ФОРМИРОВАНИЕ КРИПТОГРАФИЧЕСКОГО КЛЮЧА В СОПРЯЖЕННЫХ ПРИЕМО-ПЕРЕДАЮЩИХ АТМОСФЕРНЫХ ЛАЗЕРНЫХ СИСТЕМАХ

DOI: 10.36724/2072-8735-2023-17-2-33-41

Абрамова Евгения Сергеевна,
Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ), г. Новосибирск, Россия, ***evgenka_252@mail.ru***

Адамов Егор Владимирович, Аксенов Валерий Петрович, Богач Егор Андреевич, Дудоров Вадим Витальевич, Колосов Валерий Викторович, Левицкий Михаил Ефимович, Погуца Чеслав Евгеньевич
Институт оптики атмосферы им. В.Е. Зуева СО РАН, г. Томск, Россия, ***adamov@iao.ru; avp@iao.ru; bogach@iao.ru; dvv@iao.ru; kvv@iao.ru; top@iao.ru; pce@iao.ru***

Павлов Иван Иванович,
Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ), г. Новосибирск, Россия, ***iipavlov02@mail.ru***

Manuscript received 14 January 2023;
Accepted 10 February 2023

Работа выполнена в рамках госзадания ИОА СО РАН и финансово поддержана Фондом содействия инновациям (ФСИ) в рамках выполнения НИОКР по договору №4598ГС1/73980 в части разработки приемо-передающего модуля

Ключевые слова: *лазерное излучение, конфиденциальная оптическая связь, криптография, атмосферная турбулентность, флуктуации интенсивности, теорема взаимности*

Безопасность передачи и поиска зависит от шифрования информации, отправляемой по общедоступным сетям. В настоящее время широко используются подходы к защите данных, основанные на методах криптографии с использованием однонаправленных математических функций. Разработаны симметричные и асимметричные методы передачи ключей по открытым каналам связи. Стойкость методов защиты информации с использованием односторонних математических функций базируется на алгоритмической сложности их взлома для современных компьютеров. Появление квантовых компьютеров достаточной мощности кардинально изменит ситуацию. Поэтому в настоящее время остро встает вопрос о разработке методов распределения криптографических ключей на новых принципах. К таким методам относится квантовая криптография и криптография на основе стохастических физических процессов. В данной работе выполнен краткий обзор способов формирования ключа на принципах квантовой физики, а далее исследована возможность использования для генерации ключей флуктуаций принимаемой мощности излучения, вызванных атмосферной турбулентностью. Выполнено численное и экспериментальное моделирование процесса распространения волн в системе двух сопряженных приемо-передатчиков, функционирующих в турбулентной среде (атмосфере). Для этого созданы соответствующие алгоритмы численного моделирования характеристик оптических полей, искаженных атмосферным каналом распространения. Разработана экспериментальная установка и выполнено модельное экспериментальное исследование формирования коррелированных случайных сигналов в приемо-передающих лазерных системах. Обнаружена необходимость использования фильтрации низких частот принимаемых сигналов. Исследована эффективность данной фильтрации. Результаты работы позволяют сделать вывод о том, что использование в качестве генератора случайного сигнала атмосферной турбулентности, позволяет сформировать практически идентичный криптографический ключ в двух направленных друг на друга каналах связи.

Информация об авторах:
Абрамова Евгения Сергеевна, *Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ), доцент кафедры радиотехнических устройств и техносферной безопасности, доцент, к.т.н., г. Новосибирск, Россия*
Адамов Егор Владимирович, *Институт оптики атмосферы им. В.Е. Зуева СО РАН, аспирант лаборатории оптической локации, г. Томск, Россия*
Аксенов Валерий Петрович, *Институт оптики атмосферы им. В.Е. Зуева СО РАН, г.н.с. лаборатории оптической локации, д.ф.-м.н, г. Томск, Россия*
Богач Егор Андреевич, *Институт оптики атмосферы им. В.Е. Зуева СО РАН, аспирант лаборатории оптической локации, г. Томск, Россия*
Дудоров Вадим Витальевич, *Институт оптики атмосферы им. В.Е. Зуева СО РАН, г.н.с. лаборатории оптической локации, д.ф.-м.н, г. Томск, Россия*
Колосов Валерий Викторович, *Институт оптики атмосферы им. В.Е. Зуева СО РАН, г.н.с. лаборатории оптической локации, д.ф.-м.н, г. Томск, Россия*
Левицкий Михаил Ефимович, *Институт оптики атмосферы им. В.Е. Зуева СО РАН, с.н.с. лаборатории оптической локации, г. Томск, Россия*
Погуца Чеслав Евгеньевич, *Институт оптики атмосферы им. В.Е. Зуева СО РАН, н.с. лаборатории оптической локации, к.ф.-м.н, г. Томск, Россия*
Павлов Иван Иванович, *Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ), доцент кафедры радиотехнических устройств и техносферной безопасности, доцент, к.т.н., г. Новосибирск, Россия*

Для цитирования:
Абрамова Е.С., Адамов Е.В., Аксенов В.П., Богач Е.А., Дудоров В.В., Колосов В.В., Левицкий М.Е., Погуца Ч.Е., Павлов И.И. Формирование криптографического ключа в сопряженных приемо-передающих атмосферных лазерных системах // T-Comm: Телекоммуникации и транспорт. 2023. Том 17. №2. С. 33-41.

For citation:
Abramova E.S., Adamov E.V., Aksenov V.P., Bogach E.A., Dudorov V.V., Kolosov V.V., Levitsky M.E., Pogutsa C.E., Pavlov I.I. (2023). Cryptographic key formation in coupled transmit-receiving atmospheric laser systems. *T-Comm*, vol. 17, no.2, pp. 33-41. (*in Russian*)

Введение

Обеспечение безопасности и защиты данных является одной из самых серьезных проблем, связанных с быстрым развитием современных информационных технологий. Все больше и больше конфиденциальных данных хранится на удаленных компьютерных серверах, например, в облаке, что делает безопасный доступ к этим данным главной задачей. Безопасность передачи и поиска зависит от шифрования информации, отправляемой по общедоступным сетям. В настоящее время широко используются подходы к защите данных, которые используют методы криптографии, основанные на математических функциях.

Присущая беспроводной связи широковещательная природа позволяет получать передачи любому пользователю в пределах досягаемости, в результате чего злоумышленники могут инициировать различные пассивные атаки, такие как прослушивание, анализ и мониторинг трафика и т. д., или выполнять активные атаки, такие как глушение, спуфинг, модификация, воспроизведение и атака типа «отказ в обслуживании» (DoS) и т. д.

