РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2005 125 741** (13) **A**

(51) МПК
H04L 9/08 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2005125741/09, 13.01.2004**

(30) Приоритет: **15.01.2003 JP 2003-7349**
04.04.2003 JP 2003-101455

(43) Дата публикации заявки: **10.01.2006 Бюл. № 01**

(85) Дата перевода заявки PCT на национальную фазу: **15.08.2005**

(86) Заявка PCT:
JP 2004/000155 (13.01.2004)

(87) Публикация PCT:
WO 2004/064313 (29.07.2004)

Адрес для переписки:
129010, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Г.Б. Егоровой

(71) Заявитель(и):
МАЦУСИТА ЭЛЕКТРИК ИНДАСТРИАЛ КО., ЛТД. (JP)

(72) Автор(ы):
НАКАНО Тосихиса (JP),
ОХМОРИ Мотодзи (JP),
МАЦУЗАКИ Нацуме (JP),
ТАТЕБАЯСИ Макото (JP),
ЯМАМОТО Наоки (JP),
ИСИХАРА Хидеси (JP)

(74) Патентный поверенный:
Егорова Галина Борисовна

(54) СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИОННОГО СОДЕРЖАНИЯ, УСТРОЙСТВО ГЕНЕРАЦИИ ДАННЫХ КЛЮЧЕЙ И ОКОНЕЧНОЕ УСТРОЙСТВО

Формула изобретения

1. Система защиты содержания, в которой содержание может использоваться только действительным оконечным устройством, содержащая устройство генерации данных ключей, которое содержит блок преобразования, предназначенный для преобразования, на основе предварительно заданного правила преобразования, первых данных ключа для использования при использовании содержания, при этом генерируя вторые данные ключа; блок шифрования, предназначенный для шифрования вторых данных ключа с использованием ключа устройства, хранимого действительным оконечным устройством, при этом генерируя зашифрованные данные ключа; и блок вывода, предназначенный для вывода зашифрованных данных ключа, и оконечное устройство, которое содержит блок получения, предназначенный для получения зашифрованных данных ключа; блок дешифрования, предназначенный для дешифрования зашифрованных данных ключа с использованием ключа устройства, хранимого в оконечном устройстве, при этом генерируя вторые данные ключа; блок преобразования, предназначенный для преобразования, на основе предварительно заданного правила преобразования, вторых данных ключа, при этом получая первые данные ключа; и блок использования содержания, предназначенный для использования содержания, на основе первых данных ключа.

2. Устройство генерации данных ключей, которое генерирует данные ключей таким образом, чтобы содержание могло использоваться только действительным оконечным устройством, содержащее блок преобразования, предназначенный для преобразования, на

RU 2005125741 A

RU 2005125741 A

основе предварительно заданного правила преобразования, первых данных ключа для использования при использовании содержания, при этом генерируя вторые данные ключа; блок шифрования, предназначенный для шифрования вторых данных ключа с использованием ключа устройства, хранимого действительным оконечным устройством, при этом генерируя зашифрованные данные ключа; и блок вывода, предназначенный для вывода зашифрованных данных ключа.

3. Устройство генерации данных ключей по п.2, в котором блок преобразования генерирует вторые данные ключа путем генерации информации преобразования для ключа устройства, и выполнения обратимой операции над генерируемой информацией преобразования и первыми данными ключа, и блок вывода дополнительно выводит информацию преобразования.

4. Устройство генерации данных ключей по п.3, дополнительно содержащее блок распределения ключей, предназначенный для соотнесения ключей устройств, которые хранятся в оконечных устройствах, с узлами древовидной структуры, которая определяет соотношения между ключами устройств, совместно используемыми оконечными устройствами; и блок выбора, предназначенный для выбора, из ключей устройств, хранимых действительными оконечными устройствами, одного или более ключей устройств, которые соответствуют узлу в самой верхней позиции в древовидной структуре, причем блок преобразования генерирует информацию преобразования на основе информации о позиции каждого из одного или более выбранных ключей устройств в древовидной структуре, и блок шифрования шифрует вторые данные ключа в соответствии с использованием каждого из одного или более выбранных ключей устройства.

