РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 566 335** (13) **C1**

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
(51) МПК
H04L 9/08 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

Статус: действует (последнее изменение статуса: 27.10.2015)

(21)(22) Заявка: **2014113183/08, 04.04.2014**

(24) Дата начала отсчета срока действия патента:
04.04.2014

Приоритет(ы):
(22) Дата подачи заявки: **04.04.2014**

(45) Опубликовано: **20.10.2015** Бюл. № **29**

(56) Список документов, цитированных в отчете о поиске: **RU 2302085 C1, 27.06.2007. RU 80637 U1, 10.02.2009. RU 2507690 C1, 20.02.2014. RU 2427926 C1, 27.08.2011. US 7697693 B1, 13.04.2010. US 7894604 B2, 22.02.2011. US 8509446 B2, 13.04.2013**

Адрес для переписки:
107045, Москва, Сретенский б-р, 5, а/я 97, для Мазур Н.З.

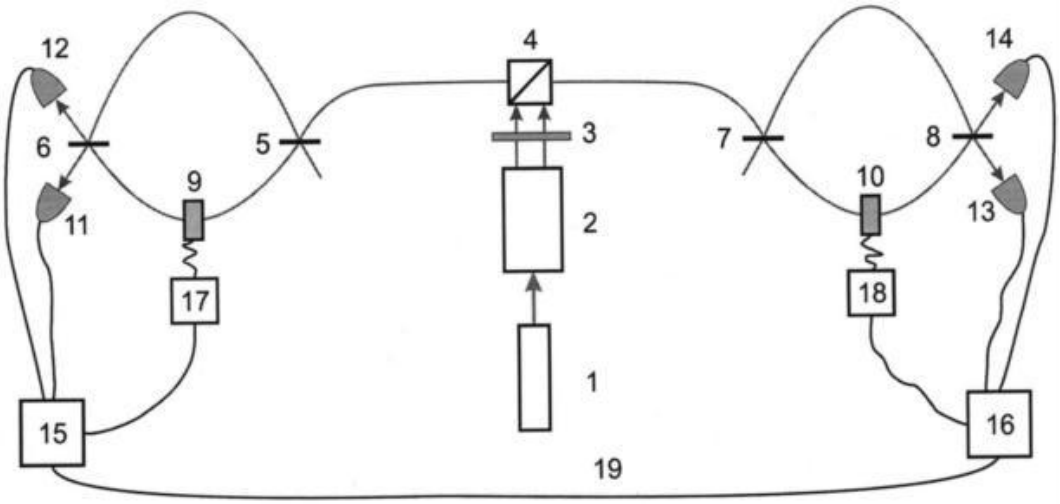
(72) Автор(ы):
Сайгин Михаил Юрьевич (RU),
Проценко Игорь Евгеньевич (RU),
Фирсов Владимир Владимирович (RU),
Магницкий Сергей Александрович (RU)

(73) Патентообладатель(и):
Общество с ограниченной ответственностью "Лаборатория оптико-электронных приборов" (ООО "ЛОЭП") (RU)

(54) СПОСОБ ГЕНЕРАЦИИ СЕКРЕТНЫХ КЛЮЧЕЙ С ПОМОЩЬЮ ПЕРЕПУТАННЫХ ПО ВРЕМЕНИ ФОТОННЫХ ПАР

(57) Реферат:

Изобретение относится к области квантовой криптографии, а более конкретно к способам генерации секретных ключей с помощью перепутанных по времени пар фотонов. Технический результат - обеспечение ускоренного распределения секретных ключей между участниками коммуникации и увеличения дальности передачи секретных ключей. Способ генерации секретных ключей с помощью перепутанных по времени фотонных пар включает распределение между двумя участниками передачи секретных ключей фотонов из перепутанных по времени фотонных пар, дальнейшее преобразование этих фотонов интерферометрами участников, их детектирование детекторами одиночных фотонов и последующую обработку результатов измерений с помощью ЭВМ, включающую коммуникацию между участниками по открытому каналу связи. Дополнительно устанавливают согласованный между участниками временной интервал, в рамках которого проводят разделение на M равные подынтервалы и определяют подынтервалы, в которых у участников срабатывают детекторы одиночных фотонов, после чего номера этих подынтервалов используют в качестве элементов ключей. 1 з.п. ф-лы, 1 ил.



Фиг. 1