Существует обширный исследовательский интерес к защите беспроводной передачи. Традиционно данные защищаются классическими схемами шифрования, которые работают в предположении, что алгоритм достаточно сложен, так что время, затрачиваемое перехватчиками на взлом криптографической системы, намного больше, чем достоверность самой информации, поэтому гарантируется обратная секретность. Классические схемы шифрования состоят из схем симметричного шифрования и схем асимметричного шифрования в зависимости от ключей, которые используют две криптографические стороны. Схемы симметричного шифрования используют один и тот же ключ и обычно используются для защиты данных благодаря их эффективности при шифровании данных.

Алгоритм с симметричным ключом, также называемый алгоритмом секретного ключа, преобразует данные таким образом, что их чрезвычайно трудно просмотреть, не имея секретного ключа. Ключ считается симметричным, поскольку он используется как для шифрования, так и для расшифровки. Эти ключи обычно известны одному или нескольким уполномоченным лицам. Алгоритмы с асимметричным ключом, также называемые алгоритмами с открытым ключом, используют для выполнения своей функции парные ключи (открытый и закрытый ключи). Открытый ключ известен всем, но закрытый ключ контролируется исключительно владельцем этой пары ключей. Закрытый ключ нельзя вычислить математически с помощью открытого ключа, даже если они криптографически связаны.

Одним из решений проблемы информационной безопасности является разработка методов распределения ключей на новых принципах. Квантовая криптография [1-5] использует стохастические свойства квантовых носителей сигнала. Существует подход, которые использует взаимность электромагнитных волн из точки передатчика в точку приемника и из точки приемника в точку передатчика. Впервые данный подход был реализован для радиоволн [6-10]. Случайной величиной в этом случае являлась задержка времени распространения или фаза несущей волны.

Принцип взаимности говорит, что интенсивность или фаза встречных волн совпадают, если волна проходит в прямом и обратном направлении одни и те же турбулентные неоднородности среды. Однако, использование фазовых флуктуаций целесообразно только в том случае, если они слабые. Если они сильные, т. е. фаза меняется на несколько π, то предпочтительнее флуктуации интенсивности. Результаты экспериментальной реализации принципа взаимности и теоретических расчетов для фиксированных расстояний распространения и апертур приемопередающих систем описаны в [11-16].

1. Криптографическая защита информации на основе квантовой физики

Будущие беспроводные технологии охватывают использование радиочастотных и оптических систем в свободном пространстве (FSO). За последние десятилетия были предприняты обширные исследования по обеспечению безопасности этих беспроводных систем. Традиционно используется классическая криптография, основанная на вычислительной стойкости математических алгоритмов, поэтому ее называют вычислительной безопасностью. Однако его безопасность может оказаться под угрозой в будущем, особенно когда станут доступны крупномасштабные мощные квантовые компьютеры. Чтобы справиться с этим потенциальным риском, должны быть разработаны криптографические схемы, обеспечивающие безопасную связь в соответствии с теорией информации, именуемые теоретико-информационной безопасностью (ТИБ).

Квантовое распределение ключей (quantum key distribution – QKD), одна из первых экспериментально реализуемых технологий в области квантовой информации.

Используя присущую квантовым состояниям непредсказуемость, квантовое распределение ключей можно использовать для безопасного распространения секретного ключа. Первый протокол QKD был предложен Беннеттом и Брассардом в 1984 г., т.е. протокол BB84, который кодирует ключевую информацию о состояниях поляризации фотонов. После этого реализацию QKD можно разделить на две схемы, а именно QKD с дискретной переменной и QKD с непрерывной переменной.

Квантовая обработка информации использует особенности квантовой механики, такие как принцип суперпозиции, запутанность и квантовая интерференция, для создания более эффективных алгоритмов вычислений и безусловно безопасных протоколов связи.

Разрабатывается ряд физических реализаций для создания квантового компьютера. За последние несколько лет фотоника стала ведущим подходом по следующим причинам: отдельные фотоны в значительной степени невосприимчивы к шуму; можно легко манипулировать для реализации логических вентилей с одним кубитом; разрешить кодирование кубитов с несколькими степенями свободы; и идеально подходят для передачи квантовых состояний.

В классических вычислениях основной фундаментальной вычислительной единицей является бит. Он может иметь значение 0 или 1. Аналогичным понятием для квантовых вычислений является квантовый бит или кубит. Как и классический бит, кубит может находиться в одном из двух ортогональных состояний.

На языке квантовой механики состояние кубита представлено вектором в двумерном гильбертовом пространстве, где состояния |0> или |1> известны как вычислительная база. Однако, в отличие от классических вычислений, кубит также может существовать в суперпозиции состояний.

Однако на практике носителями квантов обычно являются фотоны, которые распространяются в волоконно-оптических линиях связи, естественной среде или вакууме.

Любая двухуровневая квантовая система может использоваться для кодирования кубита, например, спины электронов или ядер, поляризация фотонов или сверхпроводники и джозефсоновские контакты, расположенные для формирования потоковых, фазовых или зарядовых кубитов. Однако во всех экспериментах будет использоваться поляризация фотонов как кубитов с двумя ортогональными состояниями |H> и |V>, где H и V относятся к горизонтальной и вертикальной поляризации фотона по отношению к подходящей системе отсчета. |H> и |V> соответствуют базовым вычислительным состояниям |0> и |1> соответственно. Фотоны – идеальные кубиты для квантовых коммуникационных и криптографических схем из-за их слабого взаимодействия друг с другом и большей частью материи. Это слабое взаимодействие приводит к низкой скорости декогеренции, так что кубиты сохраняют свои квантовые состояния в течение длительного времени. Кроме того, они движутся со скоростью света, что позволяет очень быстро передавать их на большие расстояния.

Беннетт и Брассард показали, как можно распределить случайный секретный ключ между двумя сторонами (Алисой и Бобом), используя одиночные кубиты по квантовому каналу. Безопасность их схемы была обусловлена случайными измерениями кубитов в одном из двух комплементарных, неортогональных базисов, а также тем фактом, что квантовая механика запрещает любому потенциальному подслушивателю (Еве) получать информацию о состоянии неизвестного кубита, не нарушая его. Таким образом, любое последующее измерение дополнительной наблюдаемой на том же кубите становится случайным. Алисе и Бобу достаточно начать с небольшого количества общих ресурсов секретный ключ для первоначальной аутентификации друг друга, а затем могут использовать распределение квантового ключа, чтобы распределить между собой настолько большой ключ, насколько это необходимо.

Квантовая криптография все еще находится в зачаточном состоянии с точки зрения практического применения. Затянувшаяся реализация квантовой криптографии является результатом проблем, связанных со скоростью передачи и ограничениями обработки. В настоящее время эти проблемы сложно решить, поскольку потребность в высококачественных одиночных фотонах от лазера на большие расстояния требует низких коэффициентов потерь при передаче, что означает более низкое отношение сигнал/шум для канала. В результате стоимость оборудования для этой технологии намного выше, чем у традиционной криптографии. Кроме того, существуют ограничения обработки из-за необходимости выполнять манипуляции с квантовым состоянием на сайте получателя для обеспечения надлежащей безопасности и защиты данных [17].