5. Устройство генерации данных ключей по п.4, в котором блок преобразования генерирует информацию преобразования для каждого из одного или более выбранных ключей устройства путем конкатенации сегментов идентификационной информации, каждый из которых идентифицирует путь на маршруте от корня до узла, которому соответствует выбранный ключ устройства в древовидной структуре.

6. Устройство генерации данных ключей по п. 4, в котором блок преобразования генерирует, в качестве информации преобразования для каждого из одного или более выбранных ключей устройств, данные, которые отражают позицию узла, соответствующего выбранному ключу устройства, причем позиция выражается через соотношение позиций между уровнями в древовидной структуре и между узлами на одном уровне.

7. Устройство генерации данных ключей по п.3, дополнительно содержащее блок распределения ключей, предназначенный для соотнесения ключей устройств, которые хранятся в оконечных устройствах, с узлами древовидной структуры, которая определяет соотношения между ключами устройств, совместно используемыми оконечными устройствами, и определяет, не был ли аннулирован каждый из ключей устройств; и блок выбора, предназначенный для выбора, из ключей устройств, хранимых действительными оконечными устройствами, одного или более ключей устройств, которые соответствуют узлу в самой верхней позиции в древовидной структуре, причем блок преобразования генерирует информацию преобразования для каждого из одного или более выбранных ключей устройств на основе информации об аннулировании, определенной на основе узла, с которым соотнесен выбранный ключ устройства, и состояния аннулирования для других узлов.

8. Устройство генерации данных ключей по п.7, в котором блок преобразования генерирует информацию преобразования путем конкатенации сегментов информации аннулирования, каждый из которых относится к узлу, позиционированному на маршруте от корня до узла, которому соответствует выбранный ключ устройства.

9. Устройство генерации данных ключей по п. 7, в котором блок преобразования генерирует информацию преобразования путем конкатенации, из информации аннулирования, соответствующей узлам, упорядоченным в предварительно заданном порядке, от первого сегмента информации аннулирования до сегмента информации аннулирования узла, который соответствует выбранному ключу устройства.

10. Устройство генерации данных ключей по п.2, в котором блок преобразования

RU 2005125741 A

RU 2005125741 A

генерирует вторые данные ключа путем генерации информации преобразования для ключа устройства, и помещает информацию преобразования по меньшей мере в часть избыточной части первых данных ключа.

11. Устройство генерации данных ключей по п.10, в котором блок преобразования генерирует вторые данные ключа путем генерации случайного числа для ключа устройства и помещения генерированного случайного числа по меньшей мере в часть избыточной части первых данных ключа.

12. Устройство генерации данных ключей по п.11, в котором блок преобразования использует оставшуюся часть избыточной части, в которую не помещено случайное число, для передачи другой информации.

13. Устройство генерации данных ключей по п.2, в котором блок вывода записывает зашифрованные данные ключа на переносной носитель записи.

14. Устройство генерации данных ключей по п.2, в котором блок вывода выводит зашифрованные данные ключа с использованием среды передачи данных.

15. Устройство генерации данных ключей по п.2, в котором блок преобразования преобразует первые данные ключа на основе правила преобразования, определенного во взаимосвязи с ключами устройств, хранимых действительными оконечными устройствами.

