЕР Томас (DE)

(54) АУТЕНТИФИКАЦИЯ ПОТОКОВ ДАННЫХ

(57) Формула изобретения

1. Способ кодирования потока данных, включающего ряд кадров данных, где способ включает этапы, на которых

- генерируют криптографическую величину для количества N последовательных кадров данных и информации о конфигурации с использованием криптографической хэш-функции; где информация о конфигурации включает информацию для рендеринга потока данных; и

- осуществляют вставку криптографической величины в кадр потока данных, следующий за N последовательными кадрами данных; и

- осуществляют итеративное генерирование промежуточной криптографической величины для каждого из N последовательных кадров с использованием исходного состояния; где исходное состояние представляет собой промежуточную криптографическую величину предыдущей итерации; и где исходное состояние первой итерации представляет собой промежуточную криптографическую величину для информации о конфигурации.

2. Способ по п.1, отличающийся тем, что способ дополнительно включает этапы, на которых

- группируют количество N последовательных кадров данных для формирования первого сообщения; и

- группируют первое сообщение с информацией о конфигурации для формирования

RU 2012107995 A

RU 2012107995 A

второго сообщения;

где криптографическую величину генерируют для второго сообщения.

3. Способ по одному из предыдущих пунктов, отличающийся тем, что криптографическую величину вставляют в элемент<DSE>потока данных; где элемент<DSE>потока данных представляет собой синтаксический элемент кадра потока данных; и где поток данных представляет собой поток MPEG4-AAC или MPEG2-AAC.

4. Способ по п.1, отличающийся тем, что количество кадров N больше единицы.

5. Способ по п.1, отличающийся тем, что кадры данных представляют собой видео- или аудиокадры.

6. Способ по п.1, отличающийся тем, что кадры данных представляют собой кадры AAC или HE-AAC.

7. Способ по п.1, отличающийся тем, что информация о конфигурации включает, по меньшей мере, один из следующих указателей:

- указатель частоты дискретизации;
- указатель конфигурации каналов системы кодирования звукового сигнала;
- указатель количества дискретных значений в кадре данных.

8. Способ по п.1, отличающийся тем, что криптографическую величину генерируют с использованием ключевой величины.

9. Способ по п.8, отличающийся тем, что этап генерирования криптографической величины включает

- вычисление значения HMAC-MD5 для количества N последовательных кадров данных и информации о конфигурации.

10. Способ по п.9, отличающийся тем, что этап генерирования криптографической величины включает

- усечение значения HMAC-MD5 для получения криптографической величины.

11. Способ по п.10, отличающийся тем, что значение HMAC-MD5 усекается до 16, 24, 32, 48, 64, 80, 96 или 112 бит.

12. Способ по п.1, отличающийся тем, что криптографическую величину для N последовательных кадров данных вставляют в следующий кадр данных.

13. Способ по п.1, отличающийся тем, что дополнительно включает этап, на котором

- вставляют указатель синхронизации после N последовательных кадров данных, где указатель синхронизации указывает на то, что криптографическая величина была вставлена.

14. Способ по п.1, отличающийся тем, что элемент<DSE>потока данных вставляют в конец кадра перед элементом<TERM>.

15. Способ по п.1, отличающийся тем, что содержимое элемента<DSE>потока данных выровнено по границе байта потока данных.

16. Способ по п.1, отличающийся тем, что этапы генерирования и вставки криптографической величины повторяют для ряда блоков из N последовательных кадров данных.

17. Способ по п.16, отличающийся тем, что криптографическую величину для блока из N последовательных кадров данных генерируют на блоке из N последовательных кадров данных, включающем криптографическую величину для предыдущего блока из N последовательных кадров данных.

18. Способ по п.1, отличающийся тем, что включает этап, на котором

- выбирают N таким образом, чтобы N последовательных кадров максимально возможно близко покрывали заранее определенную длительность соответствующего сигнала при воспроизведении в соответствующей конфигурации.

19. Способ по п.18, отличающийся тем, что включает этап, на котором

- выбирают N таким образом, чтобы заранее определенная длительность не была

RU 2012107995 A

RU 2012107995 A

превышена.

20. Способ по одному из пп.18 или 19, отличающийся тем, что заранее определенная длительность составляет 0,5 секунд.

21. Способ по п.5, отличающийся тем, что дополнительно включает этап, на котором

- осуществляют взаимодействие с видео- и/или аудиокодером потока данных.

22. Способ по п.21, отличающийся тем, что на этапе взаимодействия с видео- и/или аудиокодером потока данных осуществляют

- установку для видео- и/или аудиокодера такой максимальной битовой скорости передачи данных, чтобы указанная битовая скорость передачи данных для потока данных, включающего криптографическую величину, не превышала заранее определенное значение.

23. Способ верификации потока данных в декодере, где поток данных включает ряд кадров данных и криптографическую величину, связанную с количеством N предшествующих последовательных кадров данных, где способ включает этапы, на которых

- генерируют вторую криптографическую величину для количества N последовательных кадров данных и информации о конфигурации с использованием криптографической хэш-функции; где информация о конфигурации включает информацию для рендеринга данных;

- извлекают криптографическую величину из потока данных;

- сравнивают криптографическую величину со второй криптографической величиной; и

- осуществляют итеративное генерирование промежуточной второй криптографической величины для каждого из N последовательных кадров с использованием исходного состояния; где исходное состояние представляет собой промежуточную вторую криптографическую величину предыдущей итерации; где исходное состояние первой итерации представляет собой промежуточную вторую криптографическую величину для информации о конфигурации.

24. Способ по п.23, отличающийся тем, что поток данных представляет собой поток MPEG4-AAC или MPEG2-AAC; где криптографическая величина извлекается из элемента<DSE>потока данных; и где элемент<DSE>потока данных представляет собой синтаксический элемент кадра потока данных.