Представленные выше методы передачи информации на основе поляризации фотонов и теорема о запрете клонирования квантовых состояний явились основой для разработки протоколов секретного квантового распределения ключей (QKD). К наиболее распространенным схемам QKD (протоколам) можно отнести следующие: BB84 [18], B92 [19], Ekert91 [20] и Yuen-Kumar (Alpha-Eta или Y00) [21], E91 [22].

В [1] приведены результаты натурных экспериментов по апробации алгоритмов QKD на разных линиях в земной атмосфере. Оказывается, что квантовая частота появления ошибочных битов (QBER) пока очень высока и составляет в разных схемах и трассах от 0.5 до 10 %. Это еще одна из очевидных проблем квантовой криптографии.

Сравнение вышеупомянутых алгоритмов приведено в таблице 1.

Таблица 1

Сравнение алгоритмов безопасности

Алгоритм	Описание	Реализация	Сложность	Плюсы	Минусы
Симметричное шифрование	Легитимные пользователи используют один и тот же ключ для шифрования данных	Да	Низкая	Эффективность шифрования данных	Вычислительная безопасность; надежный ключ, необходимый перед
Асимметричное шифрование	Легитимные пользователи используют один и тот же открытый ключ, но разные закрытые ключи для распространения сеансового ключа	Да	Высокая	Распределение ключей с различными закрытыми ключами	Вычислительная безопасность; требуется инфраструктура открытых ключей; не подходит для устройств с низкой вычислительной мощностью
Безопасность без ключа	Легитимные пользователи безопасно общаются, используя разработанный код и свойства канала		Высокая	Информационно-теоретически безопасносный; секретная передача без ключей	Обычно требуется криминалистическая экспертиза подслушивающих устройств
Распределение ключей	Легитимные пользователи используют сгенерированный ключ на основе случайности общего канала	Да	Низкая	Информационно-теоретически безопасный; легкий: не требуется помощь других пользователей	Ограничена динамичностью канала

2. Формирование криптографического ключа на основе случайных свойств среды (турбулентной атмосферы)

Оптические линии связи в свободном пространстве (FSO) обычно используются, когда невозможно или нецелесообразно осуществлять связь через оптоволоконные или проводные линии. Каналы FSO способны обеспечивать связь со скоростью передачи данных свыше 2,5 Гбит/с на расстоянии в несколько километров. Однако, они подвержены влиянию атмосферной турбулентности, поглощения и рассеяния. Рассмотрим теперь атмосферную турбулентность не как фактор, мешающий связи, а как фактор помогающий генерировать криптографические ключи [11].

Генерация ключей основана на трех принципах, а именно: временная вариация, взаимность каналов и пространственная декорреляция.

Временная вариация вносится движением передатчика, приемника или любых объектов в окружающей среде, что изменяет рефракцию, преломление и рассеяние канальных путей. Случайность, вызванная таким непредсказуемым движением, может быть использована в качестве случайного источника для генерации ключей. Однако в статичной среде, где эти характеристики остаются неизменными, случайность довольно ограничена. Темпоральная вариация все же необходима для того, чтобы ввести достаточный уровень случайности. Она может быть квантована автокорреляционной функцией (АКФ) сигнала.

Взаимность каналов подразумевает, что многолучевость и затухание на обоих концах одного канала, т.е. одинаковая несущая частота, идентичны, что является основанием для Алисы и Боба генерировать один и тот же ключ. Сигналы должны быть измерены аппаратными платформами, которые обычно работают в полудуплексном режиме и вносят шум. Поэтому принимаемые сигналы в восходящем и нисходящем каналах асимметричны из-за неодновременных измерений и шумовых эффектов, что ограничивает применение генерации ключей в системах с дуплексным разделением времени (TDD) и медленно затухающих каналах.

Пространственная декорреляция указывает на то, что любой подслушиватель, находящийся на расстоянии более одной полуволны от любого пользователя. Это свойство важно для безопасности систем генерации ключей и утверждается в большинстве работ по генерации ключей. Однако оно может быть выполнено не во всех условиях. Изменчивость канала обусловлена крупномасштабными замираниями (т.е. потерями пути и затенением) и мелкомасштабными замираниями. В модели Джейка с равномерно рассеивающей средой Рэлея и без пути прямой видимости (LoS), если число рассеивателей возрастает до бесконечности, сигнал декоррелирует на расстоянии приблизительно одной полуволны. Однако, когда преобладают крупномасштабные замирания, требуется особое внимание, поскольку канал становится более коррелированным. Существуют исследования, в которых сообщается, что сигналы, наблюдаемые подслушивающими, коррелируют с сигналами легитимных пользователей, что делает системы генерации ключей уязвимыми и требует особого внимания для борьбы с подслушиванием. В целом, пространственная декорреляция изучена недостаточно полно и заслуживает дополнительных исследований.

Исследуем на основе численного моделирования возможность использования атмосферной турбулентности для генерации криптографического ключа, функционирующего в атмосферной линии связи.

Для оценки количественной степени совпадения сигналов (значений принимаемой мощности) рассчитывается коэффициент корреляции Пирсона K_P:

$$K_P = \frac{\sum\left(P_0 - \langle P_0\rangle\right)\left(P_Z - \langle P_Z\rangle\right)}{\sqrt{\sum\left(P_0 - \langle P_0\rangle\right)^2 \sum\left(P_Z - \langle P_Z\rangle\right)^2}}. \quad (1)$$

Где P_0, P_Z – значения мощностей падающих на апертуры оптических систем (PIB - power-in-the-bucket), расположенных в сопряженных плоскостях $z = 0$ (P_0 = PIB0) и $z = Z$ (P_Z = PIBZ). Суммирование в (1) и вычисление средних, обозначенных угловыми скобками, рассчитывалось на основе выполненных отсчетов P_0, P_Z , число которых обозначим как N. Наряду с (1), будем использовать и такую величину, как коэффициент декорреляции P_0, и P_Z

$$\Delta = \left(1 - K_P\right)\cdot 100\%. \quad (2)$$

Условия турбулентности на трассе характеризуется безразмерным параметром $D_0 = d_0/r_0$, где r_0 – радиус Фрида

$$r_0 = 1.68\left(k^2 z C_n^2\right)^{-3/5}.$$

Здесь C_n^2 – структурная характеристика показателя преломления, d_0 – диаметр апертуры.

2.1. Численное моделирование (z = 100 - 7000 м)

На рисунке 1 представлена принципиальная схема работы системы беспроводной оптической связи через турбулентную атмосферу. Будем предполагаем, что размеры апертур на обеих сторонах линии связи одинаковы [24].

