На правах рукописи

ПОДОШВЕДОВ Сергей Анатольевич

НЕКЛАССИЧЕСКИЕ ПЕРЕМЕЩЕННЫЕ СОСТОЯНИЯ СВЕТА

Специальность 01.04.02 – Теоретическая физика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико-математических наук

ЧЕЛЯБИНСК — 2015

Работа выполнена на кафедре общей и теоретической физики федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Южно-Уральский государственный университет» (национальный исследовательский университет) и в Корейском научно-исследовательском институте КИАС (Korea Institute for Advanced Study (KIAS)) г. Сеул, Южная Корея.

Научный консультант - профессор КИАС Джаеван Ким (Jaewan Kim)

Официальные оппоненты:

Кулик Сергей Павлович — доктор физико-математических наук, профессор, заведующий лабораторией квантовой информации и квантовой оптики кафедры квантовой электроники физического факультета федерального образовательного учреждения высшего профессионального образования «Московский государственный университет им. М.В. Ломоносова»;

Моисеев Сергей Андреевич — доктор физико-математических наук, профессор, заведующий лабораторией квантовой оптики и информатики федерального государственного бюджетного учреждения науки «Казанский физико-технический институт им. ЕК Завойского»;

Алоджанц Александр Павлович — доктор физико-математических наук, профессор кафедры физики и прикладной математики федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых».

Ведущая организация:

Институт физики имени Б. И. Степанова Национальной академии наук Беларуси.

Защита состоится «23» октября 2015 года в 14.00 на заседании диссертационного совета Д 212.296.03 при Челябинском государственном университете по адресу: 454001, г. Челябинск, ул. Братьев Кашириных, 129; конференц-зал.

С диссертацией можно ознакомиться в библиотеке Челябинского государственного университета.

Автореферат разослан «___ »_____ 2015г.

Ученый секретарь диссертационного
совета, доктор физико-математических
наук, профессор Е.А. Беленков

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Квантовый компьютер --- вычислительное устройство, в основу работы которого положены законы квантовой механики. Квантовый компьютер принципиально отличается от классических компьютеров, работающих на основе законов классической физики. Вся информация кодируется в состоянии физической системы. Поэтому изучение информации связано с изучением физических процессов, положенных в основу устройств обработки информации. Квантовая механика и теория информации являются двумя наиболее важными интеллектуальными достижениями прошлого века. Квантовая информатика обеспечивает наиболее точное описание микроскопических объектов на атомном уровне таких как электроны и фотоны. С другой стороны теория информации была создана для того, чтобы успешно обрабатывать и хранить информацию. В настоящее время значимость теории информации полностью признано успешным развитием телекоммуникационных технологий и компьютеров. Цифровые компьютеры используют двоичные гейты, и информация кодируется в виде последовательности двоичных битов, которые принимают значения 0 и 1. Обычно значение 1 кодируется несколькими вольтами, а значение 0 отсутствием напряжения, и вся обработка информации происходит манипулированием напряжений. В отличии от классической информации, квантовая информация кодируется квантовыми битами или кубитами, которые могут находиться в суперпозиции 0 и 1

$$\alpha|0\rangle+\beta|1\rangle, \quad |\alpha|^2+|\beta|^2=1.$$

Данное выражение означает, что с вероятностью $|\alpha|^2\left(|\beta|^2\right)$ кубит будет найден в состоянии $|0\rangle\left(|1\rangle\right)$ после измерения. Кубит может взаимодействовать с другим кубитом таким образом, что состояние совместной системы становится запутанным

$$\left(|0\rangle_1|1\rangle_2+|1\rangle_1|0\rangle_2\right)/\sqrt{2},$$

где нижние индексы 1 и 2 относятся в первой и второй частицам. Данные свойства носителей квантовой информации положены в основу построения квантовых алгоритмов и квантовых компьютеров. В настоящее время полноценный квантовый компьютер является гипотетическим устройством. Тем не менее, данная модель позволяет глубже понять законы квантового мира и является основой для освоения новых будущих технологий.

Одна из первых моделей квантового компьютера была предложена Р. Фейнманом в [1]. Квантовый параллелизм совместно с запутанностью состояний положены в основу построения квантовых компьютеров и квантовых алгоритмов. В настоящее время наиболее известны два таких квантовых протокола: протокол Шора [2], который используется для быстрой факторизации больших чисел и протокол Гровера [3] для более быстрого поиска нужного элемента из большого набора не отсортированной информации. Возможность построения квантового компьютера связана с дальнейшим серьезным развитием квантовой теории эволюции многих частицы. Представляет интерес и реализация новых сложных экспериментов, которые связаны с построением элементов квантовых компьютеров. Поэтому работы по реализации элементов квантовых компьютеров даже на абстрактном уровне находятся на переднем крае современной физики.

Параллельно с теоретическим развитием идей квантового компьютера и квантовых алгоритмов развивались и другие идеи, прямо проистекающие из базовых постулатов квантовой механики. А именно, протокол квантовой телепортации не известного состояния кубита [4], протокол плотного кодирования информации [5], разнообразные протоколы квантовой криптографии [6-8], квантовая литография [9] и другие протоколы. Все вместе данные направления и составляют предмет квантовой информатики. В настоящее время имеет место бурное развитие квантовой информатики, что выливается в рассмотрение идей квантовых сетей, квантовых игр, и даже вводится свой высокоуровневый язык программирования Quipper для квантовых компьютеров.

Тем не менее, успешное развитие абстрактных идей квантовой информатики делает особо актуальным вопрос как на практике реализовать данные протоколы и еще раз проверить корректность квантового описания. В какой среде может быть наиболее эффективно реализован тот или иной протокол квантовой информации? Существует несколько физических систем пригодных для практической реализации квантовых компьютеров и других квантовых протоколов: ядерный магнитный резонанс, ионные ловушки, нейтральные атомы, полупроводники и оптические методы. Вопрос выбора физической системы, которая бы наилучшим образом подходила для реализации того или иного протокола квантовой информатики, является ключевым. Решение данной проблемы должно учитывать свойства физической системы, ее поведение в тех или иных условиях, взаимодействие физической системы с окружающей средой.

Свет обладает рядом полезных свойств (максимальная скорость распространения, свойства света не зависят от температуры, достаточно сильная сопротивляемость эффекту декогерентности при распространении в свободном пространстве), которые делают разработку квантовых протоколов с оптическими кубитами и запутанными состояниями очень перспективным направлением. Например, протоколы квантовой криптографии могут быть реализованы только на световых носителях информации. Многие экспериментальные работы по квантовой информации были реализованы с фотонными носителями информации [10]. Создание оптических элементов квантовых компьютеров также является очень перспективным направлением. Хотя, скорее всего, будущий квантовый компьютер будет реализован на основе нескольких физических систем в том числе с использованием оптических кубитов. Другой аспект квантово-механического рассмотрения света --- это реализация оптического аналога Шредингеровского состояния котов [11]. Данная проблема является фундаментальной, связанной с вопросом полноты квантовой механики. Почему существует такое резкое различие в поведении классических и квантовых частиц. Где проходит граница между классическим и квантовым мирами и есть ли она вообще? Возможно ли применять законы квантовой механики к макроскопическим (оптическим) состояниям?. И как следствие возможно ли использовать макроскопические оптические состояния в протоколах квантовой информации?

Все выше изложенное и определяет актуальность темы настоящей диссертации.

Цель диссертационной работы --- исследование фундаментальных вопросов полноты квантовой механики по отношению к неклассическим перемещенным состояниям света, которые могут быть рассмотрены в качестве макроскопических (состояний с большой энергией) в случае увеличения амплитуды перемещения, и расширение возможностей реализации квантовых протоколов с неклассическими перемещенными (макроскопическими) фотонными состояниями света.

Основные задачи работы:

--- Развить математический аппарат точных матричных преобразований из одного набора перемещенных фотонных (макроскопических) состояний в другой набор базисных (микроскопических) состояний безграничного Гильбертова пространства, а также обратное преобразование;

--- Развить новый математический аппарат $\alpha-$ представления неклассических состояний света в терминах перемещенных фотонных состояний с амплитудой перемещения α;

--- Развить теорию генерации трех-модового запутанного состояния света на выходе спонтанного параметрического преобразователя с учетом истощения волны накачки;

--- Рассмотреть новый подход реализации одно-кубитовых и двух-кубитовых преобразований на основе $\alpha-$представления;

--- Изучить новые подходы реализации протоколов квантовой информатики (протокол плотного кодирования, квантовая криптография) на основе нового $\alpha-$представления неклассических состояний света, ключевым моментом в данных протоколах является модуляция фотонных состояний амплитудой перемещения.

Научная новизна:

--- Предложено рассмотреть неклассические перемещенные фотонные состояния с большим значением амплитуды перемещения (макроскопические) в качестве ответа на фундаментальный вопрос современной физики применимости законов квантовой механики к макроскопическим объектам;

--- Построен математический аппарат точных матричных преобразований перемещенных фотонных состояний с отличными амплитудами перемещения, введено понятие $\alpha-$ представления произвольного состояния, разложение произвольного состояния в терминах перемещенных фотонных состояний с амплитудой перемещения α;

--- Получены точные аналитические выражения $\alpha-$ представления следующих состояний: суперпозиции когерентных состояний, двух-модового сжатого вакуума, суперпозиции вакуума и одного фотона;

--- Построена квантовая теория взаимодействия световых волн в кристалле с квадратичной нелинейностью с учетом истощения волны накачки;

--- Рассмотрен метод генерации произвольной (как четой, так не четной) суперпозиции когерентных состояний посредством извлечения двух, трех и четырех фотонных состояний из начальных сжатых когерентных состояний с отличными амплитудами, определены условия, при которых реализуется прямое действие матрицы Адамара на входных базисных состояниях;

--- В общем случае рассмотрен вопрос де-Гауссификации изначально Гауссового состояния посредством извлечения двух фотонов из начального состояния. определены

условия, при которых возможно аппроксимировать максимально неклассические состояния (суперпозиции когерентных состояний) сгенерированными фотон-извлеченными состояниями с наибольшей точностью;

--- Впервые предложен и исследован новый способ генерации неклассических состояний света посредством извлечения перемещенных фотонных состояний из одной части исходного коррелированного состояния, показана возможность реализации элементарных одно- и двух-кубитовых квантовых гейтов controlled-Z гейта и матрицы Адамара на гибридных состояниях;

--- Предложена и развита теория нового протокола плотного кодирования с перемещенными фотонными состояниями, предложено использовать по два состояния из отличных друг от друга Гильбертовых пространств перемещенных фотонных запутанных состояний для того, чтобы успешно закодировать и раскодировать посылаемые сообщения;

--- Развита теория нового протокола квантовой криптографии, в котором носителями информации являются не ортогональные перемещенные состояния, показано, что модуляция двух статистических смесей вакуума и единичного фотона амплитудой перемещения позволяет отправителю закодировать свою информацию, а получателю извлечь из них битовые значения.

