



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: 2017106302, 29.07.2014

Приоритет(ы):

(22) Дата подачи заявки: 29.07.2014

(43) Дата публикации заявки: 28.08.2018 Бюл. № 25

(85) Дата начала рассмотрения заявки РСТ на национальной фазе: 28.02.2017

(86) Заявка РСТ:
CN 2014/083222 (29.07.2014)(87) Публикация заявки РСТ:
WO 2016/015222 (04.02.2016)

Адрес для переписки:

109012, Москва, ул. Ильинка, 5/2, ООО
"Союзпатент"

(71) Заявитель(и):

ХУАВЕЙ ТЕКНОЛОДЖИЗ КО., ЛТД.
(CN)

(72) Автор(ы):

ЧЖАНГ Лисюэ (CN),
ЛУ Чжэньвэй (CN)**(54) УСТРОЙСТВО И СПОСОБ ШИФРОВАНИЯ И ПЕРЕДАЧИ ДАННЫХ****(57) Формула изобретения**

1. Устройство шифрования и передачи данных, содержащее: модуль (11) обработки, выполненный с возможностью равномерного разделения исходных данных на N пакетов первых данных, причем N является положительным целым числом; шифрования по меньшей мере одного пакета первых данных в N пакетах первых данных для получения N пакетов зашифрованных первых данных, где номер по меньшей мере одного первого пакета данных имеет максимум N-1; и кодирования, с использованием фонтанного кода, N пакетов зашифрованных первых данных для получения M пакетов вторых данных, где M представляет собой целое положительное число, причем $M > N$; и

модуль (12) передачи, выполненный с возможностью передачи M пакетов вторых данных, полученных модулем (11) обработки, на сторону приема.

2. Устройство шифрования и передачи данных по п. 1, в котором модуль (11) обработки в частности выполнен с возможностью шифрования по меньшей мере одного пакета первых данных в N пакетах первых данных и добавления, к заголовку каждого из пакетов, первых данных информации указания, указывающей, зашифрован ли пакет первых данных, для получения N пакетов зашифрованных первых данных.

3. Устройство шифрования и передачи данных по п. 1 или 2, в котором модуль (12) передачи дополнительно выполнен с возможностью передачи информации уведомления шифрования на сторону приема перед передачей M пакетов вторых данных, полученных

с помощью модуля (11) обработки, на сторону приема, при этом информация уведомления шифрования включает в себя информацию указания, указывающую, что исходные данные сначала шифруются, а затем кодируются с помощью фонтанного кода.

4. Устройство шифрования и передачи данных по п. 1, в котором модуль (12) передачи дополнительно выполнен с возможностью передачи информации уведомления шифрования на сторону приема перед передачей M пакетов вторых данных, полученных с помощью модуля (11) обработки, на сторону приема, при этом информация уведомления шифрования включает в себя информацию указания, указывающую, что исходные данные сначала шифруются и затем кодируются с помощью фонтанного кода, и информацию указания, указывающую, зашифрован ли каждый из пакетов первых данных.

5. Устройство шифрования и передачи данных, содержащее:

модуль (31) обработки, выполненный с возможностью равномерного разделения исходных данных на N пакетов первых данных, причем N является положительным целым числом; кодирования, с использованием фонтанного кода, N пакетов первых данных для получения M пакетов вторых данных, где M представляет собой целое положительное число и $M > N$; и шифрования по меньшей мере $M-N+1$ пакетов вторых данных в M пакетах вторых данных для получения M пакетов зашифрованных вторых данных, где номер по меньшей мере $M-N+1$ пакетов вторых данных имеет максимум $M-1$; и

модуль (32) передачи, выполненный с возможностью передачи M пакетов зашифрованных вторых данных, полученных с помощью модуля (31) обработки, на сторону приема.

6. Устройство шифрования и передачи данных по п. 5, в котором модуль (31) обработки, в частности, выполнен с возможностью шифрования по меньшей мере $M-N+1$ пакеты вторых данных в M пакетах вторых данных и добавления, к заголовку каждого из пакетов вторых данных информации указания, указывающей, зашифрован ли пакет вторых данных, для получения M пакетов зашифрованных вторых данных.