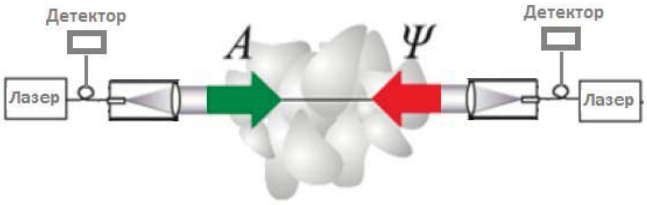

Рис. 1. Принципиальная схема работы систем беспроводной оптической связи через турбулентную атмосферу

2.2. Численное моделирование

Расчеты выполнялись для широкого диапазона изменения параметров приемо-передающей системы и турбулентных условий. Дистанцию z меняли в диапазоне от 100 м до 7000 м. Диаметр приемо-передающих апертур d_0 изменялся в диапазоне от 5 мм до 35 мм. Значение параметра C_n^2 изменялось в диапазоне от $5{,}0\cdot10^{-17}$ м$^{-2/3}$ до $5{,}0\cdot10^{-13}$ м$^{-2/3}$. Параметром, характеризующим степень приближения апертуры к точечному источнику (приемнику), является параметр дифракции $\Omega = \frac{kd_0^2}{8L}$, ($k$ – волновое число) [24]. На рисунке 2 представлена зависимость декорреляции Δ от параметра r_0 для различных значений параметра дифракции Ω.

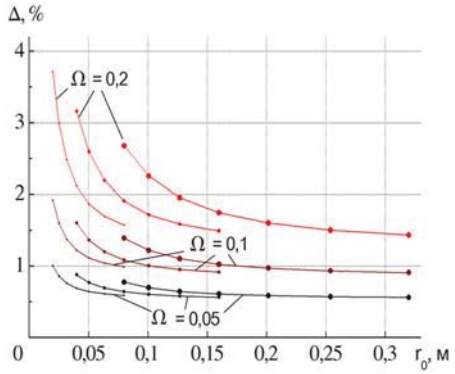

Рис. 2. Зависимость коэффициента декорреляции Δ от параметра r_0 для различных Ω

Уточним, что в данной работе число отсчетов *N*, с помощью которых вычислялся коэффициент корреляции Пирсона, достигало 5 000.

Степень корреляции сигнала может быть увеличена за счет уменьшения дифракционных параметров, т.е. диаметра приемной апертуры. Результаты расчетов на рисунке 3 показывают значительное уменьшение степени декорреляции сигналов с уменьшением параметра дифракции. Чем больше дистанция *z*, тем ниже коэффициент декорреляции при фиксированном параметре дифракции. Степень декорреляции увеличивается с усилением турбулентных флуктуаций показателя преломления. Коэффициент декорреляции $\Delta < 1\%$ при $\Omega < 0{,}05$ во всем рассматриваемом диапазоне параметров.

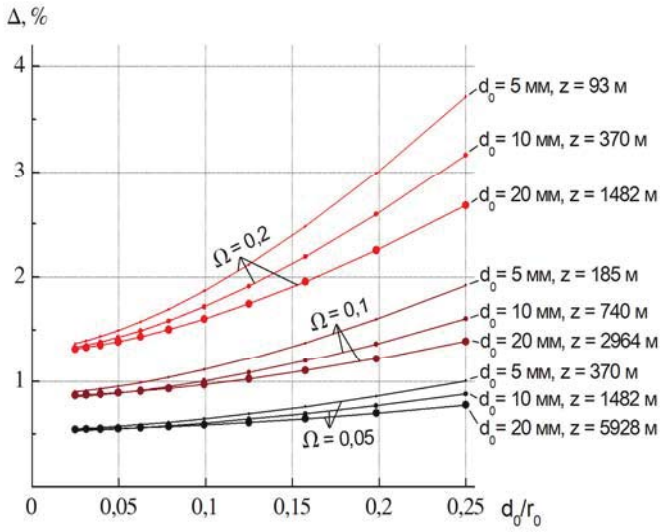

Рис. 3. Зависимость коэффициента декорреляции Δ от параметра d_0/r_0 для различных Ω; значения пар (d_0, *z*) указаны справа от кривых

На рисунке 4 представлено сравнение строгих расчетных данных приведенных на рисунке 3 с результатами приближенной аналитической зависимости Δ от параметров трассы и турбулентных условий среды.

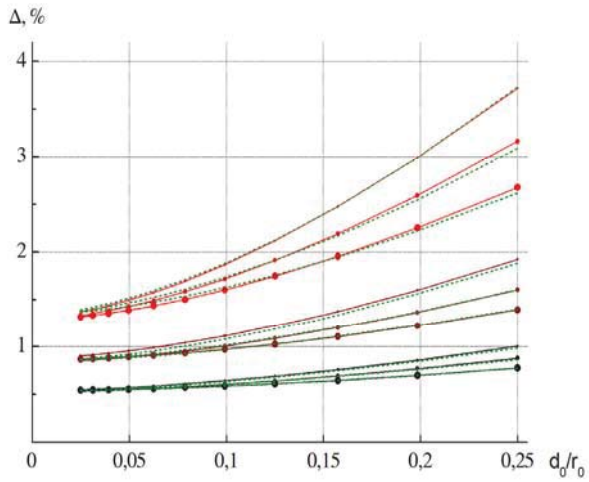

Рис. 4. Расчетные зависимости коэффициента декорреляции от параметров трассы и среды (сплошные линии). Аппроксимация результатов (штриховые линии): $\Delta \approx 3.9\,\Omega^{2/3} + 14\,\Omega^{6/5}\,(1\text{ м}/\,d_0)^{9/20}\,(d_0/r_0)^{8/5}$

На рисунке 5 представлена зависимость коэффициента декорреляции от числа отсчетов.

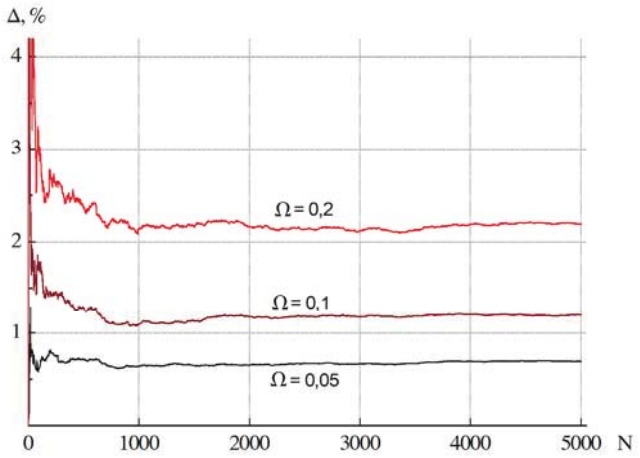

Рис. 5. Зависимость коэффициента декорреляции от числа отсчетов

Итак, нами получено, что уровень декорреляции $\Delta < 1\%$ для $\Omega<0.05$ достигается во всем диапазоне параметров.