Теоретическая и практическая значимость работы определяется тем, что предложен общий подход к исследованиям с неклассическими перемещенными (рассматриваемыми как макроскопические в случае большой амплитуды перемещения) фотонными состояниями и к использованию данных состояний для квантовой обработки информации. Известно, что большие объекты являются классическими. Одной из целей квантовой механики является расширение правил квантового мира на макроскопические объекты. Квантовые объекты с большим количеством частиц могут обладать свойствами отличными от классических, что может проявляться в их странном поведении не совместимым с известным. Известно, что эффект декогерентности является основным препятствием на пути создания больших квантовых объектов. Эффект декогерентности быстро разрушает зародившуюся квантовую систему из большого числа частиц, превращая ее в классический объект [12]. Можно сказать даже более, что эффект декогерентности является ответственным за различие в свойствах между квантовыми и классическими объектами.

В настоящее время предложено два подхода к реализации оптических квантовых компьютеров: KLM подход [13] и “one-way computer” метод [14]. Оба данных подхода базируются на первоначальной генерации запутанных состояний особого типа. Данные запутанные состояния состоят из большого количества частиц, каждая из которых связана с остальными достаточно сложным образом. Система квантовых частиц может быть подвержена большему влиянию эффекта декогерентности в силу того, что каждая частица вступает во взаимодействие с окружающей средой, усиливая общий эффект на начальное состояние. Поэтому сложные запутанные состояния [13, 14] могут преобразовываться в классические сразу же после их генерации. Эффект декогерентности не позволяет на практике реализовать квантовые операции, которые предложены в работах [13, 14]. Вполне возможно, что в будущем получится снизить влияние эффекта декогерентности на сгенерированные состояния. Но и обратная точка зрения, что никогда не получится избежать влияния эффекта декогерентности на большую систему квантовых частиц, имеет право на существование.

Тем не менее, возможно взглянуть на проблему системы быть одновременно большой и квантовой под другим углом, не увеличивая количество частиц квантовой системы, а рассматривая неклассические перемещенные версии фотонных состояний. Энергия неклассического перемещенного состояния увеличивается с увеличением амплитуды перемещения. Поэтому неклассические перемещенные фотонные состояния с большой амплитудой перемещения уже могут быть рассмотрены как макроскопические. Несмотря на то, что неклассическое перемещенное фотонное состояние является бесконечной суперпозицией других состояний, оно может быть рассмотрено как состояние одной единой частицы без учета ее внутренней структуры. Соответственно, к данным большим частицам применимы законы квантовой механики наравне с фотонными состояниями света. Развиваемый подход позволяет связать перемещенные фотонные состояния между собой, для того чтобы иметь возможность рассмотреть новые (макроскопические квантовые) эффекты.

Полученные результаты представляют интерес не только с фундаментальной точки зрения, но могут быть использованы для практической реализации предложенных протоколов квантовой информатики. Результаты работы показывают, что неклассические перемещенные фотонные (макроскопические) состояния могут быть использованы в квантовой информатике, наравне с микроскопическими состояниями. Теоретический подход к решению задач квантовой информатики может быть использован для дальнейшего развития одно и двух-кубитовых унитарных

преобразований на базе гибридных состояний и созданию блоков квантового компьютера, в котором носителями информации являются оптические кубиты. Результаты и выводы, полученные при рассмотрении протокола плотного кодирования и протокола квантовой криптографии с перемещенными фотонными состояниями, могут быть напрямую использованы на практике.

Положения, выносимые на защиту:

1. Развитие теории неклассических перемещенных фотонных состояний для квантовой обработки информации;
2. Общий метод преобразования между неклассическими перемещенными фотонными состояниями с отличными друг от друга амплитудами перемещения; введение понятия $\alpha-$ представления произвольного чистого состояния в терминах перемещенных фотонных состояний; аналитические выражения $\alpha-$ представления суперпозиции когерентных состояний, двух-модового сжатого вакуума и суперпозиции вакуума и одиночного фотона;
3. Точная квантовая теория параметрического преобразования в среде с квадратичной нелинейностью с учетом истощения волны накачки;
4. Общий метод реализации состояний и квантовых операций посредством извлечения перемещенных фотонных состояний; развитие теории генерации суперпозиции когерентных состояний (оптический аналог Шредингеровского состояния котов) большей амплитуды с высокой точностью; обобщение теории де-Гауссификации изначально Гауссового состояния;
5. Построение теории реализации элементарных одно- (матрица Адамара) и двух-кубитовых (controlled-Z) элементарных гейтов на базе $\alpha-$ представления;
6. Построение протокола плотного кодирования с перемещенными фотонными состояниями или Бэлловскими состояниями взятыми из разных базисных наборов с отличными амплитудами перемещения реализуется методами линейной оптики.
7. Развитие протокола квантовой криптографии с перемещенными не ортогональными состояниями для распределения секретного кода между отправителем и получателем.

Личный вклад автора заключается в выборе и постановке задач настоящего исследования, в выборе методов исследования, проведении аналитических и численных расчетов. В обсуждении результатов принимали участие соавторы: K. Kim (разделы 3.1, 3.2), J. Kim (разделы 4.2, 4.3, 5.2, 5.3), B. A. Nguyen (разделы 4.2 4.4). Обсуждение полученных результатов и выводы проводились совместно с соавторами.

Достоверность результатов обеспечивается корректным использованием аппарата квантовой механики, математических методов расчета, ясным физическим объяснением полученных результатов. Корректность полученных результатов проверена сравнением с ранее известными выводами и экспериментальными результатами.

Апробация работы. Материалы диссертационной работы докладывались на международных конференциях: ежегодная встреча Корейского физического общества в Республике Корея в 2004г., 5 международный семинар по атомной и молекулярной физики Южной Корее в 2006г., 2 совместная Азиатско-Тихоокеанской конференция и KIAS-KAISR семинар по квантовой информатике в Сеуле в 2007г., а также ежегодная встреча Корейского физического общества в Республике Корея в 2013г.

Публикации. Основное содержание диссертации базируется на результатах 32 научных статей, в том числе 31 статьи в рецензируемых журналах, рекомендованных ВАК для опубликования результатов диссертаций на соискание ученых степеней доктора и кандидата наук, а также в трудах перечисленных выше конференций и семинаров.

Структура и объем диссертации. Диссертация состоит из введения, шести глав, заключения и списка цитированной литературы, включающего 238 наименований. Полный объем диссертации 300 страниц, включая 53 рисунка и одну таблицу.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обусловлена актуальность выбранной темы, сформированы цели и задачи, приведены основные положения, выносимые на защиту и излагается краткое содержание диссертации по главам.

Глава 1 состоит из семи разделов и посвящена введению в основные понятия и идеи квантовой механики, квантовой оптики и квантовой информатики. В данной главе представлен обзор литературы по теме диссертации.

В разделе 1.1 кратко излагаются основные правила и базисные понятия кантовой механики, рассматриваются вопросы исторического развития квантовой информатики как попытка ответить на парадоксы квантовой механик. Показана структура квантовой информатики. Приведен обзор основных работ, которые дали толчок развитию

данному научному направлению. Даны ссылки на основные достижения квантовой информатики. Сжато определен круг задач, которые выбраны для анализа и обсуждения в данной работе и возможные методы их решения.

В разделе 1.2 вводится понятие квантового бита. Ключевым моментом введения понятие квантового бита (кубита) как основной единицы квантовой информации является определение суперпозиции состояний в Гильбертовом пространстве. Приводится пример введения квантового бита на примере квантовой частицы, которая одновременно находится в двух локализованных, разделенных друг от друга потенциальных ямах. На данном примере показаны основные правила поведения квантовой частицы и методы квантовых расчетов. На примере сферы Блоха показано отличие кубита от классического бита информации. Показано, что измерение квантового кубита разрушает исходное состояние в отличии от классического бита. Рассмотрено как кубит может эволюционировать со временем, в том числе трансформируясь в смешанное состояние под влиянием эффекта декогерентности.

В разделе 1.3 вводится одно из основных понятий квантовой информатики --- квантовая запутанность. Показано отличие запутанных состояний от раздельных.

В разделе 1.4 вводится понятие когерентного состояния и рассматриваются некоторые свойства данного состояния.

В разделе 1.5 вводится понятие когерентного кубита, состояния которое формируется из двух когерентных состояний света с равными по модулю, но противоположными по знаку амплитудами. Суперпозиции когерентных состояний являются оптическим аналогом Шредингеровских состояний котов. Рассмотрены основные свойства данных суперпозиций когерентных состояний. На примере функций Вигнера показано отличие суперпозиции когерентных состояний от когерентных состояний и их статистической смеси.

В разделе 1.6 вводится понятие запутанных когерентных состояний. Данные состояния формируют полный набор Бэлловских состояний. Рассмотрены основные свойства данных состояний.

В разделе 1.7 приведены доводы в обоснование выбора неклассических перемещенных состояний, в частности, когерентных кубитов, в качестве носителей информации. Рассмотрены направления основных усилий в последующих главах диссертации, направленные на реализацию квантовых протоколов с неклассическими перемещенными состояниями света.

Глава 2 состоит из пяти разделов и содержит результаты теоретического развития математического аппарата с неклассическими перемещенными фотонными состояниями света. В частности, фотонные состояния являются частным случаем перемещенных состояний с амплитудой перемещения равной нулю. Показано, что возможно рассматривать перемещенные фотонные состояния как состояния одной “большой” частицы без учета ее внутренней структурой, а также возможно воспользоваться ее разложением по базисным состояниям из выбранного набора. Вводится матрица преобразования из одного набора неклассических перемещенных состояний в другой базисный набор перемещенных состояний с отличным значением амплитуды перемещения. Представлен математический вывод матрицы преобразования. Рассматриваются физические следствия из данного преобразования, в частности, возможность разложения микроскопических состояний (состояния с меньшей энергией) в ряд по макроскопическим состояниям (состояния с большей энергией). Данное разложение имеет место в силу унитарности оператора перемещения. Показано как использование матрицы преобразования позволяет ввести понятие $\alpha-$ представления произвольного квантового состояния. Рассмотрен вопрос наблюдаемых для работы с $\alpha-$ представлением квантового состояния. Представлен вывод $\alpha-$ представления суперпозиции когерентных состояний (СКС). $\alpha-$ представление СКС положено в основу генерации данных состояний большой амплитуды посредством извлечения нескольких фотонов из изначально запутанного состояния света. Данный подход положен в основу теории реализации элементарных одно-кубитовых гейтов таких как матрица Адамара с когерентными базисными элементами.

