

О Т З Ы В

официального оппонента на диссертацию Кравцова Константина Сергеевича
«Управление оптическими полями для задач связи и защиты информации»,
представленную на соискание
учёной степени доктора физико-математических наук
по специальности 01.04.21 – лазерная физика

Докторская диссертация Кравцова К.С. посвящена экспериментальной и теоретической разработке новых подходов к представлению, обработке, передаче и защите информации в виде оптических сигналов, в том числе на основе квантовых оптических технологий.

Актуальность таких исследований не вызывает сомнений. В настоящее время во всем мире наблюдается экспоненциальный рост потоков информации, передаваемой по каналам связи, объемов информации, обрабатываемой в вычислительных и дата-центрах, числа объектов критической инфраструктуры, объединенных в общую сеть и требующих исключительно высокой степени информационной безопасности. Дальнейший прогресс в этих направлениях немыслим без развития оптических методов представления, передачи и обработки информации. В частности, ограниченные ресурсы оптоволоконных каналов связи требуют постоянного повышения эффективности представления информации в виде оптических сигналов, методов их модуляции и мультиплексирования. Все более широкое внедрение таких вычислительно-сложных операций, как распознавание голоса и изображений, перевод текста с языка на язык и других аналогичных задач, ведет к бурному росту технологий искусственного интеллекта и нейроморфной обработки сигналов, которые в перспективе могут быть реализованы с высокой скоростью путем оптического представления информации. Наконец, постоянный рост нарушений информационной безопасности, даже без учёта вирусных атак, приводит к значительным финансовым потерям. В этой связи, актуальной задачей является разработка квантовых сетей связи, использующих протоколы квантовой криптографии, которые гарантируют абсолютную секретность передаваемой информации. При этом, для решения многих практических задач требуется квантовая связь не только по оптоволоконным каналам связи, но и по открытому пространству, что позволяет организовать обмен секретными ключами между беспилотными транспортными средствами и повысить безопасность интернета вещей. Цель диссертационной работы как раз и состоит в том, чтобы решить наиболее актуальные проблемы в области передачи, обработки и защиты информации с использованием оптических полей.

Научная и практическая значимость диссертации связана с тем, что полученные в ней теоретические и экспериментальные результаты расширяют возможности

эффективной обработки и передачи информации с использованием оптических сигналов и, тем самым, способствуют развитию оптических информационных технологий, имеющих широкий спектр применения. В частности, разработанная голографическая интегрально-оптическая платформа позволяет решать разнообразные задачи управления оптическим полем на чипе, в том числе – создание высокоскоростной связи между вычислительными ядрами. Разработанный квантовый генератор случайных чисел обеспечивает предельно простое и эффективное решение задачи экстракции случайных чисел, что является крайне важным для более широкого внедрения устройств квантовой криптографии. Представленный в работе протокол квантовой криптографии на геометрически однородных квантовых состояниях является перспективным для использования в коммерческих системах квантового распределения ключа. Результаты исследования турбулентных свойств атмосферных линий связи способствуют более глубокому пониманию процессов передачи квантовых состояний света через атмосферу, что позволяет точнее оценивать перспективность решений в области квантовых коммуникаций через атмосферные и космические каналы связи.

Полученные в диссертации результаты представляют интерес для специалистов, работающих в области квантовой оптики, интегральной оптики, оптической связи, квантовой информатики и квантовых оптических технологий, и могут быть использованы при подготовке учебных курсов в высших учебных заведениях Российской Федерации.

Достоверность положений и результатов диссертации обеспечивается высоким уровнем владения экспериментальными методами, хорошим согласием экспериментальными данными с теоретическими расчётами, а также тем, что разработанные методы и принципы успешно применялись в более поздних экспериментальных исследованиях, в том числе других научных коллективов. Все результаты имеют простое качественное объяснение в рамках известных физических моделей квантовой оптики.

Новизна проведённых исследований и полученных результатов заключается в следующем:

- Впервые предложено универсальное полностью оптическое устройство для реализации прямого и обратного преобразования Фурье, на базе которого экспериментально продемонстрирована система связи с ортогональным частотным разделением каналов (OFDM);
- Впервые предложена идея оптического нейроморфного устройства на базе полупроводникового оптического усилителя, позволяющая реализовать сверхбыстрые оптические нейронные сети, а также продемонстрирована его полноценная реализация;

- Впервые разработана модель турбулентного канала по открытому пространству, позволяющая непосредственно предсказывать затухание для конкретных пространственных мод и амплитуды соответствующих перекрестных помех;
- Впервые предложен и экспериментально продемонстрирован новый подход к томографии пространственных квантовых состояний света на базе микроэлектромеханического деформируемого зеркала;
- Впервые экспериментально реализован релятивистский протокол квантовой криптографии;
- Впервые приведено доказательство и анализ секретности для протокола квантового распределения ключей на базе геометрически-однородных квантовых состояний света общего вида.

