РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2014 151 791** (13) **A**

(51) МПК
H04L 9/08 (2006.01)

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2014151791, 24.04.2013**

Приоритет(ы):
(30) Конвенционный приоритет:
21.05.2012 US 61/649,464;
04.12.2012 US 61/732,997;
07.12.2012 EP 12196092.6

(43) Дата публикации заявки: **20.07.2016** Бюл. № **20**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **22.12.2014**

(86) Заявка PCT:
IB 2013/053224 (24.04.2013)

(87) Публикация заявки PCT:
WO 2013/175324 (28.11.2013)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"

(71) Заявитель(и):
КОНИНКЛЕЙКЕ ФИЛИПС Н.В. (NL)

(72) Автор(ы):
ГАРСИЯ МОРЧОН Оскар (NL),
ТОЛХЭЙЗЕН Людовикус Маринус Герардус Мария (NL)

(54) ОПРЕДЕЛЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

(57) Формула изобретения

1. Способ функционирования первого блока (101) связи, при этом способ содержит этапы, на которых:

- получают (401) материал для локального ключа для первого блока (101) связи, причем материал для локального ключа предоставлен от доверительной третьей стороны и задает первую функцию генерирования ключа для генерирования криптографического ключа как функции по меньшей мере одного идентификатора блока связи, отличного от первого блока связи;
- получают (403) идентификатор для второго блока (103) связи, причем второй блок (103) связи отличен от первого блока (101) связи;
- определяют (405) первый криптографический ключ с помощью первой функции генерирования ключа на основе идентификатора упомянутого второго блока (103) связи;
- локально генерируют (407) значение возмущения для первого криптографического ключа, причем значение возмущения не определяется однозначно данными, предоставленными от доверительной третьей стороны; и
- определяют (409) второй криптографический ключ посредством применения значения возмущения к первому криптографическому ключу.

RU 2014151791 A

RU 2014151791 A

2. Способ по п. 1, дополнительно содержащий этапы, на которых:

генерируют (411) данные с использованием второго криптографического ключа; и

передают (413) данные второму блоку (103) связи.

3. Способ по п. 1, в котором этап локального генерирования (407) содержит этап, на котором генерируют значение возмущения в зависимости от идентификатора для второго блока связи.

4. Способ по п. 3, в котором этап локального генерирования (407) значения возмущения содержит этап, на котором определяют значение возмущения как функцию идентификатора второго блока связи.

5. Способ по п. 1, в котором значение возмущения генерируется как произвольное значение с использованием распределения вероятностей.

6. Способ по п. 5, в котором распределение вероятностей является конфиденциальным для первого блока (101) связи.

7. Способ по п. 1, в котором значение возмущения имеет величину не более чем 10% от величины первого криптографического ключа.

8. Способ по п. 1, в котором второй криптографический ключ генерируется за счет модульного объединения первого криптографического ключа и значения возмущения, причем модульное объединение использует общедоступное значение модуля.

9. Способ функционирования первого блока (103) связи, при этом способ содержит этапы, на которых:

- получают (501) материал для локального ключа для первого блока (103) связи, причем материал для локального ключа предоставлен от доверительной третьей стороны и задает функцию генерирования ключа для генерирования криптографического ключа как функции по меньшей мере одного идентификатора блока связи, отличного от первого блока связи;

- получают (503) идентификатор для второго блока (101) связи, причем второй блок (101) связи отличен от первого блока (103) связи;

- определяют (505) первый криптографический ключ с помощью функции генерирования ключа на основе идентификатора второго блока (101) связи;

- принимают (511) данные из второго блока (101) связи, причем данные сгенерированы с использованием третьего криптографического ключа, при этом третий криптографический ключ представляет собой объединение значения возмущения и криптографического ключа, зависящего от идентификатора первого блока связи;

- определяют (507) набор возможных значений возмущения для второго блока (101) связи;

- определяют (509) набор возможных криптографических ключей с помощью набора возможных значений возмущения и первого криптографического ключа; и

- выбирают (513) криптографический ключ коллективного пользования для второго блока (101) связи посредством выполнения криптографической операции в отношении данных, используя каждый из криптографических ключей из набора возможных криптографических ключей, и выбора криптографического ключа коллективного пользования в качестве криптографического ключа из набора возможных криптографических ключей, который удовлетворяет критерию достоверности для криптографической операции.

10. Способ по п. 9, в котором этап определения (509) набора возможных криптографических ключей дополнительно содержит этап, на котором определяют возможные криптографические ключи в ответ на возможную несимметричность между первым криптографическим ключом и криптографическим ключом, зависящим от идентификатора первого блока (103) связи.

11. Способ функционирования системы связи, содержащей множество блоков связи,

RU 2014151791 A

RU 2014151791 A

при этом способ содержит этап, на котором первый блок (101) связи выполняет этапы, на которых:

- получают (401) материал для локального ключа для первого блока (101) связи, причем материал для локального ключа предоставлен от доверительной третьей стороны и задает первую функцию генерирования ключа для генерирования криптографического ключа как функции по меньшей мере одного идентификатора блока связи, отличного от первого блока связи;
- получают (403) идентификатор для второго блока (103) связи, причем второй блок (103) связи отличен от первого блока (101) связи;
- определяют (405) первый криптографический ключ с помощью первой функции генерирования ключа на основе идентификатора упомянутого второго блока (103) связи;
- локально генерируют (407) значение возмущения для первого криптографического ключа, причем значение возмущения не определяется однозначно данными, предоставленными от доверительной третьей стороны; и
- определяют (409) второй криптографический ключ посредством применения значения возмущения к первому криптографическому ключу;
- генерируют (411) данные с использованием второго криптографического ключа;
- передают (412) данные второму блоку (103) связи; и

