

ПРОТОКОЛ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА АКСИАЛЬНО-СИММЕТРИЧНЫХ ПОЛЯРИЗАЦИОННЫХ ПУЧКАХ В АТМОСФЕРНОМ КАНАЛЕ

Д. Д. Решетников¹, А. Л. Соколов², Е. А. Вашукевич¹, В. М. Петров¹, Т. Ю. Голубева¹
¹ Санкт-Петербургский государственный университет, 199034 Санкт-Петербург, Россия
² Национальный исследовательский университет «МЭИ», 11250 Москва, Россия

Аннотация

В работе предлагается протокол квантового распределения ключа с использованием аксиально-симметричных поляризационных пучков, инвариантных к вращению радиальной координаты в плоскости, нормальной к оси распространения пучка. Приводится описание и способ генерации векторных пучков с аксиально-симметричной поляризационной структурой, образованных векторной суперпозицией мод Эрмита-Гаусса с индексами 10 и 01. Показано, что аксиальная поляризационная симметрия делает такие пучки не чувствительными к поворотам относительно оптической оси, что дает возможность использовать их для передачи информации в криптографических протоколах в системах космической связи. Подробно показан механизм формирования мод с использованием радиальных поляризаторов и уголкового отражателя. Хотя классический канал связи может быть организован с использованием радиальных поляризаторов, включение неунитарных элементов в квантовый канал связи разрушает его криптостойкость. Исходя из этого мы рассматриваем процедуру детектирования фазовых сдвигов в конфигурации интерферометра Маха-Цандера, элементами которого служат уголкового отражатели.

Ключевые слова

Квантовая криптография, поляризационный протокол, аксиально-симметричная поляризационная структура, радиальный поляризатор, векторное поле, уголкового отражатель.

ВВЕДЕНИЕ

Развитие систем квантовой криптографии [1–3] обусловлено необходимостью защиты информации в современных коммуникационных сетях. Использование различных типов пространственно-структурированных пучков может быть одним из эффективных решений задачи по оптической передаче информации в реальных условиях турбулентности среды как по классическим, так и по квантовым каналам связи.

На сегодняшний день поиск устойчивых каналов передачи информации в свободном пространстве ведется как в теоретическом, так и в экспериментальном русле. Так, например, исследовано влияние турбулентности атмосферного канала на распространение векторных пучков Лагерра-Гаусса и Бесселя-Гаусса и на пропускную способность канала [4, 5], продемонстрирована передача высших мод пучков Лагерра-Гаусса в реальных условиях городской турбулентности на расстоянии 1.6 км с использованием длины волны 809 нм [6], экспериментально продемонстрирована скорость распределения ключа со скоростью не менее 120 Мбит/с с использованием мультиплексирования по орбитальному угловому моменту, спектрального и поляризационного мультиплексирования на длине волны 1550.12 нм (193.4 ТГц) [7]. В работе [7] имитация турбулентности атмосферы осуществлялась при помощи двух двумерных фазовых модуляторов света, обеспечивающих на трассе длиной 2.6 км турбулентность, соответствующую величине параметра Рытова $\delta_R^2 = 0.2$. Наряду с этим, вихревые поля используют и для волоконной связи. Так в работе [8] экспериментально продемонстрирована квантовое распределение ключа через вихревое оптическое волокно длиной 60 м. В этом случае использовалась пара запутанных фотонов, получаемых в результате процесса спонтанного параметрического рассеяния на длине волны 405 нм. Активно ведутся работы по исследованию распространения Гауссовых и вихревых пучков в условиях атмосферной турбулентности на значительные расстояния, до 1000 м [9].

Особое место занимают задачи передачи информации на расстояния более тысячи километров с помощью низкоорбитальных космических аппаратов, оснащенных соответствующим оборудованием [10–13]. Если ещё в 2017 году, в работе [11] сообщалось о достигнутой скорости передачи ключа в «несколько килогерц» на спутник, находящийся на расстоянии 1200 км от Земли, то в 2021 году уже сообщалось об «интегрированной волоконно-оптической и спутниковой сети» общей протяженностью 4600 км и скоростью передачи секретного ключа на спутник со скоростью 47.8 кБит/с [12]. Отметим, что возможность использования в космических системах пучков с аксиально-симметричной поляризационной структурой, т. е. обладающих пространственной модуляцией поляризации в плоскости, ортогональной направлению распространения, в качестве базисных пучков, формирующих поляризационный криптографический ключ показана в работе [13].

Базовый для квантовой криптографии протокол квантового распределения ключа (КРК) BB84 использует два базиса однофотонных квантовых состояний с линейной поляризацией. В первом базисе фотон линейно поляризован вертикально или горизонтально (0° или 90°), во втором – фотон линейно поляризован диагонально или антидиагонально (45° или 135°).

Важно отметить, что применение протокола BB84 с использованием базисов, основанных на линейной поляризации фотонов, для задач КРК для низкоорбитальных космических аппаратов значительно затруднено в связи с необходимостью в каждый момент времени фиксировать положение плоскости поляризации света как передающей, так и приемной системами на земле и в космосе. Анализ показывает, что в передающих оптико-лазерных системах состояние поляризации существенно изменяется для различных точек полусферы [14]. В случае поляризационного протокола это означает зависимость двух развернутых на 45° базисов от взаимной ориентации передающего телескопа и космического аппарата (см. рис.1).

Данную зависимость можно устранить, если использовать аксиально-симметричные пучки. В [15] в качестве возможной модификации протокола КРК рассматривается использование мод с орбитальным угловым моментом. Однако управление генерацией и детектированием таких мод осуществляется использованием пространственно-неоднородных двулучепреломляющих пластин с топологическим зарядом (q-plate) [16, 17] или фазовых масок [18]. Такое управление существенно уменьшает скорость генерации квантового ключа, так что техника использования таких мод не может конкурировать с поляризационным кодированием.

Мы предлагаем использовать для квантового кодирования пучки с аксиально-симметричной поляризационной структурой [19–21]. В существующих протоколах квантовой криптографии с использованием мод с топологическим зарядом (орбитальным угловым моментом), векторные свойства поля не задействованы для кодирования информации. В этой работе мы хотя и будем оперировать пучками с топологическим зарядом, не используем его для кодирования. Мы предлагаем использовать векторные пучки, обладающие не только топологическим зарядом, но и пространственно неоднородным состоянием поляризации. Именно поляризационная степень свободы этих пучков будет использоваться нами как носитель информации.