Диссертация состоит из введения, шести глав, заключения, списка литературы, а также списка использованных сокращений, списка опубликованных статей и списка зарегистрированных патентов. Общий объём диссертации составляет 199 страниц машинописного текста, диссертация включает 94 рисунка и список цитируемой литературы из 218 наименований.

Во введении обосновывается актуальность диссертации, обсуждается степень разработанности темы исследования, формулируются цель работы, научная новизна исследования и защищаемые положения, обсуждается теоретическая и практическая значимость полученных результатов. Приведены также данные об апробации результатов на международных конференциях.

В первой главе предложены два новых решения для представления и передачи информации в виде оптических сигналов. Первое посвящено оптическим системам на основе ортогонального частотного разделения каналов (OFDM) и представляет собой полностью оптическую реализацию дискретного преобразования Фурье на основе планарных волноводных решеток. Экспериментально продемонстрирована полностью оптическая система OFDM, потенциально позволяющая достигать общей пропускной способности в 120 Гбит/с. Второе решение посвящено использованию технологии цифровой планарной голографии для изготовления широкого класса оптических приборов на чипе. В частности, был спроектирован целый ряд устройств, демонстрирующих перспективность использования данной технологии, среди которых система оптического множественного доступа с кодовым разделением каналов (CDMA), оптический интерконнект на чипе, мультиплексор/демультиплексор для линий связи со спектральным уплотнением (WDM), а также и многочастотный и селективный по длине волны переключатель.

Вторая глава посвящена разработке оптического метода обработки информации, основанного на нейроморфных вычислениях. Экспериментально продемонстрирован

полнофункциональный сверхбыстрый оптический нейрон с импульсным режимом работы, который может стать базовым элементом аналогово-оптических вычислителей общего назначения. Продемонстрированный на базе полупроводникового оптического усилителя нейрон обеспечивает полный функционал, необходимый для модели нейронов с импульсами, и при этом работает с импульсами пикосекундной ширины, имея постоянную времени интегрирования порядка 100 пс, что соответствует ускорению порядка 10^8 по сравнению с биологическими нейронами.

В третьей главе предложен и экспериментально продемонстрирован метод генерации и распределения секретного ключа с использованием фазовых флуктуаций в волоконно-оптических линиях связи. Предложенный метод использует крупномасштабный интерферометр Маха-Цандера, покрывающий все расстояние между абонентами, так что защищенность ключей проистекает из практической невозможности измерения оптической разности фаз между двумя некогерентными широкополосными оптическими сигналами. Представленная лабораторная демонстрация показала скорость генерации ключей 160 бит/с на линии связи длиной 26 км со средней долей битовых ошибок менее 4%.

Четвёртая глава посвящена экспериментальным и теоретическим исследованиям процесса распространения квантовых состояний света через турбулентную атмосферу. В экспериментальном плане разработана и реализована турбулентная камера с контролируемыми параметрами турбулентности, проведены экспериментальные измерения ее основных параметров, в том числе сравнение с реальным турбулентным каналом. Кроме того, разработано необходимое теоретическое описание каналов связи для передачи пространственных квантовых состояний, которое показало хорошее качественное сходство с результатами прямых измерений. Представленный формализм позволяет рассчитывать потерю мощности в конкретной моде и связь ее с другими модами, что необходимо для детальной характеристики одномодовых каналов или каналов с модовым мультиплексированием по открытому пространству в турбулентной атмосфере.

В пятой главе экспериментально демонстрируется метод томографии пространственных квантовых состояний света с помощью деформируемого зеркала. Предложенный подход позволяет выполнять томографию на порядки быстрее (за миллисекундные временные интервалы) и с меньшими потерями излучения, чем при традиционном подходе на основе пространственных фазовых модуляторов. Метод также позволяет избавиться от поляризационной чувствительности восстановления квантовых состояний. В проведенных экспериментах продемонстрирована квантовая томография в четырехмерном гильбертовом пространстве путем проведения измерений во взаимно несмещенных базисах. Достигнуто среднее значение меры соответствия (fidelity), равное 0.95. Предлагаемое решение может найти применение для томографии турбулентных оптических атмосферных каналов в реальном времени, а также в других нестационарных экспериментальных условиях.