В разделе 2.1 приведены общие сведения об унитарных матрицах, которые отвечают за одно-кубитовые преобразования кубитов. Показано, что одно-кубитовые преобразования могут быть реализованы несколькими способами. Представлены математические выражения, связывающие одно-кубитовые преобразования из различных наборов базисных унитарных матриц.

В разделе 2.2 представлен теоретический вывод матричного преобразования из одного базиса неклассических перемещенных фотонных состояний в другой базис с отличной амплитудой перемещения. В частности, получена следующая матрица преобразования макроскопического базиса (в случае больших значений амплитуды перемещения) в микроскопические базисные состояния

$$\begin{vmatrix} |0\rangle \\ |1\rangle \\ |2\rangle \\ |3\rangle \\ |4\rangle \\ |5\rangle \\ |6\rangle \\ \dots \\ |n\rangle \\ \dots \end{vmatrix} = U \begin{vmatrix} |0,\alpha\rangle \\ |1,\alpha\rangle \\ |2,\alpha\rangle \\ |3,\alpha\rangle \\ |4,\alpha\rangle \\ |5,\alpha\rangle \\ |6,\alpha\rangle \\ \dots \\ |n,\alpha\rangle \\ \dots \end{vmatrix} = \exp\left(-|\alpha|^2/2\right) \begin{vmatrix} c_{00} & c_{01} & c_{02} & c_{03} & c_{04} & c_{05} & c_{06} & \dots & c_{0m} & \dots \\ c_{10} & c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} & \dots & c_{1m} & \dots \\ c_{20} & c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} & \dots & c_{2m} & \dots \\ c_{30} & c_{31} & c_{32} & c_{33} & c_{34} & c_{35} & c_{36} & \dots & c_{3m} & \dots \\ c_{40} & c_{41} & c_{42} & c_{43} & c_{44} & c_{45} & c_{46} & \dots & c_{4m} & \dots \\ c_{50} & c_{51} & c_{52} & c_{53} & c_{54} & c_{55} & c_{56} & \dots & c_{5m} & \dots \\ c_{60} & c_{61} & c_{62} & c_{63} & c_{64} & c_{65} & c_{66} & \dots & c_{6m} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{n0} & c_{n1} & c_{n2} & c_{n3} & c_{n4} & c_{n5} & c_{n6} & \dots & c_{nm} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{vmatrix} \begin{vmatrix} |0,\alpha\rangle \\ |1,\alpha\rangle \\ |2,\alpha\rangle \\ |3,\alpha\rangle \\ |4,\alpha\rangle \\ |5,\alpha\rangle \\ |6,\alpha\rangle \\ \dots \\ |n,\alpha\rangle \\ \dots \end{vmatrix}$$

и обратное преобразование

$$\begin{vmatrix} |0,\alpha\rangle \\ |1,\alpha\rangle \\ |2,\alpha\rangle \\ |3,\alpha\rangle \\ |4,\alpha\rangle \\ |5,\alpha\rangle \\ |6,\alpha\rangle \\ \dots \\ |n,\alpha\rangle \\ \dots \end{vmatrix} = U^{-1} \begin{vmatrix} |0\rangle \\ |1\rangle \\ |2\rangle \\ |3\rangle \\ |4\rangle \\ |5\rangle \\ |6\rangle \\ \dots \\ |n\rangle \\ \dots \end{vmatrix} = \exp\left(-|\alpha|^2/2\right) \begin{vmatrix} c_{00}^* & c_{10}^* & c_{20}^* & c_{30}^* & c_{40}^* & c_{50}^* & c_{60}^* & \dots & c_{m0}^* & \dots \\ c_{01}^* & c_{11}^* & c_{21}^* & c_{31}^* & c_{41}^* & c_{51}^* & c_{61}^* & \dots & c_{m1}^* & \dots \\ c_{02}^* & c_{12}^* & c_{22}^* & c_{32}^* & c_{42}^* & c_{52}^* & c_{62}^* & \dots & c_{m2}^* & \dots \\ c_{03}^* & c_{13}^* & c_{23}^* & c_{33}^* & c_{43}^* & c_{53}^* & c_{63}^* & \dots & c_{m3}^* & \dots \\ c_{04}^* & c_{14}^* & c_{24}^* & c_{34}^* & c_{44}^* & c_{54}^* & c_{64}^* & \dots & c_{m4}^* & \dots \\ c_{05}^* & c_{15}^* & c_{25}^* & c_{35}^* & c_{45}^* & c_{55}^* & c_{65}^* & \dots & c_{m5}^* & \dots \\ c_{06}^* & c_{16}^* & c_{26}^* & c_{36}^* & c_{46}^* & c_{56}^* & c_{66}^* & \dots & c_{m6}^* & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{0n}^* & c_{1n}^* & c_{2n}^* & c_{3n}^* & c_{4n}^* & c_{5n}^* & c_{6n}^* & \dots & c_{mn}^* & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{vmatrix} \begin{vmatrix} |0\rangle \\ |1\rangle \\ |2\rangle \\ |3\rangle \\ |4\rangle \\ |5\rangle \\ |6\rangle \\ \dots \\ |n\rangle \\ \dots \end{vmatrix},$$

где некоторые матричные элементы имеют вид

$$c_{on}(\alpha) = \frac{(-1)^n \alpha^n}{\sqrt{n!}},$$

$$c_{10}(\alpha) = \alpha^*, \quad c_{1n}(\alpha) = \frac{(-1)^n \alpha^{n-1}}{\sqrt{n!}}\left(n - |\alpha|^2\right), \quad n \geq 1,$$

$$c_{20}(\alpha) = \frac{\alpha^{*2}}{\sqrt{2!}}, \; c_{21}(\alpha) = \frac{\alpha^*}{\sqrt{2!}}\left(2 - |\alpha|^2\right), \; c_{2n}(\alpha) = \frac{(-1)^{m-2}\alpha^{m-2}}{\sqrt{2!}\sqrt{n!}}\left(n(n-1) - 2n|\alpha|^2 + |\alpha|^4\right), \; n \geq 2.$$

Получены распределения фотонных состояний по перемещенным фотонными состояниям для различных значений амплитуды перемещения. Вводится понятие α – представления произвольного квантового состояния. α – представление --- это разложение состояния в базисе неклассических перемещенных фотонных состояний с амплитудой перемещения α. Детально представлен вывод аналитического выражения α – представление СКС. Предложено использовать усеченные волновые функции, чтобы аппроксимировать СКС большой амплитуды.

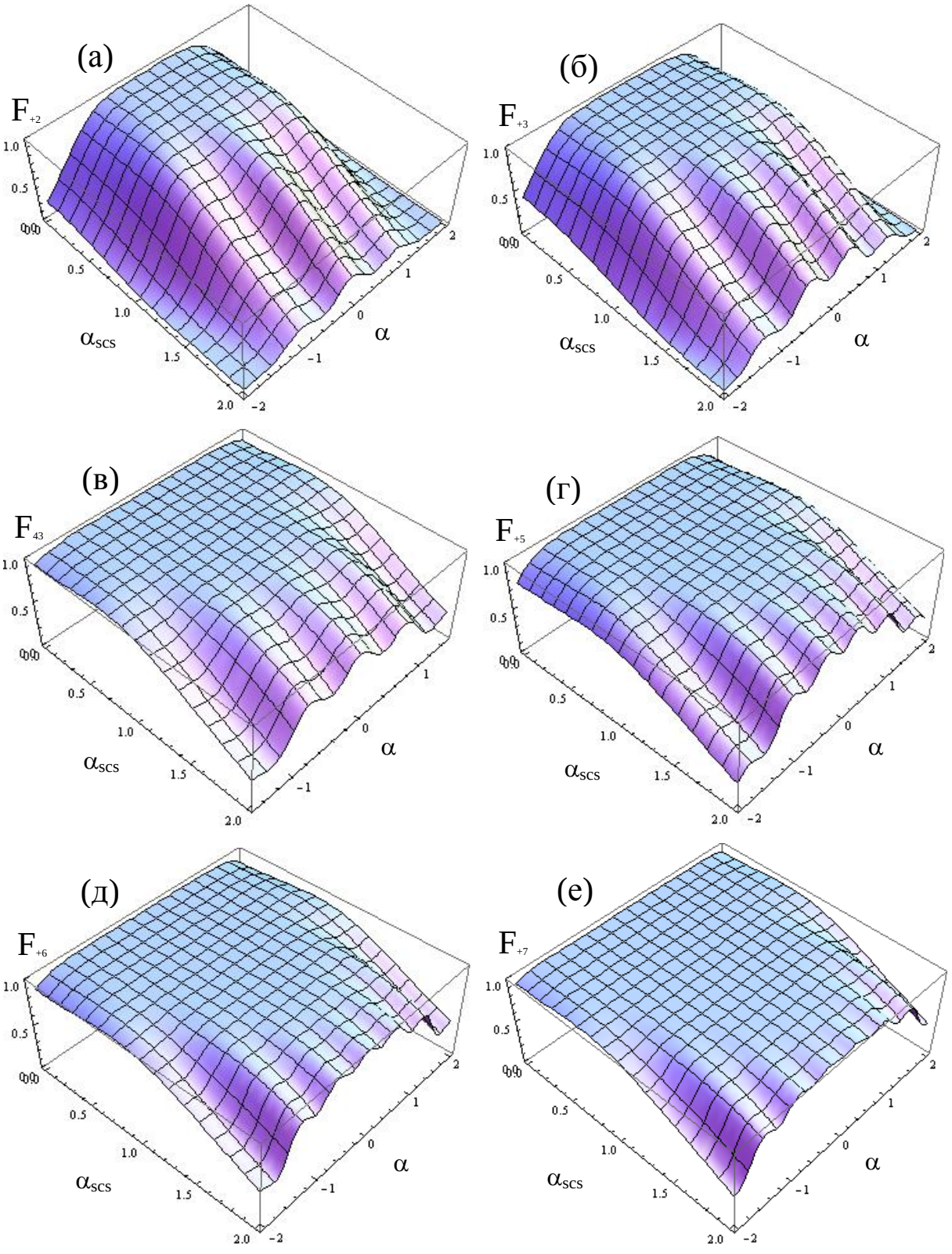

Рис. 1 График зависимости точности между четной СКС и ее усеченной суперпозицией с (а) $n=2$, (б) $n=3$, (в) $n=4$, (г) $n=5$, (д) $n=6$, (е) $n=7$ от амплитуды СКС α_{SCS} и амплитуды сдвига на фазовой плоскости α.