Отдельными задачами являются как получение пучков с заданной аксиальной поляризационной структурой, так и их детектирование. Способы их получения можно разделить на два основных: первый – это внутрирезонаторные методы, когда вместо основной моды лазера генерируются моды первого порядка [22, 23], и внерезонаторные методы с помощью дифракционных оптических элементов [24]. В [25] было показано, что пучки второго порядка образуются при отражении линейно поляризованного пучка от уголкового отражателя [26], в частности, при наличии специального интерференционного покрытия граней, формируется оптический вихрь второго порядка. Использование таких оптических элементов позволяет быстро управлять поляризацией оптических векторных полей, что является ключевым моментом для их применения в криптографических системах.

Задача детектирования пучков в классическом криптографическом канале может быть решена при помощи устройства, выполняющего роль радиального поляризатора [21]. Для квантовых каналов использование поглощающих элементов недопустимо. Исходя из этого мы рассматриваем процедуру детектирования поляризационных степеней свободы в конфигурации интерферометра Маха-Цандера, элементами которого служат уголковые отражатели.

Цель настоящей работы – предложить реализацию криптографического протокола для космической системы передачи квантовой информации на основе векторных полей. Особенностью такой реализации должна быть её инвариантность относительно поворота вокруг оси z , совпадающей с направлением распространения пучка и сохранение скорости генерации ключа на уровне традиционных поляризационных протоколов.

1. ПУЧКИ С АКСИАЛЬНО-СИММЕТРИЧНОЙ ПОЛЯРИЗАЦИОННОЙ СТРУКТУРОЙ

В случае аксиально-симметричной поляризационной структуры, независимо от радиальной координаты в плоскости поперечного сечения пучка, каждому значению азимута соответствует определенная ориентация плоскости колебаний вектора \mathbf{E} , которая изменяется так, что при возвращении к исходному значению азимута эта плоскость совершает целое число оборотов. Поляризационно-симметричные структуры имеют по две модификации, в зависимости от направления поворота плоскости колебаний вектора \mathbf{E} .

Поляризационная структура этих пучков инвариантна к повороту относительно оси пучка: состояние поляризации сохраняется вдоль радиус-вектора r для произвольного азимутального угла φ (Рис. 1).

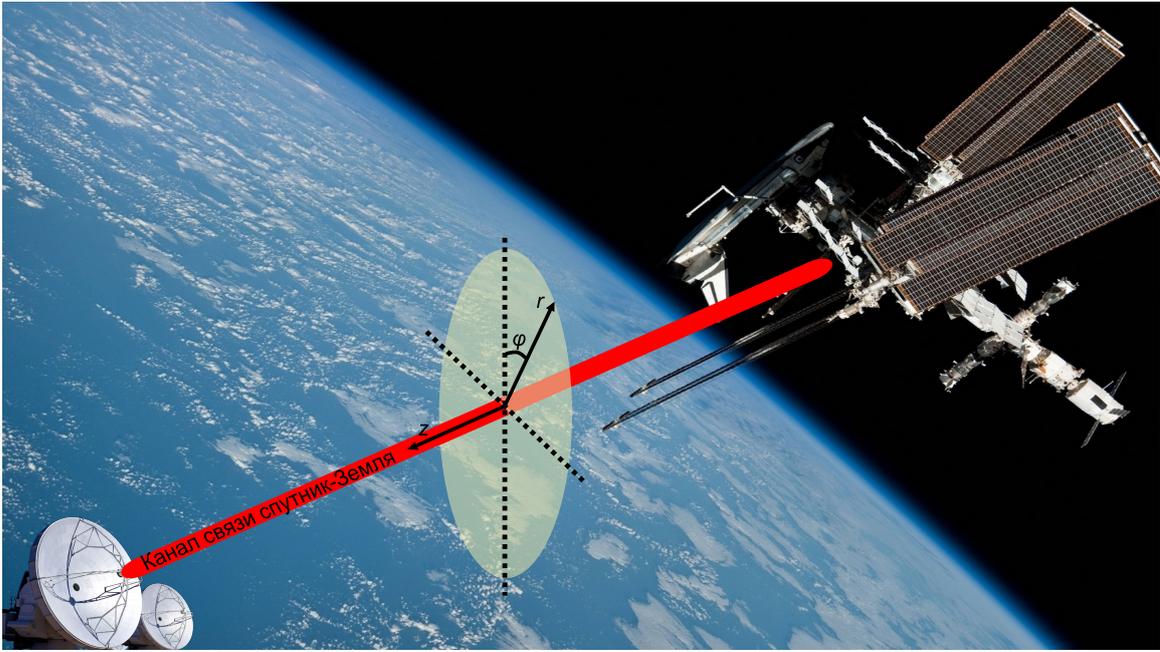


Рис. 1. Геометрия распространения пучков с аксиальной симметрией. φ – угол поворота радиус-вектора r , z – направление распространения.

Прежде чем обсуждать возможность использования аксиально-симметричных векторных полей в протоколе квантового распределения ключа, обсудим подробнее структуру мод, которые мы будем далее рассматривать в качестве базисных.

В табл.1 показано, как формируются аксиально-симметричные структуры, составляющие набор для модифицированного поляризационного протокола.

Отметим, что далее мы будем применять другой, отличный от указанного здесь, механизм формирования этих же мод с помощью уголкового отражателя. Однако приведенное здесь описание, как нам кажется, помогает лучше понять свойства рассматриваемых полей.

Базисными попарно-ортогональными поляризационными структурами предлагаемого поляризационного протокола являются пучки, образованные векторной суперпозицией линейно-поляризованных мод Эрмита-Гаусса с индексами 10 и 01 (табл.1). Это радиальная поляризационная структура – вектор \mathbf{E} в каждой точке поперечной плоскости ориентирован вдоль радиуса (РП-пучок), азимутальная – вектор \mathbf{E} направлен в каждой точке по касательной к концентрическим окружностям (АП-пучок), и две ортогональные поляризационные структуры, обладающие аксиальной симметрией, которые развернуты на 45° относительно РП-пучка и АП-пучка: право-скрученная (право-скрученный пучок - ПСП) и лево-скрученная (лево-скрученный пучок - ЛСП). Векторы Джонса в табл.1 записаны в цилиндрическом базисе, где φ – азимутальный угол.