Оказывается [11], что доля мощности, перехватываемой приёмной апертурой, определяется дифракционным параметром Ω и не зависит от дистанции *z*.

Мощность растет с увеличением Ω и наоборот, при $\Omega = 0.1$ уменьшается квадратично с уменьшением Ω; она составляет около 2% при $\Omega = 0{,}15$. В свою очередь, увеличение мощности сопровождается уменьшением степени корреляции сигналов.

На рисунке 6 показана относительная дисперсия случайного (турбулентного) сигнала, для различных Ω.

Дисперсия полезного сигнала, очевидно, быстро уменьшается по мере ослабления турбулентности. Дисперсия выше при меньших значениях дифракционного параметра. Уменьшение дисперсии с увеличением Ω вызвано эффектом усреднения апертурой флуктуирующего полезного сигнала [25].

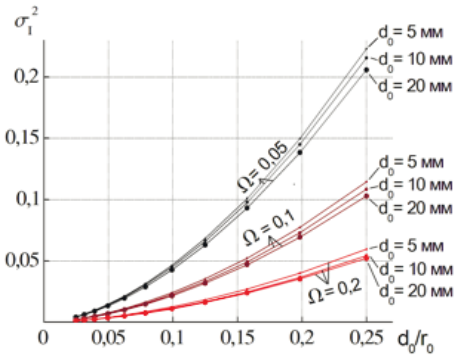

Рис. 6. Относительная дисперсия случайного (турбулентного) сигнала как функция D_0 для различных Ω; диаметры апертуры обозначены справа от кривых

2.2. Лабораторный эксперимент (z = 8 - 35 м)

Для определения криптографического ключа, создаваемого случайными процессами в атмосфере, в лабораторных условиях использовалась схема эксперимента, приведенная на рисунке 7.

В схеме используются два приемо-передающих канала и один чисто приемный канал, так называемого «наблюдателя».

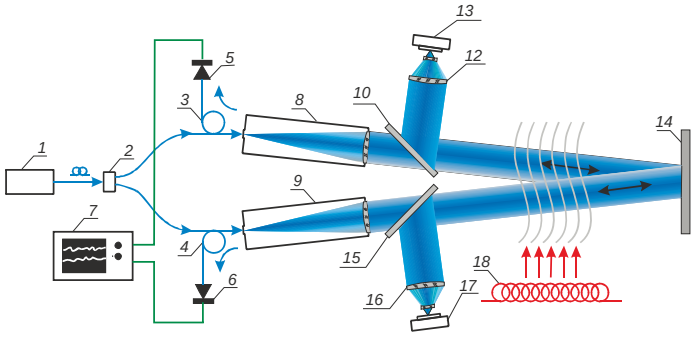

Рис. 7. Схема экспериментальной установки:
1 – одномодовый лазер; 2 – волоконный разветвитель; 3 и 4 – волоконные циркуляторы; 5 и 6 фотодетекторы; 7 – осциллограф; 8 и 9 – коллиматоры (f = 6.12 mm, d_0 = 1.3 mm); 10 и 15 светоделительные пластины; 12 и 16 обратные коллиматоры; 13 – измеритель пространственных характеристик пучка; 14 – плоское зеркало; 17 – датчик Шака-Гартмана; 18 – нагреватель

Экспериментальная установка, показанная на рисунке 7, была использована для анализа атмосферных параметров канала и оптического излучения.

Одномодовый полупроводниковый лазер 1 с распределенными решетками Брэгга и волоконным выходом использовался в качестве источника линейно поляризованного излучения с центральной длиной волны λ = 1064 нм и выходной мощностью 150 мВт. Лазерное излучение было разделено на два канала равные по мощности с помощью волоконного разветвителя (муфты) 2. Волоконно-оптические циркуляторы 3 и 4 были установлены в каждом канале. Циркуляторы подключены к волоконно-оптическим коллиматорам 8 и 9, которые использовались для передачи излучения и приема. Полученное излучение регистрировалось фотодетекторами 5 и 6. Коллиматоры 8 и 9 были одинаковыми, фокусное расстояние которых составляло 6,12 мм; они формировали гауссовы пучки излучения с выходными диаметрами 1,33 мм при уровне интенсивности e^{-2} и расходимости близкой к дифракционному порогу.

Коллимированное излучение распространялось на заданное (переменное) расстояние, отражалось от плоского зеркала 14 и частично (из-за большой расходимости) попадало на приемную апертуру коллиматора 9, затем направлялось циркулятором 4 на фотодетектор 6. В свою очередь, выходное волокно циркулятора 4 было подключено к коллиматору 9, после чего коллимированное излучение распространялось на такое же (переменное) расстояние, отражалось от плоского зеркала 14, частично попадало на приемную апертуру коллиматора 8, а затем направлялось циркулятором 3 к фотодетектору 5. Сигналы с фотодетекторов регистрировались с помощью двухлучевого осциллографа 7.

Часть излучения отводилась из каждого канала с помощью светоделительных пластин 10 и 15, а затем, с помощью обратных коллиматоров 12 и 16, которые в четыре раза сжимали пучки, подавалась на пространственный измеритель пространственных характеристик пучка 13, установленный в одном из каналов, или на датчик Шака-Гартмана 17, установленный в другом канале.

Трассы длиной z = 7, 14, 23 и 35 м были реализованы в эксперименте. Протяженный (длиной 1 м) нагреватель 18 был установлен на дистанции распространения. Температура нагревателя менялась под действием напряжения. Форма сигнала показана на рисунке 8 в зависимости от напряжения.

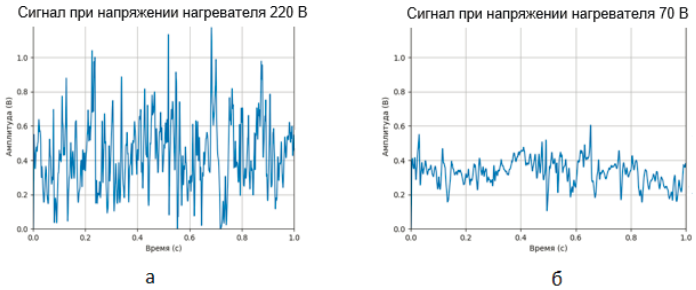

Рис. 8. Развертка сигнала для напряжения нагревателя U, равного (а) 220 и (б) 70 В

Сравнение сигналов до и после фильтрации можно выполнить, исходя из рисунке 9.