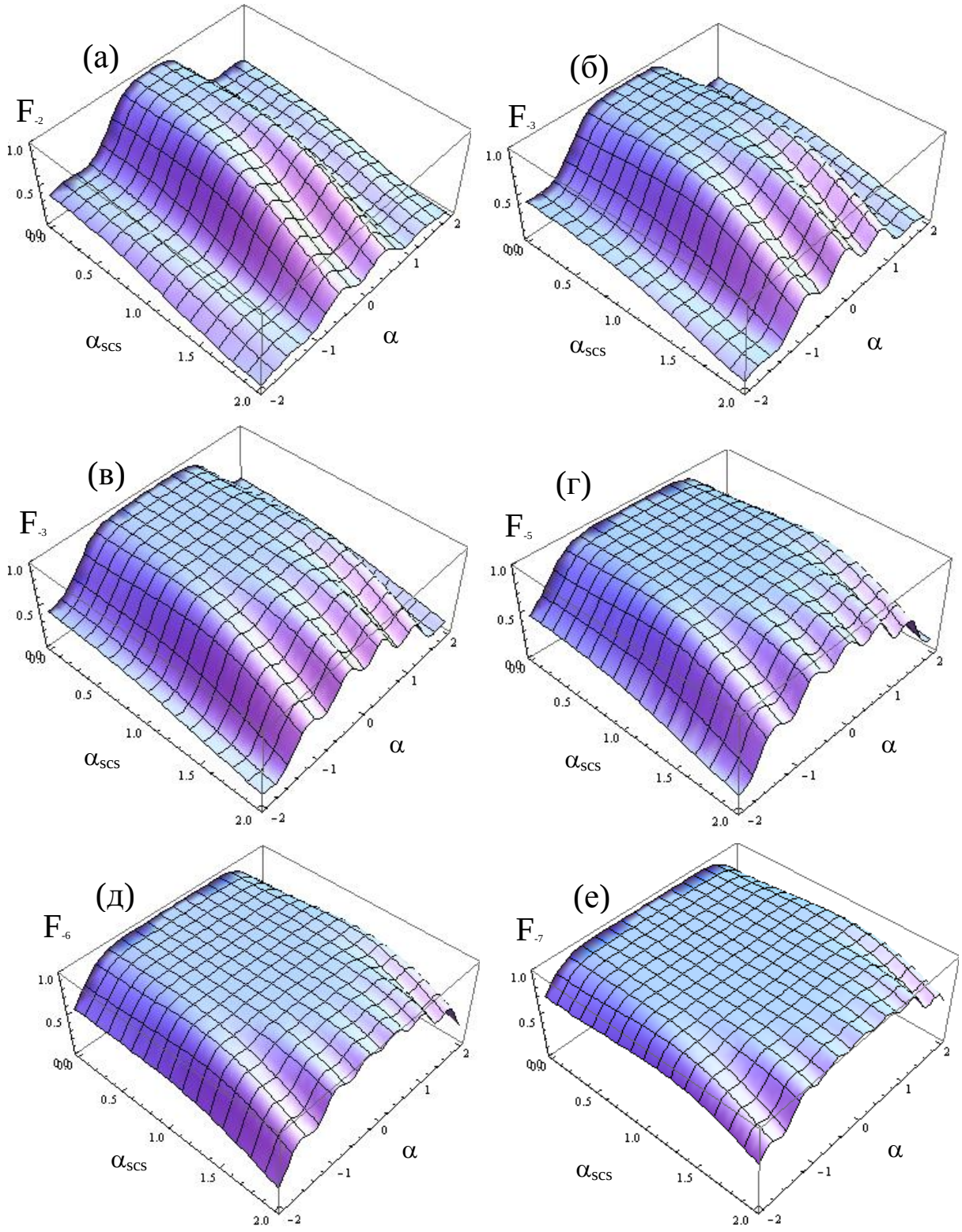

Рис. 2 График зависимости точности между не четной СКС и ее усеченной суперпозицией с (а) $n=2$, (б) $n=3$, (в) $n=4$, (г) $n=5$, (д) $n=6$, (е) $n=7$ от амплитуды СКС α_{SCS} и амплитуды сдвига на фазовой плоскости α.

Показано, что увеличение числа членов в усеченных состояниях гарантирует их высокую точность с суперпозициями когерентных состояний. Как показано на рисунках 1 и 2, высокая точность наблюдается при больших значениях амплитуды когерентных суперпозиций в широком диапазоне амплитуды сдвига α. Усеченные волновые функции с большим количеством членов могут быть использованы вместо суперпозиций когерентных состояний. Данные усеченные волновые функции также являются ортогональными в широком диапазоне значений также как и суперпозиции, которые они аппроксимируют.

В разделе 2.3 представлен метод генерации четной и не четной суперпозиции сжатых когерентных состояний из начальных сжатых когерентных состояний. Механизм извлечения нескольких фотонов из начальных состояний позволяет эффективно реализовать нелинейный эффект на исходных состояниях. Численно обнаружено, что если число извлеченных фотонов растет, то точность генерируемых суперпозиций увеличивается. Данный метод может быть использован для генерации оптического аналога Шредингеровских состояния котов большой амплитуды. Показана возможность реализовать прямое действие матрицы Адамара на используемых базисных состояниях при определенном выборе значений используемых параметров как это показано на рисунке 3.

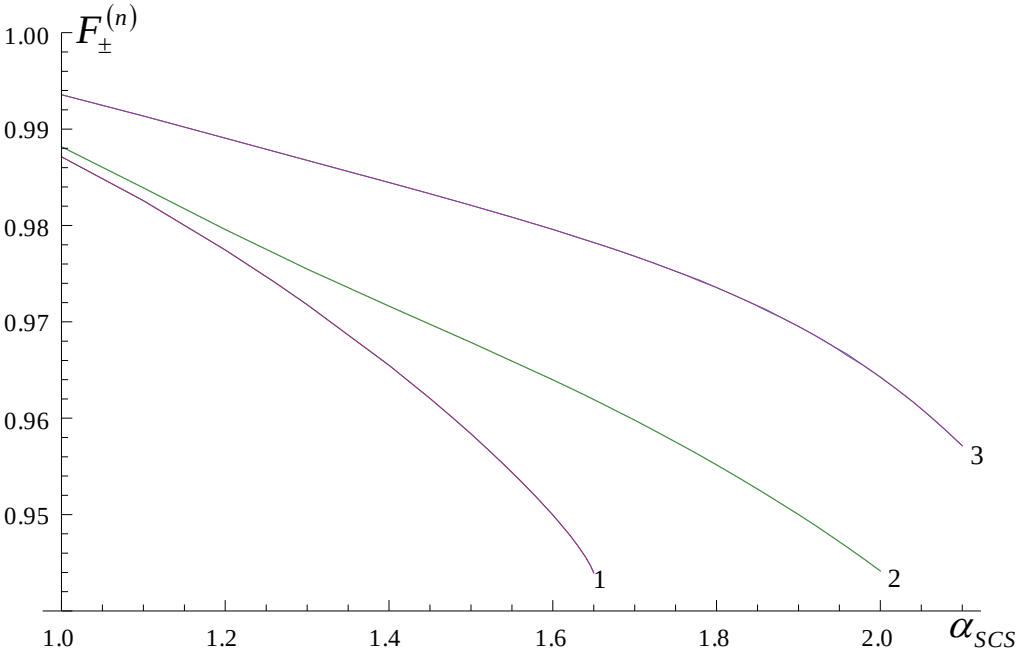

Рис. 3 График зависимости точности $F_{\pm}^{(n)}$ от амплитуды СКС состояний α_{SCS} для 2PSS (кривая 1), 3PSS (кривая 2) и 4PSS (кривая 4). Значения параметров выбраны таким образом, чтобы обеспечить равенство точностей $F_{+}^{(n)} = F_{-}^{(n)}$. Чем больше фотонов извлекается из начального пучка света, тем выше точность, с которой nPSS аппроксимируют выходные состояния гейта Адамара.

На основе развитого математического подхода рассмотрен вопрос детерминированного выполнения прямого действия матрицы Адамара на базисных элементах при условии, что некоторое состояние создано заранее. Данное состояние генерируется посредством извлечения нескольких фотонов из сжатого когерентного состояния. Показано, что проекционное измерение сгенерированного состояния на когерентные состояния с отличными амплитудами гарантирует генерацию как четной, так и не четной суперпозиции сжатых когерентных состояний с высокой точностью.

В разделе 2.4 представлены результаты теоретического исследования вопроса реализации прямого действия матрицы Адамара с когерентными состояниями с помощью последовательности операторов рождения и перемещения. Предложена оптическая схема, которая позволяет генерировать суперпозиции сжатых когерентных состояний из изначальных когерентных состояний.

В разделе 2.5 представлено обсуждение общих моментов, связанных с развиваемым методом извлечения фотонных состояний из начальных базисных. В частности, обсуждаются дальнейшие шаги по решению данной проблемы. Отмечено, что в рассматриваемом случае преобразование Адамара происходит между отличными двух-мерными Гильбертовыми пространствами. Кратно обсуждены пути решения обратного преобразования Адамара на выходных состояниях.

Глава 3 состоит из четырех разделов и содержат обобщающие результаты теоретического исследования извлечения некоторого числа фотонов из Гауссовых состояний света. Разработана теория де-Гауссификации изначально Гауссового состояния посредством извлечения некоторого числа фотонов. Получено точное выражение, связывающее точность генерируемого не Гауссового состояния с экспериментальными параметрами.

Представлен математический вывод аналитического выражения α – представления двух-модового сжатого вакуума и суперпозиции вакуума и единичного фотона. Предложен новый метод генерации неклассических состояний света посредством извлечения перемещенных фотонных состояний из начальных состояний. Вводится понятие гибридного состояния, которое формируется из когерентных состояний большой амплитуды (макроскопических) в одной из мод и суперпозиций вакуума и единичного фотона (микроскопическое состояние) в соседней моде коррелированного состояния. Результаты анализа положены в основу оптимальной реализации элементарных одно-кубитовых и двух-кубитовых преобразований с когерентными и гибридными состояниями. В частности, показана реализация controlled-Z гейта

преобразования Адамара (прямого и обратного) из одного двухмерного Гильбертова пространства в другое двухмерное Гильбертово пространство с отличными базисными состояниями.