Взаимодействие базисных пучков с радиальными поляризационными элементами удобно демонстрировать в специальном поляризационном (спиральном) базисе.

II. СПИРАЛЬНЫЕ БАЗИСЫ

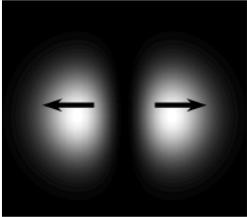
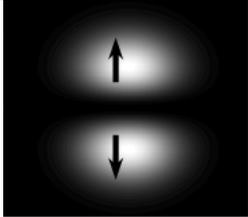
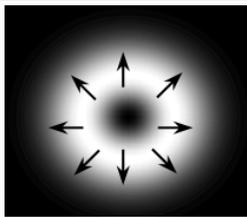
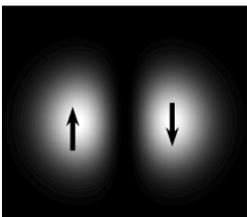
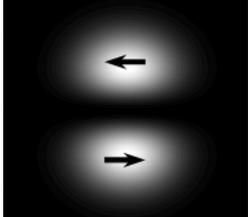
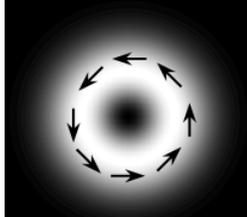
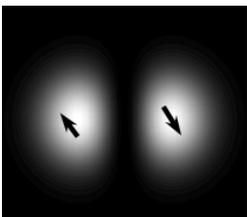
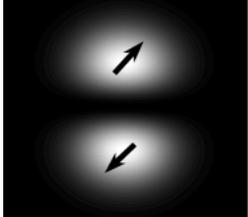
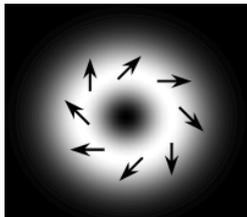
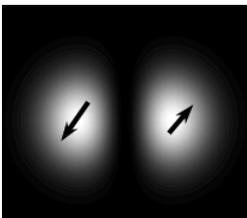
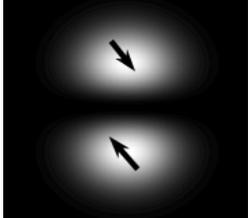
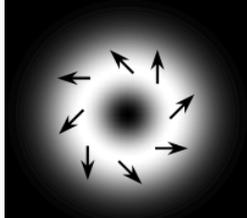
Для удобства математических выкладок используем спиральные базисы, которые задаются с помощью двух матриц [10]:

$$P = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix}, \quad N = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}, \quad (1)$$

где φ – азимутальный угол, отсчитываемый от так называемой нулевой полуоси, в направлении которой матрицы становятся единичными.

Матрица P описывает переход вектора Джонса \mathbf{D} из декартова в спиральный P -базис, где соответствующий вектор Джонса будем обозначать индексом \mathbf{p} , а матрица N – в спиральный N -базис с индексом \mathbf{n} . Если нулевая

Таблица 1. Формирование четырех базисных пучков с помощью мод Эрмита-Гаусса первого порядка: R-пучок (РП-пучок); A-пучок (АП-пучок); LR - ЛСП-пучок; RR - ПСП-пучок

Обозначение	Первая мода	Вторая мода	Совокупность мод	Вектор Джонса
1 РП-пучок				$\mathbf{D}_R = \begin{pmatrix} \cos(\varphi) \\ \sin(\varphi) \end{pmatrix}$
2 АП-пучок				$\mathbf{D}_A = \begin{pmatrix} -\sin(\varphi) \\ \cos(\varphi) \end{pmatrix}$
3 ЛСП-пучок				$\mathbf{D}_{LR} = \begin{pmatrix} -\sin(\varphi + 45^\circ) \\ \cos(\varphi + 45^\circ) \end{pmatrix}$
4 ПСП-пучок				$\mathbf{D}_{RR} = \begin{pmatrix} \cos(\varphi + 45^\circ) \\ \sin(\varphi + 45^\circ) \end{pmatrix}$

полуось согласована с осью X декартова базиса, то имеем

$$\mathbf{D}_p = P\mathbf{D}, \quad \mathbf{D}_n = N\mathbf{D}. \quad (2)$$

Преобразование матрицы Джонса T_d из декартова поляризационного базиса в матрицу T_p в спиральном базисе и обратно осуществляется следующим образом:

$$T_p = PT_dN, \quad T_d = NT_pP. \quad (3)$$

Собственными для спирального базиса являются поляризационные структуры РП-пучка и АП-пучка, у которых вектор \mathbf{E} вращается против часовой стрелки при изменении азимутального угла φ , при этом поляризационная структура не изменяется при поворотах осей координат.

При преобразовании из декартова базиса в спиральный P -базис векторы Джонса данных пучков приобретают

следующий вид:

$$\mathbf{D}_{\mathbf{R}\mathbf{P}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \mathbf{D}_{\mathbf{A}\mathbf{P}} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (4)$$

Для N -базиса собственными являются поляризационные структуры с поворотом плоскости колебаний вектора \mathbf{E} по часовой стрелке. В этом случае поляризационная структура изменяется при повороте декартова базиса.

Векторы Джонса ПСП-пучка и ЛСП-пучка в спиральном базисе имеют вид:

$$\mathbf{D}_{\mathbf{R}\mathbf{R}\mathbf{P}} = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \end{pmatrix}, \quad \mathbf{D}_{\mathbf{L}\mathbf{P}\mathbf{P}} = \frac{\sqrt{2}}{2} \begin{pmatrix} \frac{-\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \end{pmatrix}. \quad (5)$$

III. РАДИАЛЬНЫЙ ПОЛЯРИЗАТОР И УСТРОЙСТВА НА ЕГО ОСНОВЕ

Устройством для распознавания различных векторных базисных состояний, является радиальный поляризатор (РП). Оси пропускания радиального поляризатора направлены вдоль поперечного радиуса $r = \sqrt{x^2 + y^2}$, ($\varphi = const$). В азимутальном направлении, т.е. при ориентации вектора \mathbf{E} по касательным к концентрическим окружностям, пропускание равно нулю. Покажем, как РП может быть получен с помощью обычного линейного поляризатора, расположенного между двух спиральных вращателей [23].