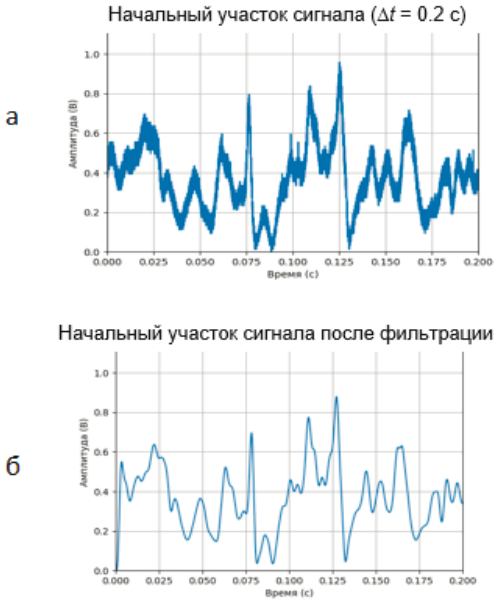

Рис. 9. Начальный участок (Δt = 0,2 с) сигнала (а) до фильтрации с частотой среза 300 Гц и (б) после фильтрации

На рисунке 10 представлена экспериментальная зависимость коэффициента декорреляции, которая составляет около 1% для дифракционного параметра Ω ≅ 0,1.

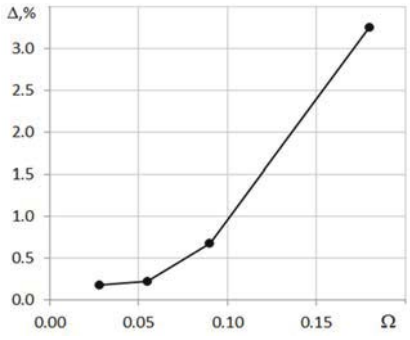

Рис. 10. Экспериментальная зависимость коэффициента декорреляции Δ от дифракционного параметра Ω (z = 7, 14, 23 и 35 м)

Соответствующее цифровое преобразование флуктуирующих из-за атмосферной турбулентности мощности световых пучков, перехваченных направленными навстречу приемными апертурами [26], позволяет сделать вывод, что атмосферная турбулентность может быть использована для генерации криптографического ключей.

Заключение и перспективы работы

Генерация ключей на основе случайности каналов беспроводной связи является многообещающим методом безопасного обмена криптографическими ключами между законными пользователями. Его относительно легко реализовать с помощью готовых беспроводных сетевых адаптеров, и он может обеспечить теоретико-информационную безопасность.

Работа посвящена решению проблемы распределения криптографических ключей на основе стохастических свойств физических процессов.

В первой части работы выполнен краткий обзор способов формирования ключа на принципах квантовой физики. Определены достоинства и проблемы использования квантовых систем в качестве носителей информации, выявленные к настоящему времени.

Вторая часть работы посвящена исследованию возможности использования для генерации ключей флуктуаций принимаемой мощности излучения, вызванных атмосферной турбулентностью. В ней выполнено численное и экспериментальное моделирование процесса распространения волн в системе двух сопряженных приемо-передатчиков, функционирующих в турбулентной среде (атмосфере). Для этого созданы соответствующие алгоритмы численного моделирования характеристик оптических полей, искаженных атмосферным каналом распространения.

На основе численного моделирования установлены зависимости коэффициента корреляции встречных сигналов от геометрических параметров системы и турбулентных условий на трассе для широкого диапазона изменения дистанций (100-7000 м), радиусов апертур (5-35 мм), значения структурной постоянной показателя преломления C_n^2 ($5.0 \cdot 10^{-17}$ м$^{-2/3}$ - $5.0 \cdot 10^{-13}$ м$^{-2/3}$). Установлено, что для дифракционного параметра $\Omega < 0.05$ достигается уровень корреляции сигналов > 99% во всем диапазоне исследуемых параметров. Данный результат хорошо согласуется с результатами лабораторного эксперимента.

Результаты работы позволяют сделать вывод о том, что использование в качестве генератора случайного сигнала атмосферной турбулентности, позволяет сформировать практически идентичный криптографический ключ в двух направленных друг на друга каналах связи.

В настоящее время ООО «Цифровые лазерные системы» разрабатывает коммерческую версию приемо-передающей системы для формирования криптографического ключа, генерируемого турбулентностью атмосферы на дистанциях более 3,5 км. Дизайн-проект приемо-передающего модуля представлен на рисунке 11.

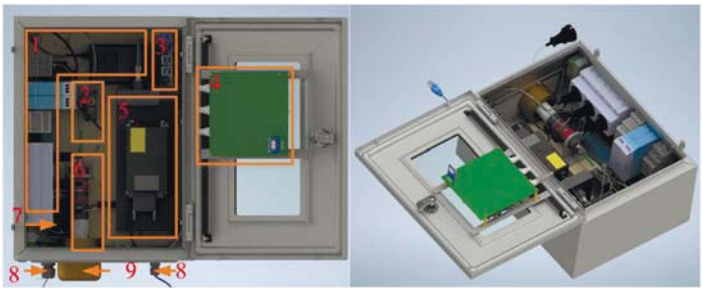

Рис. 11. Дизайн-проект приемо-передающего модуля: 1 – источники питания элементов установки; 2 – фотоприемник со встроенной диафрагмой; 3 – микроЭВМ; 4 – электронный модуль; 5 – лазерный источник; 6 – оптическая система; 7 – оптический циркулятор; 8 – сальник; 9 – кабельный ввод

Литература

1. *Majumdar K.* Advanced Free Space Optics (FSO). New York: Springer, 2015. 397 P, 1-4.
2. *Fürst H., Weier H., Nauerth S., Marangon D.G., Kurtsiefer C. and Weinfurter H.* High speed optical quantum random number generation. Optics express, 2010, 18(12), pp. 13029-13037.
3. *Fiorentino M., Santori C., Spillane S.M., Beausoleil R.G., and Munro W.J.* Secure self-calibrating quantum random-bit generator // Physical Review A, 2007, 75 (3), 032334.
4. *Gabriel C., Wittmann C., Sych D., Dong R., Mauerer W., Andersen U.L., Marquardt C., Leuchs G.* A generator for unique quantum random numbers based on vacuum states // Nature Photonics. 2010. Vol. 4. № 10. P. 711-715.
5. *Bennett C.H. and Brassard G.* Quantum cryptography: Public key distribution and coin tossing // Theoretical Computer Science, Vol. 560 (Part 1), 2014, pp. 7-11.
6. Sidorov V.V., Karpov A.V., and Sulimov A.I. Meteor generation of secret encryption keys for protection of open communication channels // Inform. Tekhnol. Vychislitel'nye Sist., 2008, № 3, pp. 45-54.
7. *Sulimov A.I., Galiev A.A., Karpov A.V., and Markelov V.V.* Verification of wireless key generation using software defined radio // in Proc. Intern. Siberian Conf. on Control and Commun. (SIBCON). Tomsk, Russia (2019), p. 1-6. https://doi.org/10.1109/SIBCON.2019.8729607
8. *Sulimov A.I. and Karpov A.V.* Performance evaluation of meteor key distribution // in Proc. the 12th Intern. Conf. on Security and Cryptography (SECRYPT-2015), Colmar, France (2015), pp. 392-397.
9. *Premnath S.N., Jana S., Croft J., Gowda P.L., Clark M., Kasera S.K., Patwari N., and Krishnamurthy S.V.* Secret key extraction from wireless signal strength in real environments // IEEE Trans. Mobile Comput., 2013, 12 (5), pp. 917-930.
10. *Wallace J.W. and Sharma R.K.* Automatic secret keys from reciprocal MIMO wireless channels: surement and Analysis // IEEE Trans. Inf. Forensics Security, 2010, № 5 (3), pp. 381-392.
11. *Аксенов В.П., Дудоров В.В., Колосов В.В., Погуца Ч.Е., Левицкий М.Е.* Анализ корреляции интенсивности в приемо-передающих лазерных системах для формирования криптографического ключа // Оптика Атмосферы И Океана. 2020. №8. С.591-597.
12. *Minet J., Vorontsov M.A., Polnau E., and Dolfi D.* Enhanced correlation of received power-signal fluctuations in bidirectional optical links // J. Opt. 15 (2), 022401 (2013).
13. *Drake M.D., Bas C.F., Gervais D.R., Renda P.F., Townsend D., Rushanan J.J., Francoeur J., Donnangelo N.C., and Stenner M.D.* Optical key distribution system using atmospheric turbulence as the randomness generating function: Classical optical protocol for information assurance // Opt. Eng. 52 (5), 055008 (2013).