16. Оконечное устройство, которое использует содержание, содержащее блок получения, предназначенный для получения зашифрованных данных ключа, которые были генерированы устройством генерации данных ключей, преобразующим первые данные ключа, на основе предварительно заданного правила преобразования, для генерации данных ключа и шифрования вторых данных ключа с использованием ключа устройства, причем первые данные ключа предназначены для использования при использовании содержания; блок дешифрования, предназначенный для дешифрования зашифрованных данных ключа с использованием ключа устройства, хранимого в оконечном устройстве, при этом получая вторые данные ключа; блок преобразования, предназначенный для преобразования, на основе предварительно заданного правила преобразования, вторых данных ключа, при этом получая первые данные ключа; и блок использования содержания, предназначенный для использования содержания, на основе первых данных ключа.

17. Оконечное устройство по п.16, дополнительно содержащее блок хранения, предназначенный для хранения множества ключей устройств, и блок выбора, предназначенный для выбора одного из ключей устройств, причем блок получения получает зашифрованные данные, которые были генерированы устройством генерации данных ключей, получающим вторые данные ключа путем выполнения обратимой операции над первыми данными ключа и информацией преобразования, генерированной для ключа устройства, и шифрования вторых данных ключа, блок дешифрования осуществляет дешифрование с использованием выбранного ключа устройства, и блок преобразования генерирует информацию первого ключа путем генерации информации преобразования для выбранного ключа устройства и применения предварительно заданной операции к выбранному ключу устройства с использованием информации преобразования.

18. Оконечное устройство по п.17, в котором блок преобразования генерирует информацию преобразования из информации заголовка, связанной с зашифрованными данными ключа.

19. Оконечное устройство по п.18, в котором информация заголовка используется для генерации информации преобразования, и генерирована устройством генерации данных ключей, которое распределяет ключи устройств с использованием древовидной структуры, выбирая из ключей устройств, хранимых действительными оконечными устройствами, один или более ключей устройств, которые соответствуют узлу в самой верхней позиции в древовидной структуре, и генерирует информацию заголовка на основе информации о позиции каждого из одного или более выбранных ключей устройств в древовидной структуре, причем блок хранения хранит информацию о позиции оконечного устройства, и блок преобразования генерирует информацию преобразования с использованием информации заголовка и хранимой информации о позиции.

RU 2005125741 A

RU 2005125741 A

20. Оконечное устройство по п.18, в котором информация заголовка предназначена для генерации информации преобразования и генерирована путем соотнесения ключей устройств, которые хранятся в оконечных устройствах, с узлами в древовидной структуре, которая определяет соотношения между ключами устройств, совместно используемыми оконечными устройствами, и определяет, аннулирован или нет каждый из ключей устройств, выбирая из ключей устройств, хранимых действительными оконечными устройствами по меньшей мере один ключ устройства, который соответствует узлу в самой верхней позиции в древовидной структуре, и основывая информацию заголовка на информации аннулирования, определенной на основе узла, которому соответствует выбранный ключ устройства, и состоянии аннулирования других узлов, блок сохранения сохраняет информацию о позиции оконечного устройства в древовидной структуре для распределения ключей устройств для оконечных устройств в устройстве генерации данных ключей, и блок преобразования генерирует информацию преобразования с использованием информации заголовка и сохраненной информации о позиции.

21. Оконечное устройство по п.16, в котором вторые данные ключа генерируются устройством генерирования данных ключей путем помещения информации преобразования, генерированной для ключа устройства по меньшей мере в часть избыточной части первых данных ключа, и блок преобразования генерирует первые данные ключа путем удаления избыточной части вторых данных ключа.

22. Оконечное устройство по п.16, в котором блок использования содержания содержит субблок шифрования, предназначенный для шифрования содержания на основе первых данных ключа, при этом генерируя зашифрованное содержание, и субблок вывода, предназначенный для вывода зашифрованного содержания.

23. Оконечное устройство по п.16, в котором блок использования содержания дополнительно содержит субблок получения содержания, предназначенный для получения зашифрованного содержания, субблок дешифрования, предназначенный для дешифрования зашифрованного содержания на основе первых данных ключа, при этом генерируя содержание; и субблок воспроизведения, предназначенный для воспроизведения содержания.