Матрицы Джонса положительного P и отрицательного N спирального вращателя в декартовом базисе имеют вид:

$$P = \begin{pmatrix} \cos(\varphi - \alpha) & \sin(\varphi - \alpha) \\ -\sin(\varphi - \alpha) & \cos(\varphi - \alpha) \end{pmatrix}, \quad N = \begin{pmatrix} \cos(\varphi - \alpha) & -\sin(\varphi - \alpha) \\ \sin(\varphi - \alpha) & \cos(\varphi - \alpha) \end{pmatrix}, \quad (6)$$

где φ – азимутальный угол, отсчитываемый от горизонтальной оси X декартова базиса в поперечном сечении пучка; α – угол, который составляет нулевая полуось спирального вращателя с осью X .

Спиральные вращатели могут быть полярными или неполярными, в зависимости от того, изменяют ли они свой знак для обратной волны.

Пусть нулевая полуось двух спиральных вращателей разного знака совпадает с осью X декартова базиса. Расположим идеальный линейный поляризатор между этими двумя вращателями так, чтобы ось его наибольшего пропускания составляла угол β с осью X . Матрица Джонса данного поляризационно-неоднородного устройства будет иметь следующий вид:

$$\begin{aligned} T_r(\beta) &= \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \begin{pmatrix} \cos(\beta) & -\sin(\beta) \\ \sin(\beta) & \cos(\beta) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \cos(\beta) & \sin(\beta) \\ -\sin(\beta) & \cos(\beta) \end{pmatrix} \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix} = \\ &= \begin{pmatrix} \cos^2(\varphi + \beta) & \sin(\varphi + \beta) \cos(\varphi + \beta) \\ \sin(\varphi + \beta) \cos(\varphi + \beta) & \sin^2(\varphi + \beta) \end{pmatrix} \end{aligned} \quad (7)$$

При $\beta = 0$ данное поляризационное устройство является радиальным поляризатором, который без потерь пропускает РП-пучок, вектор \mathbf{E} которого ориентирован вдоль поперечного радиуса (вектор Джонса $\mathbf{D}_{\mathbf{R}}$) и полностью поглощает АП-пучок с азимутальной поляризационной структурой (вектор Джонса $\mathbf{D}_{\mathbf{A}}$).

Радиальный поляризатор формирует из линейно поляризованного света пучок с радиальной поляризационной структурой, независимо от ориентации плоскости колебаний вектора \mathbf{E} – поляризационного азимута ψ , однако при этом изменяется интенсивность пучка:

$$T_r(0)\mathbf{D}(\psi) = \begin{pmatrix} \cos^2(\varphi) & \sin(\varphi)\cos(\varphi) \\ \sin(\varphi)\cos(\varphi) & \sin^2(\varphi) \end{pmatrix} \begin{pmatrix} \cos(\psi) \\ \sin(\psi) \end{pmatrix} = \begin{pmatrix} \cos(\varphi) \\ \sin(\varphi) \end{pmatrix} \cos(\varphi - \psi), \quad (8)$$

где вектор Джонса линейно поляризованного света записан в виде:

$$\mathbf{D}(\psi) = \begin{pmatrix} \cos(\psi) \\ \sin(\psi) \end{pmatrix}. \quad (9)$$

Потери в этом случае достигают 50%.

Из циркулярно-поляризованного света радиальный поляризатор формирует оптический вихрь с радиальной поляризационной структурой:

$$T_r(0)\mathbf{D} = \begin{pmatrix} \cos^2(\varphi) & \sin(\varphi)\cos(\varphi) \\ \sin(\varphi)\cos(\varphi) & \sin^2(\varphi) \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{\cos(\varphi)}{\sqrt{2}} \\ \frac{\sin(\varphi)}{\sqrt{2}} \end{pmatrix} \exp(i\varphi), \quad (10)$$

при этом потери равны 50%.

Если в (7) переставить местами спиральные вращатели, то получается уже гиперболический поляризатор, собственными состояниями поляризации которого являются векторы Джонса, у которых в отличие от РП-пучка и АП-пучка вектор \mathbf{E} вращается по часовой стрелке при увеличении азимутального угла:

$$\mathbf{D}_{\mathbf{N}_{1r}} = \begin{pmatrix} \cos(\varphi) \\ \sin(\varphi) \end{pmatrix}, \quad \mathbf{D}_{\mathbf{N}_{1a}} = \begin{pmatrix} \sin(\varphi) \\ -\cos(\varphi) \end{pmatrix}. \quad (11)$$

Если в (7) использовать полярные фарадеевские спиральные вращатели, то данное устройство будет представлять собой радиальный поляризатор для одного направления и гиперболический поляризатор для противоположного. Соответственно, в одну сторону будет проходить без потерь пучок $\mathbf{D}_{\mathbf{P}_{1r}}$, а в другую сторону - $\mathbf{D}_{\mathbf{N}_{1r}}$.

Матрица Джонса радиального поляризатора в спиральном P -базисе имеет вид:

$$T_{r\mathbf{P}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \quad (12)$$

Соответственно матрица Джонса гиперболического поляризатора имеет аналогичный вид в спиральном N -базисе.

Радиальный поляризатор, развернутый на угол β , в спиральном базисе имеет вид:

$$T_{r\mathbf{P}}(\beta) = \begin{pmatrix} \cos(\beta) & -\sin(\beta) \\ \sin(\beta) & \cos(\beta) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \cos(\beta) & \sin(\beta) \\ -\sin(\beta) & \cos(\beta) \end{pmatrix} = \begin{pmatrix} \cos^2(\beta) & \sin(\beta)\cos(\beta) \\ \sin(\beta)\cos(\beta) & \sin^2(\beta) \end{pmatrix}. \quad (13)$$

Кроме радиального поляризатора для различения базисных состояний, описанных в табл.1 требуется иметь еще три устройства. Во-первых, это радиальный поляризатор, развернутый на 90° , или, другими словами, аксиальный поляризатор, который пропускает без потерь АП-пучок. Матрица Джонса этого устройства в спиральном базисе имеет вид

$$T_{a\mathbf{P}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad (14)$$

что соответствует подстановке в (13) $\beta = 0$.