В разделе 3.1 представлен математический аппарат Гауссовых и не Гауссовых состояний света. На основе функций Вигнера даны определения Гауссового и не Гауссового состояний, показано отличие данных состояний друг от друга. Рассмотрен математический аппарат характеристических функций и функций квази-распределения. Показано, что поведение Гауссовых состояний полностью определяется первыми и вторыми моментами распределения. Вторые моменты определяют корреляционные свойства состояния. Первые моменты (средние значения) могут в какой-то мере служить индикатором микроскопичности или макроскопичности состояния. Представлены примеры функций квази-распределения различных состояний.

Вводится понятие степени неклассичности произвольного состояния и приводятся примеры расчета степени неклассичности для Гауссовых и не Гауссовых состояний света. На основе мере неклассичности рассматривается деление состояний на классические и неклассические.

В разделе 3.2 представлена точная теория генерации суперпозиции когерентных состояний посредством извлечения из начального Гауссового состояния нескольких фотонов. Данные исследования являются обобщением и дальнейшим развитием результатов параграфа 2.3. Анализ выполнен на основе функций Вигнера. Разработана общая теория извлечения двух фотонов из изначально Гауссового состояния с учетом реальных значений параметров оптических приборов. Рассмотрено поведение сгенерированных не Гауссовых состояний в предельных случаях. Показано, что поведение сгенерированного не Гауссового состояния сильно определяется средними значениями (первыми моментами) изначально Гауссового состояния. Показано, что сгенерированное смешанное не Гауссовое состояние может быть аппроксимировано Гауссовыми состоянием в предельном случае больших значений первых моментов начального состояния. Таким образом, несмотря на применение изначально не Гауссовой операции (извлечение двух фотонов) к Гауссовому состоянию, выходное состояние асимптотически приближается к Гауссовому в случае больших значений первых моментов.

Получены соответствующие точные аналитические зависимости точностей генерируемых суперпозиций сжатых когерентных состояний от экспериментальных параметров. Данные сложные зависимости позволяют найти значение точности между

аппроксимирующими состояниями и суперпозициями при произвольных значениях экспериментальных параметров. Полученные результаты могут стать основой для реализации данных преобразований на практике. Представленный анализ и полученные графики позволяют подобрать оптимальный режим для выполнения экспериментальной работы по извлечению фотонных состояний из Гауссового состояния света. Анализ приспособлен для реализации прямого действия матрицы Адамара на базисных состояниях, как это показано на рисунке 4.

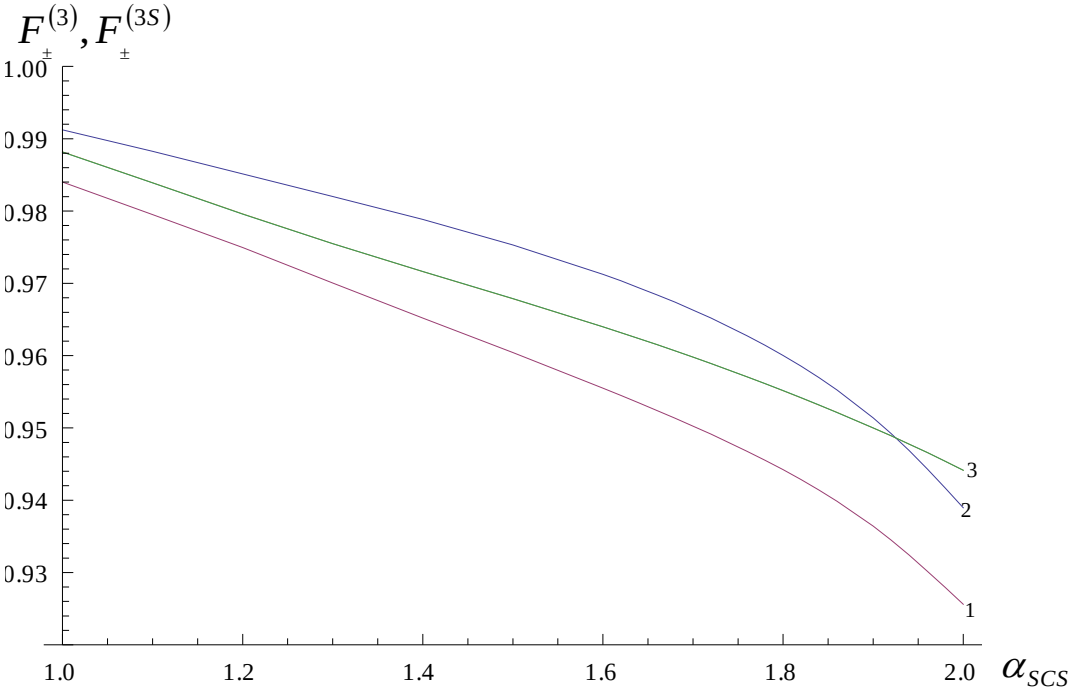

Рис. 4 Зависимость точностей между генерируемыми не Гауссовыми 3PSS состояниями и четной и не четной СПСКС от α_{SCS} в случае $Q = 0.03$, $\eta = 0.9$. Кривые 1 и 2 описывают $F_{-}^{(3)}$ и $F_{+}^{(3)}$, кривая 3 построена на основе упрощенной модели (кривая 2 на рисунке 2.10). Все остальные значения параметров для расчета кривых 1 и 2 взяты из результатов анализа оптической схемы на рисунке 2.9 на базе упрощенной модели. Наблюдается не большое различие значений точностей, полученных в реальной и упрощенных моделях.

Помимо своей экспериментальной направленности данных исследований, настоящий подход может стать основой для дальнейшего теоретического исследования с целью улучшения параметров выходных состояний и повышения качества элементов квантового компьютера.

В разделе 3.3 предложен новый подход к генерации неклассических состояний света. Данный метод основывается на извлечении перемещенного фотонного состояния света из начального состояния. Извлечение перемещенного фотонного состояния

является новым способом манипуляции выходными состояниями. Данный подход позволяет значительно увеличить возможности управления выходными состояниями света. Действительно, перемещенное фотонное состояние обладает дополнительной степенью свободы амплитудой перемещения, комплексной величиной которая может принимать произвольные значения. В случае нулевого значения амплитуды перемещения развиваемый метод становится обычным методом извлечения фотонных состояний. Таким образом, все результаты, проистекающие из теории извлечения фотонных состояний, могут быть получены из подхода с перемещенными фотонными состояниями, если выбрать значение амплитуды перемещения равной нулю. Показано как на практике выполнить извлечение перемещенного фотонного состояния с помощью пучкового делителя с почти единичной прозрачностью, вспомогательного когерентного состояния большой амплитуды и лавинного фотодетектора.

В рамках нового развиваемого метода получено точное аналитическое выражение $\alpha-$представления двух-модового сжатого вакуума

$$|\Psi\rangle_{12} = \left(\exp\left(-(\sinh r)^2\|\delta\|^2/2\right)/\cosh r\right)D_1\left(\alpha^*\tanh r\right)D_2(\alpha)$$

$$\sum_{n=0}^{\infty}\left((\tanh r)^n\left(a_1^+-\delta^*\right)^n|0\rangle_1/\sqrt{n!}\right)|n\rangle_2 = \qquad ,$$

$$\left(\exp\left(-(\sinh r)^2\|\delta\|^2/2\right)/\cosh r\right)D_1\left(\alpha^*\tanh r\right)D_2(\alpha)\sum_{n=0}^{\infty}(\tanh r)^n N_n|\Psi_n\rangle|n\rangle_2$$

где нормированное состояние $|\Psi_n\rangle$ имеет вид

$$|\Psi_n\rangle = A^{+n}|0\rangle/\left(N_n\sqrt{n!}\right) = (1/N_n)$$

$$\left(|n\rangle+\sum_{l=1}^{n}\left((-1)^l\delta^{*ll}\sqrt{n(n-1)(n-2)...(n-l+1)}/l!\right)|n-l\rangle\right),$$

$$A^+ = a^+ - \delta^*$$

оператор рождения перемещенного фотонного состояния с амплитудой перемещения δ и нормировочный множитель дается выражением

$$N_n = \left(1+\sum_{l=1}^{n}\frac{|\delta|^{2l}\,n(n-1)(n-2)...(n-l+1)}{|l|^2}\right)^{1/2}.$$

Рассмотрено соответствующее распределение неклассических перемещенных фотонных состояний в соседних модах двух-модового сжатого вакуума для различных значений амплитуды перемещения. Проекционное измерение на перемещенное n фотонное состояние позволяет сгенерировать в соседней коррелированной моде новое состояние. Данное сгенерированное состояние является результатом действия

оператора рождения перемещенного фотонного состояния с некоторой амплитудой δ, возведенного в n степень и действующего на вакуумное состояние.

Показана возможность генерации гибридного состояния, составленного из когерентных состояний и состояний вакуума и единичного фотона. Гибридное состояние является запутанным и формируется из базисных элементов отличных друг от друга двухмерных Гильбертовых пространств. Когерентные состояния с большими амплитудами перемещения одного из двух Гильбертовых пространств можно считать макроскопическими. Базисные элементы (вакуум и единичный фотон) другого Гильбертова пространства можно рассматривать как микроскопические. Предложена оптическая схема, которая приспособлена для генерации гибридного состояния посредством извлечения перемещенного единичного фотона из вспомогательного двух-модового сжатого вакуума. Приведено объяснение физического механизма, положенного в основу генерации гибридного состояния.

Предложено использовать данный механизм для реализации элементарных одно-кубитовых и двух-кубитовых гейтов ключевых блоков квантового компьютера. Показана возможность реализации двух-кубитовой операции controlled-Z гейта, где когерентные (макроскопические) состояния применяются в качестве управляющего кубита, а суперпозиции вакуума и единичного фотона используются в качестве управляемого кубита. Показано, что изначально микроскопический кубит находится в вспомогательном двух-модовом сжатом вакууме и извлечение перемещенного единичного фотона из данного состояния является движущей силой, которая генерирует выходное состояние controlled-Z гейта для используемых кубитов.

$$P_1(\pi)M_4^{(1)}B_{12}B_{13}B_{24}B_{12}^{"}\left(\left|\Psi_{ab}\left(\alpha t\sqrt{1+(\tanh s)^2}\,/r\right)\right\rangle_1|0\rangle_2 S(r)|00\rangle_{34}\right)\rightarrow$$
$$a|0,,\gamma\rangle_1\left(a_1|0\rangle_2+b_1|1\rangle_1\right)+b|0,-\gamma\rangle_1\left(-a_1|0\rangle_2+b_1|1\rangle_2\right)= \quad ,$$
$$aa_1|0,,\gamma\rangle_1|0\rangle_2+ab_1|0,,\gamma\rangle_1|1\rangle_2-ba_1|0,,-\gamma\rangle_1|0\rangle_2+bb_1|0,,-\gamma\rangle_1|1\rangle_2$$

где $M_4^{(1)}=\left(|1\rangle\langle 1|\right)_4$ --- проекционный оператор на состояние единичного фотона. Показано, что ключевым моментом успешной реализации controlled-Z гейта является тот факт, что вероятность зарегистрировать перемещенное фотонное состояние в двух-модовом сжатом состоянии не зависит от знака амплитуды перемещения.