этап, на котором второй блок (103) связи выполняет этапы, на которых:

- получают (501) материал для локального ключа для второго

блока (103) связи, причем материал для локального ключа предоставлен от доверительной третьей стороны и задает вторую функцию генерирования ключа для генерирования криптографического ключа как функции по меньшей мере одного идентификатора блока связи, отличного от второго блока связи;

- получают (503) идентификатор для первого блока (101) связи;
- определяют (505) третий криптографический ключ с помощью второй функции генерирования ключа на основе идентификатора первого блока (101) связи;
- принимают (511) данные из первого блока (101) связи;
- определяют (507) набор возможных значений возмущения для первого блока (101) связи;
- определяют (509) набор возможных криптографических ключей посредством применения набора возможных значений возмущения к третьему криптографическому ключу; и
- выбирают (513) криптографический ключ коллективного пользования для первого блока (101) связи посредством выполнения криптографической операции в отношении данных, используя каждый из криптографических ключей из набора возможных криптографических ключей, и выбора криптографического ключа коллективного пользования в качестве криптографического ключа из набора возможных криптографических ключей, который удовлетворяет критерию достоверности для криптографической операции.

12. Блок связи, содержащий:

- процессор (203) для получения материала для локального ключа для блока связи, причем материал для локального ключа предоставлен от доверительной третьей стороны и задает первую функцию генерирования ключа для генерирования криптографического ключа как функции по меньшей мере одного идентификатора другого блока связи;
- процессор (205) для получения идентификатора для другого блока связи;
- процессор (207) для определения первого криптографического ключа с помощью первой функции генерирования ключа на основе идентификатора другого блока связи;
- генератор (209) для локального генерирования значения возмущения для первого

RU 2014151791 A

RU 2014151791 A

криптографического ключа, причем значение

возмущения не определено однозначно данными, предоставленными от доверительной третьей стороны; и

- процессор (211) для определения второго криптографического ключа посредством применения значения возмущения к первому криптографическому ключу.

13. Блок связи, содержащий:

- процессор (303) для получения материала для локального ключа для блока связи, причем материал для локального ключа предоставлен от доверительной третьей стороны и задает функцию генерирования ключа для генерирования криптографического ключа как функции по меньшей мере одного идентификатора другого блока связи;

- процессор (305) для получения идентификатора для другого блока связи;

- процессор (307) для определения первого криптографического ключа с помощью функции генерирования ключа на основе идентификатора другого блока связи;

- приемник (301) для приема данных из другого блока связи, причем данные сгенерированы с использованием третьего криптографического ключа, при этом третий криптографический ключ представляет собой объединение значения возмущения и криптографического ключа, зависящего от идентификатора блока связи;

- процессор (309) для определения набора возможных значений возмущения для другого блока связи;

- процессор (311) для определения набора возможных криптографических ключей с помощью набора возможных значений возмущения и первого криптографического ключа; и

- селектор (313) для выбора криптографического ключа коллективного пользования для другого блока связи посредством выполнения криптографической операции в отношении данных, используя каждый из криптографических ключей из набора возможных криптографических ключей, и выбора криптографического ключа коллективного пользования в качестве криптографического ключа из набора возможных криптографических ключей, который удовлетворяет критерию достоверности для криптографической операции.

14. Система связи, содержащая:

первый блок (101) связи, содержащий:

- процессор (203) для получения материала для локального ключа для первого блока связи, причем материал для локального ключа предоставлен от доверительной третьей стороны и задает первую функцию генерирования ключа для генерирования криптографического ключа как функции по меньшей мере одного идентификатора блока связи, отличного от первого блока связи;

- процессор (205) для получения идентификатора для второго блока (103) связи, причем второй блок (103) связи отличен от первого блока связи;

- процессор (207) для определения первого криптографического ключа с помощью первой функции генерирования ключа на основе идентификатора второго блока (103) связи;

- генератор (209) для локального генерирования значения возмущения для первого криптографического ключа, причем значение возмущения не определено однозначно данными, предоставленными от доверительной третьей стороны;

- процессор (211) для определения второго криптографического ключа посредством применения значения возмущения к первому криптографическому ключу;

- генератор данных для генерирования данных с использованием второго криптографического ключа;

- передатчик (201) для передачи данных второму блоку связи; и

второй блок (103) связи, содержащий:

RU 2014151791 A

RU 2014151791 A

- процессор (303) для получения материала для локального ключа для второго блока связи, причем материал для локального ключа предоставлен от доверительной третьей стороны и задает вторую функцию генерирования ключа для генерирования криптографического ключа как функции по меньшей мере одного идентификатора блока связи, отличного от второго блока связи;

- процессор (305) для получения идентификатора для первого блока (101) связи;

- процессор (307) для определения третьего криптографического ключа с помощью второй функции генерирования ключа на основе идентификатора первого блока (101) связи;

- приемник (301) для приема данных из первого блока (101) связи;

- процессор для определения набора возможных значений
возмущения для первого блока связи;

- процессор (309) для определения набора возможных криптографических ключей посредством применения набора возможных значений возмущения к третьему криптографическому ключу; и

- процессор (313) для выбора криптографического ключа коллективного пользования для первого блока связи посредством выполнения криптографической операции в отношении данных, используя каждый из криптографических ключей из набора возможных криптографических ключей, и выбора криптографического ключа коллективного пользования в качестве криптографического ключа из набора возможных криптографических ключей, который удовлетворяет критерию достоверности для криптографической операции.

15. Компьютерная программа, содержащая средство компьютерного программного кода, выполненное с возможностью осуществления всех этапов по любому одному из пп. 1-10, когда компьютерная программа выполняется на компьютере.

16. Компьютерная программа по п. 15, содержащаяся на машиночитаемом носителе.

RU 2014151791 A

RU 2014151791 A