Радиальный поляризатор, развернутый на угол 45° описывается в спиральном базисе матрицей Джонса

$$T_{r\mathbf{P}}(45^\circ) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}. \quad (15)$$

Данное поляризационное устройство полностью пропускает закрученный ПСП-пучок и полностью гасит ортогонально поляризованный ЛСП-пучок (5). Для двух других поляризационных структур (4) пропускание является частичным.

Заметим, что если применять устройство, состоящее из линейного поляризатора и двух спиральных вращателей (7), то, поворачивая линейный поляризатор на угол $\pm 45^\circ$, мы получаем два устройства для пропускания ПСП-пучка и ЛСП-пучка.

Как видно из приведенного построения, рассмотренные поляризационно-неоднородные устройства являются хорошими элементами для классического кодирования сигнала. Проблема использования таких устройств в квантовом протоколе состоит в том, что нам необходимо сохранять чистоту состояния, а значит реализовывать только унитарные преобразования сигналов. Наличие оптических потерь в системе регистрации ведёт к потере унитарности преобразования. В то же время, постулат о редукции волновой функции, лежащий в основе криптографической защищенности квантового ключа, перестает работать для смешанных состояний. Таким образом, использование радиальных поляризаторов в схеме детектирования неминуемо влечёт за собой потери в 50%, что не является критичным фактором при классической передаче сигнала, но не может быть удовлетворительным для протоколов КРК, так как данное значение лежит далеко за пределами допустимого для

сохранения защищённости значения потерь в квантовом канале. Поэтому в следующем разделе мы рассмотрим альтернативный подход, позволяющий генерировать векторные поля с требуемой поляризационной структурой используя линейно-поляризованный свет и интерферометр Маха-Цандера на базе угловых отражателей. Обратное преобразование позволяет выполнять детектирование требуемых состояний.

Генерацию интересующих нас аксиально-симметричных пучков можно выполнить, используя различные оптические методы и элементы [27]. Для того чтобы обосновать выбор схемы, представленной в следующем разделе, сформулируем основные требования к схеме генерации/детектирования.

Определяющими факторами, влияющими на выбор схемы, являются:

- 1) Осесимметричность структуры базисных мод. Именно наличие инвариантности относительно вращения пучков в поперечной плоскости обеспечивает удобство связи земля-космос
- 2) Отсутствие значительных оптических потерь при детектировании. Необходимое требование для сохранения уровня защищённости протокола КРК.
- 3) Возможность быстрого управления кодированием. Скорость генерации ключа должна быть не ниже, чем в традиционных поляризационных протоколах КРК.
- 4) Пучки должны обладать свойствами оптических вихрей. Такая особенность пучков способствует более устойчивой передаче информации в турбулентной среде.

IV. ОПИСАНИЕ ПРОТОКОЛА

В этом разделе мы рассмотрим протокол квантового распределения ключа с использованием пучков с аксиально-симметричной структурой поляризации. Для дальнейшего анализа нам будет удобно представить четыре базисных состояния, на основе которых мы будем осуществлять кодирование ключа, в виде:

$$|RP\rangle = |\mathbf{D}_R|LG_{0,1}\rangle; \quad |AP\rangle = |\mathbf{D}_A|LG_{0,1}\rangle; \quad (16)$$

$$|RRP\rangle = |\mathbf{D}_{RR}|LG_{0,1}\rangle; \quad |LRP\rangle = |\mathbf{D}_{LR}|LG_{0,1}\rangle, \quad (17)$$

где \mathbf{D}_i - векторы Джонса, указанные в табл. 1, $|LG_{0,1}\rangle$ – модуль функции Лагерра-Гаусса [28]. Пара состояний $\{|RP\rangle, |AP\rangle\}$, как и пара $\{|RRP\rangle, |LRP\rangle\}$, ортогональны друг другу и образуют базис двумерного гильбертова пространства. При этом, в данной нотации мы отмечаем только пространственно-поперечные и поляризационные особенности состояний, имея в виду, что протокол распределения ключа может быть проведен с использованием однофотонных состояний, подобно традиционным базовым протоколам квантовой криптографии, либо с использованием слабых когерентных состояний. Таким образом, кет-векторы в правой части выражений соответствуют однофотонным (или слабым когерентным) состояниям поля в поляризационной моде, описываемой вектором Джонса и с пространственной поперечной структурой, задаваемой функцией $|LG_{0,1}\rangle$.

Первым шагом протокола является генерация нужных состояний. Аксиально-симметричные поляризационные состояния могут быть относительно легко получены сложением Эрмит-Гауссовых мод с нужными поляризациями, как указано в табл. 1, при этом сложение мод может быть осуществлено дифракционными методами [29]. Однако, стоит заметить, что дифракционные методы не являются удовлетворительным при работе с однофотонными (и слабыми когерентными) состояниями в связи с неизбежными потерями на разных порядках дифракции. Поэтому, мы предлагаем метод генерации путём сложения оптических вихрей с топологическими зарядами ± 1 и циркулярными поляризациями. Данный метод базируется на известном разложении аксиально-симметричных поляризационных состояний:

$$|RP\rangle = \frac{1}{\sqrt{2}} (|R\rangle | +1\rangle + |L\rangle | -1\rangle) = \frac{1}{2} \left(\begin{pmatrix} 1 \\ i \end{pmatrix} |LG_{0,1}\rangle e^{i\phi} + \begin{pmatrix} 1 \\ -i \end{pmatrix} |LG_{0,1}\rangle e^{-i\phi} \right) \quad (18)$$

$$|AP\rangle = \frac{1}{\sqrt{2}} (|R\rangle | +1\rangle - |L\rangle | -1\rangle) = \frac{1}{2} \left(\begin{pmatrix} 1 \\ i \end{pmatrix} |LG_{0,1}\rangle e^{i\phi} - \begin{pmatrix} 1 \\ -i \end{pmatrix} |LG_{0,1}\rangle e^{-i\phi} \right) \quad (19)$$

$$|RRP\rangle = \frac{1}{\sqrt{2}} (|R\rangle | +1\rangle + i |L\rangle | -1\rangle) = \frac{1}{2} \left(\begin{pmatrix} 1 \\ i \end{pmatrix} |LG_{0,1}\rangle e^{i\phi} + i \begin{pmatrix} 1 \\ -i \end{pmatrix} |LG_{0,1}\rangle e^{-i\phi} \right) \quad (20)$$

$$|LRP\rangle = \frac{1}{\sqrt{2}} (|R\rangle | +1\rangle - i |L\rangle | -1\rangle) = \frac{1}{2} \left(\begin{pmatrix} 1 \\ i \end{pmatrix} |LG_{0,1}\rangle e^{i\phi} - i \begin{pmatrix} 1 \\ -i \end{pmatrix} |LG_{0,1}\rangle e^{-i\phi} \right) \quad (21)$$

$$(22)$$

Здесь кет-векторы $|R\rangle, |L\rangle$ обозначают поляризационные моды с право- и лево-циркулярными поляризациями, соответственно, векторы $| \pm 1 \rangle$ отвечают за топологический заряд оптического вихря, при этом знак плюс отвечает вращению фазы по часовой стрелке, а минус – против часовой стрелки.