14. *Wang N., Song X., Cheng J., and Leung V.C.* Enhancing the security of free-space optical communications with secret sharing and key agreement // J. Opt. Commun. Netw., 2014, № 6 (12), pp. 1072-1081.

15. *Shapiro J.H. and Puryear A.L.* Reciprocity-enhanced optical communication through atmospheric turbulence – Part I: Reciprocity proofs and far-field power transfer optimization // J. Opt. Commun. Netw., 2012, № 4 (12), pp. 947-954.

16. *Bornman N., Forbes A., and Kempf A.* Random number generation & distribution out of thin (or thick) air // J. Opt. 22 (7), 2020, 075705.

17. *Актаева А.У., Баймуратов О.А., Галиева Н.Г., Байкенов А.С.* Безопасность информации: применение квантовых технологий // International Journal of Open Information Technologies, 2016. Vol. 4, № 4. P. 40-48.

18. *Bennett C., Brassard G.* Quantum Cryptography: Public key distribution and coin tossing // Proceedings IEEE International Conference on Computers, Systems and Signal Processing. Bangalore.1984. IEEE.1984. P. 175.

19. *Bennet C.* Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. 1992. Vol. 68, pp. 3121-3124.

20. *Ekert A.* Quantum cryptography based on Bell's theorem// Phys. Rev. Lett. 1991. Vol. 67, pp. 661-663.

21. *Barbosa G., Corndorf E., Kumar P., Yuen H.* Quantum cryptography in free space with coherent-state light // Proc. SPIE 4821.2002, pp. 409-420.

22. *Ling A., Peloso M., Marcikic I., Lamas-Linares A., Kurtsiefer C.* Experimental E91 quantum key distribution // Proc. SPIE 6903. 2008. 69030-U.

23. *Дудоров В.В., Колосов В.В.* Анализ корреляции переданного и принятого сигналов для системы беспроводной оптической связи // Синергия наук, 2018. №28. С. 1319-1327.

24. *Дудоров В.В., Колосов В.В., Филимонов Г.А.* Алгоритм формирования бесконечных турбулентных экранов для моделирования долговременных лазерных экспериментов в атмосфере // Известия Томского политехнического университета. Инжиниринг георесурсов. 2006. Т. 309. № 8. С. 85-89.

25. *Kolosov, V.V., Dudorov, V.V., Filimonov, G.A., Panina, A.S., Vorontsov, M.A.* Accounting for the effect of large-scale atmospheric inhomogeneities in problems of laser radiation propagation along long high-altitude paths // Atmos Ocean Opt. 2014. Vol. 27. № 2, pp. 123-129.

26. *Адамов Е.В., Колосов В.В., Левицкий М.Е.* Система обработки данных формирования криптографического ключа для беспроводной системы оптической связи // Наука. Технологии. Инновации. сборник научных трудов: в 9 ч. Новосибирск, 2020. С. 3-7.

CRYPTOGRAPHIC KEY FORMATION IN COUPLED TRANSMIT-RECEIVING ATMOSPHERIC LASER SYSTEMS

Evgenia S. Abramova, *Siberian state University of telecommunications and Informatics, Novosibirsk, Russia,* ***evgenka_252@mail.ru***

Egor V. Adamov, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Tomsk, Russia,* ***adamov@iao.ru***

Valerii P. Aksenov, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Tomsk, Russia,* ***avp@iao.ru***

Egor A. Bogach, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Tomsk, Russia,* ***bogach@iao.ru***

Vadim V. Dudorov, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Tomsk, Russia,* ***dvv@iao.ru***

Valeriy V. Kolosov, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Tomsk, Russia,* ***kvv@iao.ru***

Mikhail E. Levitsky, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Tomsk, Russia,* ***top@iao.ru***

Cheslav E. Pogutsa, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Tomsk, Russia,* ***pce@iao.ru***

Ivan I. Pavlov, *Siberian state University of telecommunications and Informatics, Novosibirsk, Russia,* ***iipavlov02@mail.ru***

Abstract

The security of transmission and retrieval depends on the encryption of information sent over public networks. At present, approaches to data protection based on cryptography methods using one-way mathematical functions are widely used. Symmetric and asymmetric methods of key transmission over open communication channels have been developed. The stability of information protection methods using one-way mathematical functions is based on the algorithmic complexity of their hacking for modern computers. The emergence of quantum computers of sufficient power will radically change the situation. Therefore, at present, the question of developing methods for distributing cryptographic keys based on new principles is acute. Such methods include quantum cryptography and cryptography based on stochastic physical processes. In this work, a brief review of the key generation methods based on the principles of quantum physics is carried out, and then the possibility of using fluctuations of the received radiation power caused by atmospheric turbulence to generate keys is investigated. Numerical and experimental modeling of the process of wave propagation in a system of two coupled transceivers operating in a turbulent medium (atmosphere) has been performed. For this purpose, appropriate algorithms for numerical simulation of the characteristics of optical fields distorted by the atmospheric propagation channel have been developed. An experimental setup has been developed and a model experimental study of the formation of correlated random signals in transmit-receive laser systems has been carried out. The need to use low-frequency filtering of the received signals was found. The efficiency of this filtration has been studied. The results of the work allow us to conclude that the use of atmospheric turbulence as a random signal generator makes it possible to form an almost identical cryptographic key in two communication channels directed towards each other.