Шестая глава посвящена разработке базовых устройств и протоколов квантовой криптографии. Предложен вариант простого и надежного квантового генератора случайных чисел с детерминистическим экстрактором случайности на базе измерения временных интервалов между срабатываниями однофотонного детектора. В экспериментальной реализации получены потоки случайных бит более 1 Мбит/с. Продемонстрированы две реализации релятивистского протокола квантового распределения ключей: однопроходная и двухпроходная. Во втором случае реализована система активного трекинга в канале связи по открытому пространству и продемонстрировала асимптотическую скорость генерации секретных ключей в сотни бит в секунду при дальности канала по открытому пространству 180 м. Теоретически разработан протокол квантовой криптографии на геометрически-однородных квантовых состояниях с состояниями-ловушками. Приведены доказательства секретности предлагаемого протокола и моделирование эффективности его работы при различных условиях передачи.

В заключении сформулированы основные результаты диссертации.

По диссертационной работе имеются следующие **замечания**:

1. В диссертации выполнено много численных расчетов, однако в ряде случаев (разделы 1.1.2, 1.1.3, 4.2.4) нет указаний того, с помощью каких методов и с какой точностью они проводились.
2. В разделе 1.2.2 приводится оценка величины, на которую нужно изменить показатель преломления для перестройки голограммы. Важным вопросом, который при этом не обсуждается, является допустимая погрешность и ее достижимость в эксперименте.
3. В разделе 3.4.1 при описании лабораторной реализации предложенного метода генерации ключа обсуждаются два важных этапа настройки интерферометра: выравнивание длин плеч и настройка поляризаций. При этом нет информации о методике настройки и возможности ее использования в полевых, а не лабораторных условиях.
4. В разделе 6.3.6 при обсуждении результатов вычислений доли секретной информации в просеянном ключе и скорости генерации ключа (рис. 6.19) делается вывод, что значение параметра $2\mu = 0.9$ является близким к оптимальному для длины канала 100 км в смысле скорости генерации секретной информации. При этом остается неясным, каков критерий оптимальности.
5. На рисунке 4.6 отсутствует цветовая шкала.

Тем не менее, эти замечания не носят принципиального характера и не снижают общей очень высокой оценки диссертационной работы. Диссертация представляет собой цельное и законченное научное исследование, содержание которого соответствует целям работы и названию диссертации. Все защищаемые научные положения, выводы и

рекомендации хорошо обоснованы. Работа выполнена автором на высоком научном уровне, характеризуется необходимой новизной и достоверностью полученных результатов, написана понятным и грамотным литературным языком, хорошо оформлена и показывает, несомненно, высокую квалификацию и научную зрелость автора. По теме диссертации опубликовано двадцать работ в высокорейтинговых международных научных журналах и зарегистрировано пять патентов, а полученные результаты неоднократно докладывались на международных научных конференциях. Автореферат диссертации полностью соответствует ее содержанию.

На основании вышесказанного считаю, что содержание работы и форма ее представления полностью соответствует требованиям пунктов 9-14 «Положения о порядке присуждения ученых степеней» ВАК Минобрнауки России в редакции Постановления Правительства РФ № 842 от 24 сентября 2013 г., предъявляемым к докторским диссертациям. Автор – Кравцов Константин Сергеевич, обладает высокой квалификацией и, несомненно, достоин присуждения искомой степени доктора физико-математических наук по специальности 01.04.21 – лазерная физика.

Официальный оппонент:

Калачев Алексей Алексеевич, доктор физ.-мат. наук по специальности 01.04.05 – оптика, доцент по специальности 01.04.05 – оптика, член-корреспондент РАН, директор Федерального государственного бюджетного учреждения науки «Федеральный исследовательский центр «Казанский научный центр Российской академии наук».
Эл. почта: a.kalachev@knc.ru, раб. тел. (843)2319000.



А.А.Калачев
22.08.22

Федеральное государственное бюджетное учреждение науки «Федеральный исследовательский центр «Казанский научный центр Российской академии наук».

Адрес: 420011, Казань, ул. Лобачевского, 2/31.

<http://www.knc.ru>, эл. почта: presidium@knc.ru, тел. (843)2319000