будет использовано нами при детектировании. Таким образом, на выходе интерферометра Маха-Цандера мы имеем одно из четырех состояний, определённых выражениями (16)-(17).

Схема детектирования состояний Бобом показана на рисунке 2в. Боб использует тот же интерферометр с поляризационными светоделителями, что и Алиса, для разделения азимутально-симметричных поляризационных состояний на суперпозицию оптических вихрей $|R\rangle|+1\rangle$ и $|L\rangle|-1\rangle$, после чего преобразует свет в первом и втором каналах на выходе первого интерферометра в состояния с нулевым топологическим зарядом и горизонтальной поляризацией. Такие преобразования, как и ранее, могут быть выполнены с использованием статических оптических элементов и не требуют быстрого переключения. После указанных преобразований Боб получает два одинаковых состояния в двух выходных каналах с относительной фазой, которая была задана Алисой при кодировании. Боб осуществляет выбор базиса детектирования при помощи установки дополнительной фазы (PP 2 на рис. 2в) в первом выходном канале: фаза 0 отвечает детектированию в базисе $\{|RP\rangle, |AP\rangle\}$, а фаза $-\pi/2$ - детектированию в базисе $\{|RR\rangle, |LR\rangle\}$. После всех вышеописанных действий, Боб смешивает пучки на обыкновенном светоделителе и проводит измерение в обоих каналах при помощи однофотонных детекторов. При измерении в базисе $\{|RP\rangle, |AP\rangle\}$ срабатывание детектора SFD 1 будет означать, что разность фаз между пучками равна нулю, а значит Алиса отправляла состояние $|RP\rangle$, а срабатывание детектора SFD 2 говорит о фазе π и отправке состояния $|AP\rangle$. При этом попытка измерения таких состояний в сопряжённом базисе (Боб ставит в один из каналов дополнительную фазовую пластину $\pi/2$), приведёт к равновероятному срабатыванию детекторов. Просеивание ключа Алиса и Боб осуществляют подобно протоколу BB84.

Несомненно, криптостойкость представленного протокола квантовой криптографии должна быть проанализирована в деталях и оценена. Этот вопрос является предметом отдельного исследования и вынесен за пределы этой статьи. В настоящей работе мы ограничились описанием перспективы использования аксиально-симметричных состояний векторных полей, а также презентацией методов кодирования и детектирования информации на таких физических системах.

Отметим, что представленный протокол, в отличие от поляризационного кодирования, использует состояния, инвариантные относительно поворота поляризационного базиса, и кроме того, в отличие от протокола фазового кодирования, предложенного в [32], не требует отправки дополнительных состояний. Также стоит отметить, что, поскольку измеряется относительная фаза между двумя компонентами пучка, протокол нечувствителен к длине оптического пути, то есть нам не нужно знать точную фазу, которую приобретает световой пучок при распространении в канале связи, а только относительную фазу. Несомненным преимуществом протокола является возможная скорость генерации ключа, так как для кодирования и детектирования нам нужно менять только фазу, что может быть сделано достаточно быстро [33, 34], поэтому мы ограничены только характеристиками фазовых модуляторов и источника однофотонных или слабых когерентных состояний. К минусам данного протокола можно отнести относительную сложность юстировки большого числа интерферометров, однако эта проблема может быть нивелирована использованием высокостабильных интегральных схем [35].

Практическая реализация может быть осуществлена следующим образом. На спутнике на входе оптико-лазерной системы наведения должен находиться узкополосный лазер и четвертьволновая пластинка для генерации света с горизонтальной поляризацией. На выходе из системы наведения необходимо расположить интерференционную схему, описанную выше, которая формирует четыре базисных пучка с различной аксиально-симметричной поляризационной структурой. Важным условием является совпадение оптической оси пучка и системы детектирования на Земле. Этого можно достичь, используя систему наведения с соосным пучком, который обладает достаточной мощностью и, возможно, другой длиной волны, например, 532 нм, что удобно при юстировке системы. Заметим, что кроме аксиально-симметричной поляризационной структуры пучки на выходе будут обладать свойствами оптического вихря, поскольку, согласно 10, фазовая структура пучков изменяется пропорционально азимутальному углу. Как известно (см., например, [36]), оптические вихри обладают большей устойчивостью к флуктуациям атмосферы, чем обычные лазерные пучки.

На Земле должно располагаться устройство детектирования, подобно описанному выше.

В качестве иллюстрации возможности генерации рассматриваемых здесь пучков, на рис. 3 нами приведены полученные экспериментально изображения поперечного сечения пучка, прошедшего сквозь турбулентную среду, а также фрагмент интерференционной картины с изображением «вилки», что подтверждает сохранение оптического вихря после прохождения турбулентной среды.

V. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ, ВЫВОДЫ

В работе предложена реализация квантового криптографического протокола с использованием пучков, обладающих аксиальной симметрией состояния поляризации. Данная реализация инвариантна по отношению к повороту относительно оси распространения пучка, что делает её устойчивой для случая даже существенного

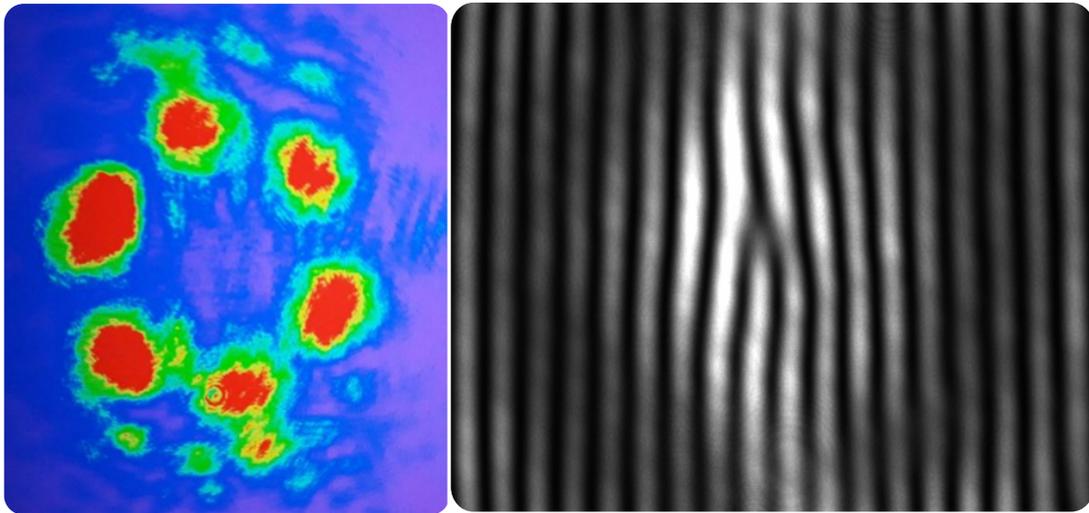


Рис. 3. Эксперимент. Слева: прохождение пучка через турбулентную среду. Справа: наличие «вилки» в интерференционной картине. Изображения получены в интерферометре с использованием угловых отражателей в качестве зеркал [30].

изменения состояния поляризации в различных точках небесной полусферы. Такая проблема является характерной для систем квантового распределения ключа через низкоорбитальные космические аппараты.

Создание рассматриваемых пучков может быть выполнено различными путями. Мы показали как генерировать такие структуры с помощью неоднородных (радиальных) поляризаторов и в схеме интерференции полей, отраженных угловыми отражателями. Если для генерации полей оба метода представляются правомочными для квантового криптографического протокола (хотя использование радиальных поляризаторов приведет к снижению скорости генерации ключа), то при детектировании использование радиальных поляризаторов будет приводить к потере информации, а значит и к потере криптостойкости протокола. С этих позиций кажется логичным использовать интерферометры на угловых отражателях как на этапе генерации, так и на этапе детектирования сигналов. Именно такой протокол предъядвлен в работе.

В данной работе мы не приводим детального описания криптостойкости предлагаемого протокола, имея в виду объемность работы, однако хотели бы указать на необходимость такого анализа для оценки качества работы протокола. Оценку длины секретного ключа в асимптотическом пределе при коррекции ошибок случайными шенноновскими кодами и предела (информации) Холево следует производить на основе вычисления условной энтропии фон Неймана для матриц плотности подсистем Алиса-Ева, Алиса-Боб, подсистемы Ева и подсистемы Боб. При этом, нужно учесть специфику предлагаемого протокола и, при более строгом исследовании криптостойкости, также учесть возможность детектирования побочного излучения передающей аппаратуры Евой (наличие побочных каналов утечки информации), активного зондирования Евой состояния фазового модулятора на передающем спутнике, а также возможную неидеальность однофотонного источника. Подсчет комбинаций отдельных долей однофотонных компонент в посылке Алисы и ошибки в ней следует произвести при помощи Decoy State-метода. Эти исследования являются следующим шагом в работе и запланированы авторами.

Важным свойством предлагаемой нами схемы является возможность быстрого управления процессом генерации и распознавания базисных состояний. Поскольку выбор базиса осуществляется управлением фазовыми пластинами, то скорость генерации ключа не будет снижаться относительно традиционного поляризационного протокола. Это отличает предлагаемую реализацию от других протоколов КРК с аксиально-симметричными пучками (например, протоколов на основе мод с орбитальным угловым моментом). Именно невозможность быстрого управления осе-симметричными базисами является сдерживающим фактором применения вихревых полей в системах связи.

Наконец, наличие вихревой природы у базисных пучков позволяет надеяться на лучшую устойчивость передачи сигналов в турбулентной среде.

Авторы выражают благодарность проф. Венедиктову В. Ю. за полезные советы и обсуждения, способствующие подготовке данной работы. Г.Т.Ю. и В.Е.А. выражают благодарность Санкт-Петербургскому государственному университету за финансовую поддержку (ID 104146607, ID 105692662). В.Е.А. выражает благодарность