Keywords: *laser radiation, confidential optical communication, cryptography, atmospheric turbulence, intensity fluctuations, reciprocity theorem.*

References

1. Majumdar K. (2015) Advanced Free Space Optics (FSO). New York: Springer, 397 p.
2. Furst H., Weier H., Nauerth S., Marangon D.G., Kurtsiefer C. and Weinfurter H. (2010) High speed optical quantum random number generation. *Optics express*, no. 18(12), pp. 13029-13037.
3. M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro (2007) Secure self-calibrating quantum random-bit generator. *Physical Review* A, 75 (3), 032334.
4. Gabriel C., Wittmann C., Sych D., Dong R., Mauerer W., Andersen U.L., Marquardt C., Leuchs G. (2010) A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*. Vol. 4. No. 10, pp. 711-715.
5. C. H. Bennett and G. Brassard (2014) Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, Vol. 560 (Part 1), pp. 7-11.
6. V. V. Sidorov, A. V. Karpov, and A. I. Sulimov (2008) Meteor generation of secret encryption keys for protection of open communication channels. *Inform. Tekhnol. Vychislitel'nye Sist.*, No. 3, pp. 45-54.
7. A. I. Sulimov, A. A. Galiev, A. V. Karpov, and V. V. Markelov (2019) Verification of wireless key generation using software defined radio. *Proc. Intern. Siberian Conf. on Control and Commun. (SIBCON)*. Tomsk, Russia, p. 1-6. https://doi.org/10.1109/SIBCON.2019.8729607
8. A. I. Sulimov and A. V. Karpov (2015) Performance evaluation of meteor key distribution. *Proc. the 12th Intern. Conf. on Security and Cryptography (SECRYPT-2015),* Colmar, France, pp. 392-397.
9. S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy (2013) Secret key extraction from wireless signal strength in real environments. *IEEE Trans. Mobile Comput*. 12 (5), pp. 917-930.
10. J. W. Wallace and R. K. Sharma (2010) Automatic secret keys from reciprocal MIMO wireless channels: surement and Analysis. *IEEE Trans. Inf. Forensics Security,* no. 5 (3), pp. 381-392.
11. V. P. Aksenov, V. V. Dudorov, V.V. Kolosov, Ch.E. Pogutsa, M.E. Levitsky (2020) Analysis of the intensity correlation in transmitting and receiving laser systems for the formation of a cryptographic key. *Optics of the Atmosphere and Ocean*. No, 8. pp. 591-597.
12. J. Minet, M. A. Vorontsov, E. Polnau, and D. Dolfi (2013) Enhanced correlation of received power-signal fluctuations in bidirectional optical links. *J. Opt. no.* 15 (2), 022401.
13. M. D. Drake, C. F. Bas, D. R. Gervais, P. F. Renda, D. Townsend, J. J. Rushanan, J. Francoeur, N. C. Donnangelo, and M. D. Stenner (2013) Optical key distribution system using atmospheric turbulence as the randomness generating function: Classical optical protocol for information assurance. *Opt. Eng*. no. 52 (5), 055008.
14. N. Wang, X. Song, J. Cheng, and V. C. Leung (2014) Enhancing the security of free-space optical communications with secret sharing and key agreement. *J. Opt. Commun. Netw*. no. 6 (12), pp. 1072-1081.
15. J. H. Shapiro and A. L. Puryear (2012) Reciprocity-enhanced optical communication through atmospheric turbulence-Part I: Reciprocity proofs and far-field power transfer optimization. *J. Opt. Commun. Netw*. no. 4 (12), pp. 947-954.
16. N. Bornman, A. Forbes, and A. Kempf (2020) Random number generation & distribution out of thin (or thick) air. *J. Opt*. no. 22 (7), 075705.
17. Aktaeva A.U., Baimuratov O.A., Galieva N.G., Baikenov A.S. (2016) Information security: application of quantum technologies. *International Journal of Open Information Technologies*. Vol. 4, no. 4, pp. 40-48.
18. Bennett C., Brassard G. Quantum Cryptography: Public key distribution and coin tossing. *Proceedings IEEE International Conference on Computers, Systems and Signal Processing. Bangalore*.IEEE.1984. P. 175.
19. Bennet C. (1992) Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett*. Vol. 68, pp. 3121-3124.
20. Ekert A. (1991) Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett*. Vol. 67, pp. 661-663.
21. Barbosa G., Corndorf E., Kumar P., Yuen H. (2002) Quantum cryptography in free space with coherent- state light. *Proc. SPIE 4821*, pp. 409-420.
22. Ling A., Peloso M., Marcikic I., Lamas-Linares A., Kurtsiefer C. (2008) Experimental E91 quantum key distribution. *Proc. SPIE 6903*. 69030-U.
23. Dudorov V.V., Kolosov V.V. (2018) Analysis of the correlation of transmitted and received signals for a wireless optical communication system. *Synergy of Sciences*, no. 28, pp. 1319-1327.
24. Dudorov V.V., Kolosov V.V., Filimonov G.A. (2006) Algorithm for the formation of infinite turbulent screens for modeling long-term laser experiments in the atmosphere. Bulletin of the Tomsk Polytechnic University. *Engineering of georesources*. Vol. 309. No. 8, pp. 85-89.
25. Kolosov V.V., Dudorov V.V., Filimonov G.A., Panina A.S., Vorontsov M.A. (2014) Accounting for the effect of large-scale atmospheric inhomogeneities in problems of laser radiation propagation along long high-altitude paths. *Atmos Ocean Opt*. Vol. 27. No. 2, pp. 123-129.
26. Adamov E.V., Kolosov V.V., Levitsky M.E. (2020) Data processing system for generating a cryptographic key for a wireless optical communication system. *Nauka. Technology*. Innovation. collection of scientific papers: in 9 parts. Novosibirsk, pp. 3-7.

Information about authors:

Evgenia S. Abramova, *Siberian state University of telecommunications and Informatics, associate Professor of Department of Radio Engineering Devices and Technosphere Safety, Associate Professor, Candidate of technical sciences, Novosibirsk, Russia*

Egor V. Adamov, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, PhD student, Tomsk, Russia*

Valerii P. Aksenov, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Chief Researcher, Doktor of physico-mathematical sciences, Tomsk, Russia*

Egor A. Bogach, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, PhD student, Tomsk, Russia*

Vadim V. Dudorov, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Chief Researcher, Doktor of physico-mathematical sciences, Tomsk, Russia*

Valeriy V. Kolosov, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Chief Researcher, Doktor of physico-mathematical sciences, Tomsk, Russia*

Mikhail E. Levitsky, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Senior Researcher, Tomsk, Russia*

Cheslav E. Pogutsa, *Laboratory of Optical Location V.E. Zuev Institute of Atmospheric Optics SB RAS, Researcher, Candidate of physico-mathematical sciences, Tomsk, Russia*

Ivan I. Pavlov, *Siberian state University of telecommunications and Informatics, associate Professor of Department of Radio Engineering Devices and Technosphere Safety, Associate Professor, Candidate of technical sciences, Novosibirsk, Russia*