25. Способ по п.23, отличающийся тем, что дополнительно включает этапы, на которых

- извлекают N последовательных кадров данных для формирования первого сообщения;

- группируют первое сообщение с информацией о конфигурации для формирования второго сообщения;

где вторая криптографическая величина генерируется для второго сообщения.

26. Способ по п.23, отличающийся тем, что поток данных включает ряд из N последовательных кадров данных и связанных с ними криптографических величин, и где способ дополнительно включает этап, на котором

- определяют число N как количества кадров между двумя последовательными криптографическими величинами.

27. Способ по п.23, отличающийся тем, что криптографическую величину генерируют в соответствующем кодере из N последовательных кадров данных и информации о конфигурации согласно способу, который соответствует способу, используемому для генерирования второй криптографической величины.

28. Способ по п.27, отличающийся тем, что

- криптографическую величину и вторую криптографическую величину генерируют

RU 2012107995 A

RU 2012107995 A

с использованием уникального ключевого значения и уникальной криптографической хэш-функции.

29. Способ по п.23, отличающийся тем, что дополнительно включает этапы, на которых

- устанавливают флаг в случае, когда криптографическая величина соответствует второй криптографической величине; и

- обеспечивают визуальную индикацию, если флаг установлен.

30. Способ по одному из пп.23-29, отличающийся тем, что дополнительно включает этап, на котором

- осуществляют сброс флага, если криптографическая величина не соответствует второй криптографической величине или если криптографическая величина не может быть извлечена из потока данных.

31. Поток данных, который включает криптографическую величину, генерируемую и вставляемую в соответствии со способом по одному из пп.1-22.

32. Кодер, который действует для кодирования потока данных, включающего ряд кадров данных, где кодер содержит процессор, действующий для

- генерирования криптографической величины для количества N последовательных кадров данных и информации о конфигурации с использованием криптографической хэш-функции; где информация о конфигурации включает информацию для рендеринга потока данных;

- вставки криптографической величины в кадр потока данных, следующий за N последовательными кадрами данных; и

- итеративного генерирования промежуточной криптографической величины для каждого из N последовательных кадров с использованием исходного состояния; где исходное состояние представляет собой промежуточную криптографическую величину предыдущей итерации; и где исходное состояние первой итерации представляет собой промежуточную криптографическую величину для информации о конфигурации.

33. Декодер, который действует для верификации потока данных, включающего ряд кадров данных и криптографическую величину, связанную с количеством N предшествующих последовательных кадров данных, где декодер содержит процессор, действующий для

- генерирования второй криптографической величины для количества N последовательных кадров данных и информации о конфигурации с использованием криптографической хэш-функции; где информация о конфигурации включает информацию для рендеринга данных;

- извлечения криптографической величины из кадра потока данных;

- сравнения криптографической величины со второй криптографической величиной; и

- итеративного генерирования промежуточной второй криптографической величины для каждого из N последовательных кадров с использованием исходного состояния; где исходное состояние представляет собой промежуточную вторую криптографическую величину предыдущей итерации; и где исходное состояние первой итерации представляет собой промежуточную вторую криптографическую величину для информации о конфигурации.

34. Носитель данных, который включает программу, реализованную программно, адаптированную для исполнения на процессоре и для выполнения этапов способа по одному из пп.1-30 при осуществлении на вычислительном устройстве.

35. Внешнее дополнительное устройство, предназначенное для декодирования принятого потока данных, включающего звуковой сигнал, где внешнее дополнительное устройство включает декодер по п.33, предназначенный для верификации принятого

RU 2012107995 A

RU 2012107995 A

потока данных.

36. Переносное электронное устройство, предназначенное для декодирования принятого потока данных, включающего звуковой сигнал, где переносное электронное устройство включает декодер по п.33, предназначенный для верификации принятого потока данных.

37. Компьютер, предназначенный для декодирования принятого потока данных, включающего звуковой сигнал; где компьютер включает декодер по п.33, предназначенный для верификации принятого потока данных.

38. Система вещания, предназначенная для передачи потока данных, включающего звуковой сигнал; где система вещания включает кодер по п.32.

39. Способ конкатенации первого и второго битовых потоков, каждый из которых включает ряд кадров данных и криптографическую величину, связанную с заданным количеством кадров данных, где способ включает этап, на котором

- генерируют конкатенированный битовый поток из первого и второго битовых потоков, где конкатенированный битовый поток включает, по меньшей мере, часть ряда кадров данных из первого и второго битовых потоков и включает криптографическую величину, генерируемую и вставляемую в соответствии со способом по одному из пп.1-30.

40. Устройство для конкатенации, действующее для конкатенации первого и второго битовых потоков, каждый из которых включает ряд кадров данных и криптографические величины, связанные с заданным количеством кадров данных, где устройство для конкатенации содержит

- кодер по п.32, предназначенный для кодирования последних кадров первого битового потока и первых кадров второго битового потока.

41. Устройство для конкатенации по п.40, отличающееся тем, что дополнительно содержит

- блок перенаправления, предназначенный для перенаправления кадров и связанных с ними криптографических величин первого и второго битовых потоков, которые не декодируются и не кодируются.

42. Устройство для конкатенации по одному из пп.40 или 41, отличающееся тем, что дополнительно содержит

- декодер по п.33, предназначенный для кодирования последних кадров первого битового потока, первых кадров второго битового потока и связанных с ними криптографических величин с целью определения статуса доверия первого и второго битовых потоков; и

блок управления, который разблокирует кодер для вставки криптографических величин в часть битового потока только в том случае, если соответствующий первый и второй битовые потоки аутентифицированы.

RU 2012107995 A

RU 2012107995 A