24. Носитель записи, предназначенный для записи данных ключа, используемых при шифровании и дешифровании содержания, в котором носитель записи содержит записанные на него зашифрованные данные ключа, которые генерированы устройством генерации данных ключей, преобразующим, на основе предварительно заданного правила преобразования, первые данные ключа, получая при этом вторые данные ключа, и зашифровывающим вторые данные ключа с использованием ключа устройства, хранимого действительным оконечным устройством.

25. Носитель записи по п.24, дополнительно содержащий записанную на нем информацию преобразования, причем информация преобразования предназначена для использования в обратимой операции, применяемой к первым данным ключа при генерации вторых данных ключа.

26. Носитель записи по п.25, в котором записанная на нем информация преобразования генерирована устройством генерации данных ключей посредством соотнесения ключей устройств, которые хранятся оконечными устройствами, с узлами в древовидной структуре, которая определяет соотношения между ключами устройств, совместно используемыми оконечными устройствами, и путем базирования информации преобразования на информации о позиции одного или более ключей устройств, из ключей устройств, хранимых действительными оконечными устройствами, которые соответствуют узлу в самой верхней позиции в древовидной структуре.

27. Носитель записи по п.25, в котором записанная на нем информация преобразования генерирована устройством генерации данных ключей посредством соотнесения ключей устройства, которые хранятся оконечными устройствами, с узлами в древовидной структуре, которая определяет соотношения между ключами устройств, совместно используемыми оконечными устройствами, и определяет, аннулирован или нет каждый из ключей устройств, выбора из ключей устройств, сохраняемых действительными

RU 2005125741 A

RU 2005125741 A

оконечными устройствами, одного или более ключей устройств, которые соответствуют узлу в самом верхней позиции в древовидной структуре, и путем базирования информации заголовка на информации аннулирования, определенной на основе узла, с которым соотнесены один или более выбранных ключей устройств, и состоянии аннулирования других узлов.

28. Способ, используемый устройством генерации данных ключей, которое генерирует данные ключей таким образом, чтобы содержание могло использоваться только действительным оконечным устройством, причем способ содержит этап преобразования в блоке преобразования, преобразующем, на основе предварительно заданного правила преобразования, первые данные ключа для использования при использовании содержания, при этом генерируя вторые данные ключа; этап шифрования в блоке шифрования, зашифровывающем вторые данные ключа с использованием ключа устройства, хранимого действительным оконечным устройством, при этом генерируя зашифрованные данные ключа; и этап вывода в блоке вывода, выводящем зашифрованные данные ключа.

29. Программа, используемая устройством генерации данных ключей, которое генерирует данные ключей таким образом, чтобы содержание могло использоваться только действительным оконечным устройством, причем программа содержит этап преобразования в блоке преобразования, преобразующем, на основе предварительно заданного правила преобразования, первые данные ключа для использования при использовании содержания, при этом генерируя вторые данные ключа; этап шифрования в блоке шифрования, зашифровывающем вторые данные ключа с использованием ключа устройства, хранимого действительным оконечным устройством, при этом генерируя зашифрованные данные ключа; и этап вывода в блоке вывода, выводящем зашифрованные данные ключа.

30. Машиночитаемый носитель записи, содержащий записанную на нем программу, используемую устройством генерации данных ключей, которое генерирует данные ключей таким образом, чтобы содержание могло использоваться только действительным оконечным устройством, причем программа содержит этап преобразования в блоке преобразования, преобразующем, на основе предварительно заданного правила преобразования, первые данные ключа для использования при использовании содержания, при этом генерируя вторые данные ключа; этап шифрования в блоке шифрования, зашифровывающем вторые данные ключа с использованием ключа устройства, хранимого действительным оконечным устройством, при этом генерируя зашифрованные данные ключа; и этап вывода в блоке вывода, выводящем зашифрованные данные ключа.

RU 2005125741 A

RU 2005125741 A