Предложено использовать гибридные состояния для реализации прямого действия матрицы Адамара из одного двухмерного Гильбертова пространства когерентных состояний в другое двухмерное Гильбертово пространство гибридных состояний.

Выполнение прямого действия матрицы Адамара базируется на извлечении перемещенного единичного фотона из вспомогательного состояния двух-модового сжатого вакуума. Для выполнения обратного действия матрицы Адамара используется $\alpha-$ представление суперпозиции вакуума и единичного фотона. Получено $\alpha-$ представление суперпозиции вакуума и единичного фотона. Рассмотрены основные свойства распределения перемещенных фотонных состояний в суперпозициях вакуума и единичного фотона. Показано, что извлечение перемещенного единичного фотона из суперпозиционного состояния вакуума и единичного фотона позволяет сгенерировать состояние, соответствующего выходному состоянию обратного действия матрицы Адамара в выбранном базисе.

Предложен другой подход для реализации матрицы Адамара с отличными друг от друга двухмерными Гильбертовыми пространствами. Входное Гильбертово пространство --- это макроскопическое двухмерное пространство когерентных состояний с большими по модулю, но отличными по знаку, амплитудами. Выходное пространство --- это микроскопическое двухмерное Гильбертово состояние, в котором вакуум и единичный фотон являются базисными элементами. Показано, что реализация такого преобразования возможна в случае извлечения перемещенного фотонного состояния из вспомогательного и дополнительного измерения, определяющего четность числа фотонов. Обратное действие выполняется с помощью операторов сжатия.

Рассмотрена реализация данных протокола в реальной экспериментальной ситуации с учетом не совершенства измерительных детекторов. Показано как предложенная оптическая схема может работать с обычными лавинными фотодетекторами, а не со специальными счетчиками фотонов, которые могут распознавать число падающих на них фотонов. В настоящее время такие фотон-разрешающие детекторы света не производятся. Показано, что выбор соответствующего значения амплитуды перемещения двух-модового сжатого состояния позволяет использовать стандартные лавинные фотодетекторы. Точность генерируемых состояний приближается к идеальной единичной за счет того, что вероятность некоторых состояний преобладает в распределении двух-модового сжатого вакуума.

В разделе 3.4 рассмотрены и проанализированы некоторые протоколы квантовой информатики, базирующиеся на использовании неклассических состояний света. В частности, рассмотрены протокол квантовой телепортации перемещенных (макроскопических) фотонных состояний света с произвольной амплитудой

перемещения и протокол квантовой литографии с $2n$ запутанными фотонными состояниями света.

Глава 4 состоит из четырех разделов и содержит результаты развиваемой точной теории параметрического взаимодействия света с кристаллом с квадратичной нелинейностью. Ранее данный параметрический процесс рассматривается в приближении не истощаемой волны накачки. Данное допущение предполагает, что не значительная часть энергии волны накачки расходуется на генерацию новых фотонов в сигнальной и холостой модах. Это равносильно предположению, что энергия волны накачки остается неизменной в процессе рассеяния. Данное допущение позволяет иметь дело с двух-модовым (одно-модовым) сжатым вакуумным состоянием. В данном приближении принимается в рассмотрение только превращение фотона накачки в два фотона с меньшей энергией. Обратный процесс преобразования фотонов в сигнальной и холостой модах в один фотон накачки не учитывается.

Тем не менее, стоит принять во внимание истощение волны накачки в случае увеличения коэффициента параметрического преобразования. Трех-модовая теория взаимодействия с кристаллом с квадратичной нелинейностью с учетом истощения волны накачки развита в Шредингеровском представлении. Развиваемая точная теория учитывает как прямой процесс превращения фотона накачки в сигнальный и холостой фотоны, так и одновременный обратный процесс преобразования генерируемых фотонов в фотон накачки. Результатом данной теории является новое трех-модовое запутанное состояние света. Свойства данного состояния изучены. Найдены интересные применения данного состояния для обусловленной генерации некоторых запутанных состояний. Предложена и проанализирована оптическая схема, в которой измерение фотона накачки, позволяет сгенерировать чистое запутанное двух-модовое состояние света.

В разделе 4.1 представлен анализ уже известных результатов по спонтанному параметрическому рассеянию света. Внимание уделено классическому рассмотрению параметрического спонтанного рассеяния. Определен круг задач, которые уже решались, и задачи, точное решение которых может привести к предсказанию новых квантовых эффектов. Представлены основные выводы из уже решенных задач.

В разделе 4.2 представлены результаты точной квантовой теории параметрического рассеяния света в среде с квадратичной нелинейностью. Рассмотрена трех-модовая (сигнальная, холостая и накачивающая моды) модель взаимодействия световых волн в кристалле с квадратичной нелинейностью. Анализ данной модели

представлен в Шредингеровском представлении. Данная модель учитывает как генерацию фотонов в сигнальной и холостой модах из фотона накачки, так и обратный одновременный процесс генерации фотона накачки из двух рожденных фотонов в других двух модах. В данной модели учитывается также наличие дополнительных начальных фотонов в одной из двух вспомогательных волн. Показано, что используемая модель позволяет перейти к системе линейных дифференциальных уравнений для волновых амплитуд. Система дифференциальных уравнений решена посредством разложения волновых амплитуд трех-модового состояния в ряд по малому значению коэффициента взаимодействия световых волн на квадратичной нелинейности. Показано, что использование асимптотического разложения волновых амплитуд позволяет представить выходное запутанное трех-модовое состояние в компактном виде. Данная форма представляет неограниченную сумму тензорных произведений фотонных состояний в сигнальной и холостой модах и некоторого состояния в накачивающей моде.

$$\left|\Psi_{Out}\right\rangle = \sum_{n=0}^{\infty} (\alpha\eta)^n \left|n\right\rangle_1 \left|n\right\rangle_2 \left|\Phi_n^{(00)}\right\rangle$$

где волновые функции $\left|\Phi_n^{(00)}\right\rangle_p$ в накачивающей моде определяются следующими бесконечными суперпозициями фотонных состояний

$$\left|\Phi_n^{(00)}\right\rangle_p \equiv \left|\Phi_n^{(00)}(\alpha,\eta)\right\rangle_p = \exp\left(-\alpha^2/2\right)\sum_{l=0}^{\infty} \frac{\alpha^{l+n}}{\sqrt{(l+n)!}} f_{2(l+n),n+1}^{(00)}(\eta)\left|l\right\rangle_p .$$

В выражении для волновых функций присутствуют величины $f_{2l,k}^{(00)}(\eta) \equiv f_{2l,k}^{(00)}(\eta,\tau=1)$ ($k = 1,2,...,l+1$ и $l \in [0,\infty)$), которые удовлетворяют набору из $l+1$ линейных дифференциальных уравнений

$$\frac{df_{2l,k}^{(00)}(\eta,\tau)}{d\tau} = \eta\left((k-1)\sqrt{l-k+2}\, f_{2l,k-1}^{(00)}(\eta,\tau) - k\sqrt{l-k+1}\, f_{2l,k+1}^{(00)}(\eta,\tau)\right),$$

Использование нулевого приближения асимптотического разложения амплитуды разложения позволяет получить на выходе состояние двух-модового сжатого вакуума с когерентным состоянием в накачивающей моде. Показано, что использование следующих членов амплитуды разложения волновых амплитуд позволяет расширить анализ, чтобы иметь дело с более точными волновыми функциями в накачивающей моде. Рассмотрены отличные начальные условия для данной трех-модовой модели. Рассмотрены различные оптические схемы для генерации модовых состояний в

сигнальной и холостой модах. Показана возможность обусловленной генерации макроскопических запутанных состояний.

В разделе 4.3 представлены результаты практического применения трех-модового запутанного состояния для обусловленной генерации максимально запутанного модового состояния двух фотонов. Для обусловленной генерации используется нелинейный интерферометр Маха-Цендера, в двух модах которого находятся два кристалла с квадратичной нелинейностью. Взаимодействие волн накачки с кристаллами генерирует новые фотоны в сигнальной и холостой модах Показано, что генерация двух-фотонного четырех-модового максимального запутанного состояния происходит после регистрации одного фотона в моде накачки.

В разделе 4.4 представлен обзор разнообразного применения трех-модового запутанного состояния, в частности, для генерации максимально запутанных состояний большой амплитуды (макроскопические состояния).

Глава 5 состоит из двух разделов и содержат результаты теоретического исследования протокола плотного кодирования с перемещенными фотонными состояниями света. Особое внимание уделено физическому пониманию отличия данного протокола от протокола плотного кодирования, основанного на четырех Бэлловских состояниях из одного Гильбертова пространства. Показано, что протокол плотного кодирования с перемещенными фотонными состояниями может быть реализован методами линейной оптики. В качестве квантового канала выступает перемещенное состояние, которое уже реализовано на практике. Изучено влияние декогерентности на количество информации, передаваемое одной перемещенной частицей.

В разделе 5.1 дано введение в теорию двух родственных протоколов квантовой информатики: протокола квантовой телепортации не известного состояния и протокола плотного кодирования информации. Рассмотрены общие черты и различия данных протоколов. Дан обзор известных результатов. Рассмотрены вопросы практической реализации протоколов квантовой телепортации и плотного кодирования информации.

В разделе 5.2 приводится теория плотного кодирования с перемещенными фотонными состояниями света. Показано, что если вместо четырех Бэлловских состояний света из одного Гильбертова пространства выбрать две пары из отличных Гильбертовых пространств, то это дает возможность отправителю закодировать все свои сообщения, а получателю успешно их раскодировать методами линейной оптики. Данные наборы базисных Бэлловских состояний отличаются друг от друга амплитудой

перемещения в одной из коррелированных мод. Показано как отправитель может успешно закодировать свою частицу, а так же как получатель может успешно раскодировать посланное ему двух-битовое значение. Рассчитано количество взаимной информации, распределенной между отправителем и получателем, на одну передаваемую перемещенную частицу. В качестве носителей информации выступают перемещенные состояния. Ключевой момент протокола плотного кодирования с перемещенными состояниями --- это возможность распознать измерительные исходы всех четырех Белловских состояний из отличных друг от друга Гильбертовых пространств с отличными амплитудами перемещения. Как известно в “классическом” протоколе плотного кодирования [5] не удается распознать измерительные исходы всех четырех Бэлловских состояний из одного Гильбертова пространства методами линейной оптики.