-
- [1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* 74 145 (2002). DOI 10.1103/RevModPhys.74.145
- [2] C. Portmann, R. Renner, Security in quantum cryptography, *Rev. Mod. Phys.* 94, 025008 (2022). DOI 10.1103/RevModPhys.94.025008
- [3] C. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theoretical Computer Science*, 560 (1), 7-11, (2014). DOI 10.1016/j.tcs.2014.05.025
- [4] M. Mirhosseini, O. S. Magana-Loaiza, M. N. O'Sullivan, et al., High-dimensional quantum cryptography with twisted light, *New J. Phys.* 17 033033 (2015). DOI 10.1088/1367-2630/17/3/033033
- [5] T. Doster, A. Watnik, Laguerre–Gauss and Bessel–Gauss beams propagation through turbulence: analysis of channel efficiency, *Appl. Opt.*, 55 (36), 10239 (2016). <http://dx.doi.org/10.1364/AO.55.010239>
- [6] M. P. J. Lavery, C. Peuntinger, K. Gunthner, et al., Free-space propagation of high-dimensional structured optical fields in an urban environment, *Sci. Adv.*, 3 (10) e1700552 (2017). DOI: 10.1126/sciadv.1700552
- [7] Z. Qu, I. B. Djordjevic, High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing, *Opt. Express*. 25 (7) 7919 (2017). <https://doi.org/10.1364/OE.25.007919>
- [8] A. Sit, R. Fickler, F. Alsairai, et al., Quantum cryptography with structured photons through a vortex fiber, *Opt. letters*, 43 (17) 4108 (2018). <https://doi.org/10.1364/OL.43.004108>
- [9] I. A. Adam, D. A. Yashin, D. A. Kargina, et al., *Nanosystems: Phys. Chem. Math.*, 13 (4) 392 (2022). DOI 10.17586/2220-8054-2022-13-4-392-403
- [10] Z. Wang, R. Malaney, J. Green, Conference paper: GLOBECOM 2019 - 2019 IEEE Global Communications Conference. 1 (IEEE 2019) <http://dx.doi.org/10.1109/GLOBECOM38437.2019.9014321>
- [11] S.-K. Liao, C. W.-Q. Cai, W.-Y. Liu, and et al., *Nature*. 549, 43 (2017). <https://doi.org/10.1038/nature23655>
- [12] Y.-A. Chen, Q. Zhang, C.-Y. Chen et al., *Nature*, 589, 214 (2021). <https://doi.org/10.1038/s41586-020-03093-8>
- [13] А. Л. Соколов, *Радиотехника* 87(3) 93 (2023) (в печати).
- [14] А. С. Акентьев, М. А. Садовников, А. Л. Соколов, Г. В. Симонов, *Оптика и спектроскопия*, 122 (6) 1044 (2017) <https://doi.org/10.7868/S0030403417060022>
- [15] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, P. Villoresi, Free-Space Quantum Key Distribution by Rotation-Invariant Twisted Photons, *Phys. Rev. Lett.* 113, 060503 (2014). DOI 10.1103/PhysRevLett.113.060503
- [16] L. Marrucci, C. Manzo, D. Paparo, Optical Spin-to-Orbital Angular Momentum Conversion in Inhomogeneous Anisotropic Media, *Phys. Rev. Lett.* 96, 163905 (2006). DOI 10.1103/PhysRevLett.96.163905
- [17] S. Maccalli, G. Pisanò, S. Colafrancesco, B. Maffei, M. W. R. Ng, M. Gray, q-plate for millimeter-wave orbital angular momentum manipulation, *Appl. Opt.* 52, 635-639 (2013). DOI 10.1364/AO.52.000635
- [18] S. Li, J. Wang, Simultaneous demultiplexing and steering of multiple orbital angular momentum modes, *Scientific Reports*. 5. 15406 (2015). DOI 10.1038/srep15406
- [19] В. Г. Низьев, А. В. Несеров, А. Л. Соколов, *Вестник МЭИ*, 2, 76 (1999).
- [20] A. Tovar, Production and propagation of cylindrically polarized Laguerre-Gaussian laser beams. *J. Opt. Soc. Am. A*. 15. 2705 (1998). <https://doi.org/10.1364/JOSAA.15.002705>
- [21] Е. Ф. Ищенко, А. Л. Соколов. *Поляризационная оптика (учебное пособие, изд. 3)*. М.: Изд.-во. ФИЗМАТЛИТ. 2019. ISBN 978-5-9221-1838-5
- [22] R. Dorn, S. Quabis, G. Leuchs, *Appl. Phys. B*. 81 (5) 597 (2005). DOI: 10.1007/s00340-005-1887-1
- [23] В. Г. Низьев, В. П. Якунин, Н. Г. Туркин, Генерация поляризационно-неоднородных мод в мощном CO₂-лазере. *Квант. электрон.*, 39 (6) 505 (2009). <https://doi.org/10.1070/QE2009v039n06ABEH013962> [*Quant. Electron.*, 39 (6) 505 (2009). <https://doi.org/10.1070/QE2009v039n06ABEH013962>]
- [24] *Дифракционная нанофотоника*. Под ред. В.А.Сойфера. М.: Физматлит. 2011. ISBN 978-5-9221-1237-6
- [25] A. L. Sokolov, Optical vortices with axisymmetric polarization structure, *J. Opt. Soc. Am. A.*, 30 (7) 1350 (2013). <http://dx.doi.org/10.1364/JOSAA.30.001350>
- [26] A. L. Sokolov, *Opt. Eng.*, 56 (1) 014109-1-9 (2017). <http://dx.doi.org/10.1117/1.OE.56.1.014109>
- [27] S. Khonina, S. Karpeev, S. Alferov, V. Soifer, Generation of cylindrical vector beams of high orders using uniaxial crystals, *Journal of Optics*. 17 (2015). DOI 10.1088/2040-8978/17/6/065001.
- [28] S. Huang, Z. Miao, C. He, F. Pang, Y. Li, T. Wang, Composite vortex beams by coaxial superposition of Laguerre–Gaussian beams. *Optics and Lasers in Engineering*, 78, 132-139 (2016). DOI 10.1016/j.optlaseng.2015.10.008
- [29] S. Khonina, S. Karpeev, Grating-based optical scheme for the universal generation of inhomogeneously polarized laser beams, *Appl Opt.*, 49(10), 1734-8 (2010). DOI 10.1364/AO.49.001734. PMID: 20357853.
- [30] М. А. Садовников, А. Л. Соколов, Пространственная поляризационная структура излучения, формируемая уголковыми отражателями с нематаллизированными гранями // *Оптика и спектроскопия*. 2009. Т. 107, № 2. С. 213 – 218, ISSN 0030-4034
- [31] A. Sokolov, V. Murashkin, Retroreflective spatial-polarization interferometer. *Applied Optics*, 59(32), 9912-9923 (2020). DOI 10.1364/AO.403232

- [32] V. Huttner, N. Imoto, N. Gisin, T. Mor, Quantum cryptography with coherent state, *Physical Review A*, 51(3), 1863 (1995).
- [33] В. Петров, А. Шамрай, И. Ильчев, П. Агрузов, В. Лебедев, Н. Герасименко, В. Герасименко, Отечественные СВЧ интегрально-оптические модуляторы для квантовых коммуникаций, *PHOTONICS Russia*, 14 (5) (2020). DOI 10.22184/1993-7296.FRos.2020.14.5.414.423
- [34] В. Петров, П. Агрузов, В. Лебедев, И. Ильичёв, А. Шамрай, Широкополосные интегрально-оптические модуляторы: достижения и перспективы развития, *Успехи Физических Наук*, 191 (7), 760-782 (2021). DOI 10.3367/UFNг.2020.11.038871
- [35] В. Петров, А. Шамрай, И. Ильичев, Н. Герасименко, В. Герасименко, П. Агрузов, В. Лебедев, Генерация оптических частотных гармоник для систем квантовых коммуникаций на боковых частотах, *PHOTONICS Russia*, 14 (7) (2020). DOI 10.22184/1993-7296.FRos.2020.14.7.570.582
- [36] C. Paterson, *Phys. Rev. Letters*. 94. (2005) 153901. DOI:<https://doi.org/10.1103/PhysRevLett.94.153901>