7. Устройство шифрования и передачи данных по п. 5 или 6, в котором модуль (32) передачи дополнительно выполнен с возможностью передачи информации уведомления шифрования на сторону приема перед передачей M пакетов зашифрованных вторых данных, полученных с помощью модуля (31) обработки, на сторону приема, при этом информация уведомления шифрования содержит информацию указания, указывающую, что исходные данные сначала кодируются с использованием фонтанного кода и затем шифруются.

8. Способ шифрования и передачи данных, содержащий этапы, на которых:

осуществляют (S501) равномерное разделение исходных данных на N пакетов первых данных, где N является положительным целым числом;

осуществляют (S502) шифрование по меньшей мере одного пакета первых данных в N пакетах первых данных, для получения N пакетов зашифрованных первых данных, где номер по меньшей мере одного первого пакета данных имеет максимум $N-1$;

кодируют (S503) с помощью фонтанного кода N пакетов зашифрованных первых данных для получения M пакетов вторых данных, где M представляет собой целое положительное число, причем $M > N$; и

передают (S504) M пакетов вторых данных на сторону приема.

9. Способ по п. 8, в котором этап шифрования (S502) по меньшей мере одного пакета первых данных в N пакетах первых данных для получения N пакетов зашифрованных первых данных содержит подэтапы, на которых:

осуществляют шифрование по меньшей мере одного пакета первых данных в N

пакетах первых данных и добавляют к заголовку каждого из пакетов первых данных информацию указания, указывающую, зашифрован ли пакет первых данных, для получения N пакетов шифрованных первых данных.

10. Способ по п. 8 или 9, дополнительно содержащий перед этапом передачи (S504) M пакетов вторых данных на сторону приема этап, на котором:

передают информацию уведомления шифрования на сторону приема, причем информация уведомления шифрования содержит информацию указания, указывающую, что исходные данные сначала шифруются и затем кодируются с помощью фонтанного кода.

11. Способ по п. 8, дополнительно содержащий перед этапом передачи (S504) M пакетов вторых данных на сторону приема этап, на котором:

передают информацию уведомления шифрования на сторону приема, при этом информация уведомления шифрования содержит информацию указания, указывающую, что исходные данные сначала шифруются и затем кодируются с помощью фонтанного кода, и информацию указания, указывающую, зашифрован ли каждый из пакетов первых данных.

12. Способ шифрования и передачи данных, содержащий этапы, на которых:

осуществляют (S701) равномерное разделение исходных данных на N пакеты первых данных, где N является положительным целым числом;

осуществляют (S702) кодирование с помощью фонтанного кода N пакетов первых данных для получения M пакетов вторых данных, причем M представляет собой целое положительное число, причем $M > N$;

осуществляют (S703) шифрование по меньшей мере $M-N + 1$ пакетов вторых данных в M пакетах вторых данных для получения M пакетов шифрованных вторых данных, где номер по меньшей мере $M-N + 1$ пакетов вторых данных имеет максимум M-1; и

передают (S704) M пакетов шифрованных вторых данных на сторону приема.

13. Способ по п. 12, в котором этап шифрования (S703) по меньшей мере $M-N + 1$ пакетов вторых данных в M пакетах вторых данных для получения M пакетов шифрованных вторых данных содержит подэтапы, на которых:

осуществляют шифрование по меньшей мере $M-N+1$ пакетов вторых данных в M пакетах вторых данных и добавляют к заголовку каждого из пакетов вторых данных информацию указания, указывающую, зашифрован ли пакет вторых данных для получения M пакетов шифрованных вторых данных.

14. Способ по п. 12 или 13, дополнительно содержащий перед этапом передачи (S704) M пакетов шифрованных вторых данных на сторону приема этап, на котором:

передают информацию уведомления шифрования на сторону приема, при этом информация уведомления шифрования содержит информацию указания, указывающую, что исходные данные сначала кодируются с использованием фонтанного кода и затем шифруются.

15. Способ по п. 14, в котором этап передачи (S704) информации уведомления шифрования на сторону приема содержит подэтап, на котором:

передают информацию уведомления дешифрования на сторону приема с помощью сообщения о конфигурации управления радиоресурсами (RRC).