Предложено использовать дополнительное состояние в протоколе плотного кодирования с перемещенными состояниями, чтобы увеличить скорость передачи информации до $\log_2 5$ на одну частицу. Показано, что дополнительное состояние имеет свой отличный от остальных измерительный исход, который получатель может распознать. Соответственно, отправитель также может закодировать свое дополнительное битовое значение через данное состояние методами линейной оптики. Данное обстоятельство позволяет увеличить емкость передающего канала. Доказано, что увеличение амплитуды перемещения ведет к быстрому достижению предельной скорости передачи информации на одну перемещенную частицу. Скорость передачи информации асимптотически быстро стремится к своему предельному значению с увеличением амплитуды перемещения частицы.

Рассмотрено влияние эффекта декогерентности на скорость передачи битов в протоколе плотного кодирования с перемещенными состояниями. Рассмотрена модельная задача влияния уменьшения амплитуды перемещения (амплитудное затухание) по мере распространения оптических импульсов по каналу связи на скорость передачи информации. Показано, что амплитудное затухание ведет к уменьшению асимптотически предельной скорости передачи информации. Тем не мене продемонстрировано, что протокол плотного кодирования может работать даже при больших значениях амплитудного затухания. Протокол плотного кодирования имеет сильную сопротивляемость к амплитудному затуханию. В конце параграфа очерчен круг подобных задач, которые являются перспективными в плане их реализации с

перемещенными фотонными состояниями и отмечены возможные пути их решения с целью увеличения скорости каналов связи на базе квантовых законов.

Глава 6 состоит из четырех разделов, в которых представлены результаты теоретического анализа нового протокола квантовой криптографии, базирующегося на использовании не ортогональных перемещенных фотонных состояний света. Детально обсуждены основные идеи протокола квантовой криптографии с перемещенными фотонными состояниями, рассмотрены его основные преимущества и отличие от уже известных протоколов. Рассмотрен вопрос реализации данного протокола на практике. Рассмотрены несколько вариантов попыток найти уязвимые места данного протокола. Показано, что не доброжелатель либо обнаруживается в результате нарушения статистики сигналов либо получает доступ к не значительной части кода, что не позволит ему раскодировать пересылаемые сообщения.

В разделе 6.1 изложены основные идеи, положенные в основу протоколов квантовой криптографии. Рассмотрены основные типы известных протоколов и отмечен прогресс, сделанный в квантовой криптографии за последнее время.

В разделе 6.2 представлены результаты теоретического исследования протокола квантовой криптографии на перемещенных фотонных состояниях света. Показано, что ключевым моментом протокола квантовой криптографии с перемещенными фотонными состояниями является модуляция статистической смеси вакуума и единичного фотона дополнительной амплитудой перемещения. Наложение амплитуды перемещения позволяет отправителю отсылать отличные друг от друга импульсы света, а получателю получать из них битовые значения секретного кода. Помимо состояний, которые могут нести битовые значения, отправитель отправляет также импульсы приманки, из которых невозможно извлечь битовое значение. Кроме того, состояния, которые могут нести битовое значение, могут давать измерительный исход, который не отличим от исхода импульса приманки. Показано, что такое решение позволяет успешно распределить секретный код между получателем и отправителем. Попытки недоброжелателя получить не санкционированный доступ к коду ведут к нарушению статистики выходных сигналов, что может быть обнаружено участниками протокола. Показано, что спонтанный параметрический конвертор, который выдает на выходе единичный фотон с примесью вакуума при регистрации другого фотона в соседней коррелированной моде, является естественным и идеальным источником носителей информации. В данном протоколе используются импульсы света как и других протоколах, широко обсуждаемых в научной литературе.

В разделе 6.3 представлены результаты теоретического анализа широкого спектра приемов (5 атак), которые может применить не доброжелатель для того, чтобы получить не санкционированный доступ к секретному коду. Показано, что во всех случаях имеет место либо нарушение статистики выходных сигналов между отправителем и получателем по сравнению со случаем отсутствия помех на линии связи, либо злоумышленник получает значительно меньшее количество информации о секретном коде, что едва ли позволит ему впоследствии воспользоваться им в расшифровке сообщений. На основе проведенного анализа можно допустить, что данный протокол будет устойчив и к другим стратегиям взлома.

В разделе 6.4 проводится сравнительный анализ протокола квантовой криптографии с перемещенными фотонными состояниями с уже известными протоколами. Обсуждаются отличительные черты и преимущества данного протокола. Намечен круг задач, анализ которых может стать полезным для практической реализации данного протокола.

В заключении сформулированы основные результаты диссертационной работы.

ЗАКЛЮЧЕНИЕ

1. Полностью разработан математический аппарат матричного преобразования из одного бесконечного набора базиса перемещенных фотонных состояний в другой с отличной амплитудой перемещения. Получены как прямая, так и обратная матрицы преобразования между отличными базисными наборами перемещенных фотонных состояний. Введено понятие $\alpha-$ представления для произвольного квантового состояния.

2. Получены точные аналитические выражения $\alpha-$представления как четной, так и не четной суперпозиции когерентных состояний. Представлен математический вывод $\alpha-$ представления двух-модового сжатого вакуума и суперпозиции вакуума и единичного фотона.

3. Рассмотрен вопрос реализации матрицы Адамара для базисных элементов посредством извлечения фотоном из начальных состояний света. В качестве входных и выходных базисных состояний выбраны состояния из отличных друг от друга двухмерных Гильбертовых пространств. Показано, что метод извлечения фотонов позволяет сгенерировать состояния, которые с высокой точностью аппроксимируют точные суперпозиции выходного Гильбертова пространства. Обнаружено, что чем

больше фотонов извлекается из начальных состояний, тем выше точность генерируемого выходного состояния.

4. Представлен полный теоретический анализ трансформации Гауссовых состояний света в не Гауссовые посредством извлечения двух и трех фотонов из начальных состояний света. Показано, что поведение сгенерированного не Гауссового состояния сильно зависит от значений первых моментов начального Гауссового состояния, которые в некоторой мере могут определять степень макроскопичности этого состояния. Получены точные аналитические зависимости точностей генерируемых суперпозиций сжатых когерентных состояний от экспериментальных параметров. Найден оптимальный режим для выполнения экспериментальной работы по извлечению фотонных состояний с целью реализации прямого действия матрицы Адамара на когерентных базисных состояниях.

5. Рассмотрены протоколы с модовыми состояниями света. Рассмотрены протоколы квантовой литографии, протокол controlled-Z гейта и протокол телепортации запутанного состояния света с фотон-модовыми состояниями света.

6. Предложен новый метод генерации выходных состояний посредством извлечения перемещенного единичного фотона как из состояния двух-модового сжатого вакуума, так и из суперпозиции вакуума и единичного фотона. Метод извлечения перемещенного фотонного состояния положен в основу реализации матрицы Адамара и двух-кубитовой операции controlled-Z гейта. Показано, что извлечение единичного фотона из вспомогательного состояния сжатого двух-модвого вакуума позволяет сгенерировать выходное состояние controlled-Z гейта. Показано, что выходное состояние controlled-Z гейта является гибридным, составленым из состояний разной физической природы: макроскопических (когерентные состояния большой амплитуды) и микроскопических (суперпозиции вакуума и единичного фотона) состояний.

7. Показана возможность реализации преобразования Адамара на когерентных и гибридных состояниях. Двух-мерное Гильбертово пространство с когерентными состояниями большой амплитуды является входным, а двух-мерное Гильбертово пространство с гибридными состояниями в качестве базисных элементов является выходным. Показано, что извлечение перемещенного единичного фотона из вспомогательного двух-модового сжатого вакуума позволяет реализовать прямое действие матрицы Адамара, а извлечение перемещенного единичного фотона из гибридного состояния дает возможность выполнить обратное действие матрицы Адамара.

8. Рассмотрена возможность реализации квантовых блоков в реалистическом сценарии. Показано, что генерация гибридных состояний, выходных состояний controlled-Z гейта и прямого действия матрицы Адамара с когерентными и гибридными состояниями осуществляется с единичной точностью и с высокой вероятностью успеха. Выбор соответствующего значения параметра перемещения позволяет провести реализацию рассматриваемых преобразований в условиях, приближающихся к идеальным.

9. Развита трех-модовая теория взаимодействия световых полей с кристаллом с квадратичной нелинейностью с учетом истощения волны накачки в Шредингеровском представлении. Развиваемая точная теория учитывает как прямой процесс превращения фотона накачки в сигнальный и холостой фотоны, так и одновременный обратный процесс преобразования генерируемых фотонов в фотон накачки. Результатом данной теории является новое трех-модовое запутанное состояние света. Свойства данного состояния изучены. Представлены результаты практического применения трех-модового запутанного состояния для обусловленной генерации максимально запутанного четырех-модового состояния двух фотонов.

10. Предложен новый протокол плотного кодирования информации, основанный на использовании перемещенных фотонных состояний света. В предложенном протоколе плотного кодирования используются по два состояния из двух наборов Бэлловских состояний с отличной амплитудой перемещения в одной из мод запутанных состояний. Доказано, что именно такой выбор состояний позволяет как закодировать пересылаемую информацию, так и успешно раскодировать ее на выходе. Показано как реализовать процесс кодирования и раскодирования информации методами линейной оптики такими как пучковый делитель, фазо-сдвигающий оптический элемент и лавинные фотодетекторы. Показано, что увеличение амплитуды перемещения используемого квантового канала позволяет передать $\log_2 5$ бита информации посредством пересылки одной перемещенной частицы. Рассмотрен вопрос влияния эффекта декогерентности на реализацию данного протокола. Показано, что протокол плотного кодирования с перемещенными состояниями света обладает сильной сопротивляемостью к влиянию эффекта декогерентности. Амплитудное затухание ведет только к уменьшению количества взаимной информации между получателем и отправителем.

11. Предложен новый протокол квантового кодирования, основанный на использовании перемещенных фотонных состояний света. Ключевым моментом данного протокола является модуляция вакуума и единичного фотона с целью создать из них

перемещенные состояния. Именно амплитуда перемещения перемещенных состояний позволяет как декодировать сигналы, так и извлечь информацию из пересылаемых импульсов. Исследуемый протокол квантовой криптографии является обобщением известного протокола B92 с не ортогональными состояниями с использованием импульсов приманок Показано, что спонтанный параметрический конвертор, который выдает на выходе единичный фотон с примесью вакуума при регистрации другого фотона в соседней коррелированной моде, является естественным и идеальным источником носителей информации. Показано, что протокол квантовой криптографии с перемещенными фотонными состояниями сохраняет свою не уязвимость в случае пяти изощренных стратегий взлома. Можно допустить, что данный протокол будет устойчив и к другим стратегиям взлома.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ

I. Статьи в журналах, рекомендованных ВАК для опубликования результатов диссертационной работы

1. Podoshvedov, S.A. Generation of correlated squeezing in nonlinear coupler / S.A. Podoshvedov, J.W. Noh, K. Kim // Optics Communications. – 2002. – Vol. 212, № 1-3. – pp. 115–126.
2. Podoshvedov, S.A. Quantum variances in field modes of parametric down converter / S.A. Podoshvedov, J.W. Noh, K. Kim // Optics Communications. – 2003. – Vol. 221, № 1-3. – pp. 121–133..
3. Podoshvedov, S.A. Stimulated parametric down conversion and generation of four-path polarization-entangled states / S.A. Podoshvedov, J.W. Noh, K. Kim // Optics Communications. – 2004. – Vol. 232, № 1-3. – pp. 357–369.
4. Podoshvedov, S.A. Influence of induced parametric down conversion on coincidence detection probability / S.A. Podoshvedov, J.W. Noh, K. Kim // Journal of the Korean Physical Society (JKFS). – 2004. – Vol. 44, № 2. – pp. 276–287.
5. Podoshvedov, S.A. Controlled sign gate through mode entangled states / S.A. Podoshvedov // J. Opt. B: Quantum Semiclass. Optics. – 2004. – Vol. 6, – pp. 549–554.
6. Podoshvedov, S.A. Quantum teleportation of entanglement via quantum channel constructed from mode entangled states / S.A. Podoshvedov // Optics Communications. – 2005. – Vol. 249, № 1-3. – pp. 245–253.
7. Podoshvedov, S.A. Controlled sign gate via modified GHZ mode entangled state / S.A. Podoshvedov // Optics Communications. – 2005. – Vol. 249, № 1-3. – pp. 239–244.
8. Podoshvedov, S.A. Quantum teleportation of entanglement using four-particle entangled states / S.A. Podoshvedov // Письма в ЖЭТФ. – 2005. – Т. 81, № 4. – С. 233–237.
9. Podoshvedov, S.A. Theoretical consideration of use of mode entangled states to beat minimal period of interference pattern / S.A. Podoshvedov // J. Opt. B: Quantum Semiclass. Optics. – 2005. – Vol. 7, № 9. – pp. 300–307.

10. Podoshvedov, S.A. Generation of two-photon KLM quantum channel / S.A. Podoshvedov // Письма в ЖЭТФ. – 2005. – Т. 82, № 7. – С. 513–517.
11. Podoshvedov, S.A. Conditional preparation of $\chi^{(2)}$ macroscopic entangled states / S.A. Podoshvedov // ЖЭТФ. – 2006. – Т. 129, № 4. – С. 615–624.
12. Podoshvedov, S.A. Generation of macroscopic entangled states by means of $\chi^{(2)}$ nonlinearity without photon number resolving detection / S.A. Podoshvedov // Письма в ЖЭТФ. – 2006. – Т. 83, № 8. – С. 420–424.
13. Podoshvedov, S.A. A simple scheme with coupled down converters with type-I phase matching as resource for conditional preparation of macroscopic entangled states / S.A. Podoshvedov, B. A. Nguyen, and J. Kim // Journal of Modern Optics. – 2006. – Vol. 53, № 13. – pp. 1853-1865.
14. Podoshvedov, S.A. Source for macroscopic entangled states / S.A. Podoshvedov // Physics Letters A. – 2006. – Vol. 357, № 6. – pp. 424-432.
15. Podoshvedov, S.A. Testing quantum mechanics against macroscopic realism using output of $\chi^{(2)}$ nonlinearity / S.A. Podoshvedov, J. Kim // Physical Review A. – 2006. – Vol. 74, – pp. 033810-1-033810-11.
16. Podoshvedov, S.A. A simple scheme for conditional generation of macroscopic entangled states using $\chi^{(2)}$ nonlinearity / S.A. Podoshvedov, B.A. Nguyen, J. Kim // Optics Communications. – 2007. – Vol. 270, № 2. – pp. 290-295.
17. Podoshvedov, S.A. Modified non-classical coherent state: squeezing, antibunching, sub-Poissonian photon statistics, realization scheme using $\chi^{(2)}$ nonlinearity, generation of macroscopic entangled state / S.A. Podoshvedov // ЖЭТФ. – 2007. – Т. 131, № 4. – С. 615–626.
18. Podoshvedov, S.A. A nonlinear $\chi^{(2)}$ Mach-Zehnder interferometer: conditional preparation of maximal microscopic entanglement / S.A. Podoshvedov, J. Kim // Physical Review A. – 2007. – Vol. 75, – pp. 032346-1-.032346-7.
19. Podoshvedov, S.A. Quantum teleportation through an entangled state composed of displaced vacuum and single-photon states / S.A. Podoshvedov // ЖЭТФ. – 2008. – Т. 133, № 3. – С. 505–517.
20. Podoshvedov, S.A. Dense coding by means of displaced photon / S.A. Podoshvedov, J. Kim // Physical Review A. – 2008. – Vol. 77, – pp. 032319-1-.032319-6.

21. Podoshvedov, S.A. Generation of a displaced qubit and entangled displaced photon state via conditional measurement and their properties / S.A. Podoshvedov, J. Kim, and J. Lee // Optics Communications. – 2008. – Vol. 281, № 14. – pp. 3748–3754.
22. Podoshvedov, S.A. Displaced photon states as resource for dense coding / S.A. Podoshvedov // Physical Review A. – 2009. – Vol. 79, – pp. 012319-1-.012319-6.
23. Podoshvedov, S.A. Performance of a quantum key distribution with dual-rail displaced photon states / S.A. Podoshvedov // ЖЭТФ. – 2010. – Т. 137, № 4. – С. 656–669.
24. Podoshvedov, S.A. Engineering of Schrödinger cat states by sequence of displacements, photon additions and subtractions / S.A. Podoshvedov // ЖЭТФ. – 2011. – Т. 139, № 4. – С. 636–648.
25. Podoshvedov, S.A. Generation of displaced squeezed superpositions of coherent states / S.A. Podoshvedov // ЖЭТФ. – 2012. – Т. 141, № 3. – С. 515–528.
26. Podoshvedov, S.A. Displaced rotations of coherent states / S.A. Podoshvedov // Quantum Information Processing (QINP). – 2012. – Vol. 11, № 6. – pp. 1809-1828.
27. Podoshvedov, S.A. Schemes for performance of displacing Hadamard gate with coherent states / S.A. Podoshvedov // Optics Communications. – 2012. – Vol. 285, № 18. – pp. 3896-3906.
28. Podoshvedov, S.A. Single qubit operations with base squeezed coherent states / S.A. Podoshvedov // Optics Communications. – 2013. – Vol. 290. – pp. 192–201.
29. Podoshvedov, S.A. Building of one-way Hadamard gate for squeezed coherent states / S.A. Podoshvedov // Physical Review A. – 2013. – Vol. 87, – pp. 012307-1-.012307-10.
30. Podoshvedov, S.A. Elementary quantum gates with Gaussian states / S.A. Podoshvedov // Quantum Information Processing (QINP). – 2014. – Vol. 13, № 8. – pp. 1723–1749.
31. Podoshvedov, S.A. Extraction of displaced number state / S.A. Podoshvedov // JOSA B. – 2014. – Vol. 31, № 10. – pp. 2491–2503.

I. Статьи в других журналах

32. Podoshvedov, S.A. Representation in terms of displaced number states and realization of elementary linear operators based on it / S.A. Podoshvedov // quant-ph arXiv:1501.05460. – 2015.

СПИСОК ЛИТЕРАТУРЫ

1. Feynman, R. Simulating physics with computers / R. Feynman // Physics. – 1982. – Vol. 467, № 6-7. – pp. 467–488.
2. Shor, P. Algorithms for quantum computation: discrete logarithms and factoring / P. Shor // Proceedings of the 35th Annual Symposium on Foundation of Computer Science (IEEE, Computer Society Press, Santa Fe, NM) – 1994. – pp. 124–134.
3. Grover, L.K. Quantum mechanics helps in searching for a needle in a haystack / L. K. Grover // Phys. Rev. Lett. – 1997. – Vol. 79, – pp. 325–328.
4. Bennett, C.H. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels / C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W.K. Wootters // Phys. Rev. Lett. – 1993. – Vol. 70. – pp. 1895–1899.
5. Bennett, C.H. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states / C.H. Bennett, S.J. Wiesner // Phys. Rev. Lett. – 1992. – Vol. 69. – pp. 2881–2885.
6. Bennett, C.H. Quantum cryptography: public key distribution anв coin tossing / C. H. Bennett and G. Brassard // Proceedings of IEEE International Conference on Computers, System and Signal Processing – 1984. – pp. 175–180.
7. Ekert A. Quantum cryptography basев on Bell's theorem / A. Ekert // Phys. Rev. Lett. – 1991. – Vol. 67, – pp. 661–665.
8. Bennett, C.H. Quantum cryptography using any two nonorthogonal states / C.H. Bennett // Phys. Rev. Lett. – 1992. – Vol. 68, – pp. 3121–3125.
9. Botto, A.N. Quantum interferometric optical lithography: exploiting entanglement to beat diffraction limit / A.N. Boto, P. Kok, D.S. Abrams, S.L. Braunstein, C.P. Williams, J.P. Dowling // Phys. Rev. Lett. – 2000. – Vol. 85. – pp. 2733–2736.
10. Bouwmeester, D. Experimental quantum teleportation / D. Bouwmeester, J.W. Pan, K. Mattle, M. Eible, H. Weinfurter, A. Zeilinger // Nature. – 1997. – Vol. 390, № 11. – pp. 575–579.
11. Schrodinger, E. The present situation in quantum mechanics / E. Schrodinger // Naturwissenschaften. – 1935. – Vol. 23, № 68. – pp. 807–812.
12. Zurek, W.H. Decoherence and the transition from quantum to classical / W.H. Zurek // Physics Today. – 1991. – Vol. 44. – pp. 36–44.

13. Knill, E A scheme for efficient quantum computation with linear optics / E. Knill, L. Laflamme, G J. Milburn // Nature. – 2001. – Vol. 409, № 4 – pp. 46–52.
14. Rausendorf, R. A one-way quantum computer / R. Rausendorf, H.J. Briegel // Phys. Rev. Lett. – 2001. – Vol. 86, – pp. 5188-5191.