На правах рукописи

УДК 530.145

Козубов Антон Владимирович

Квантовая динамика многомодовых фотонных систем и их анализ в качестве информационного ресурса

Специальность 01.04.02 —
«Теоретическая физика»

Автореферат

диссертации на соискание учёной степени
кандидата физико-математических наук

Санкт-Петербург — 2019

Работа выполнена на факультете фотоники и оптоинформатики федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Научный руководитель:

Мирошниченко Георгий Петрович

доктор физико-математических наук, профессор, профессор факультета лазерной фотоники и оптоэлектроники федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)»

Официальные оппоненты:

Калачёв Алексей Алексеевич

доктор физико-математических наук, профессор РАН, руководитель Федерального государственного бюджетного учреждения науки «Казанский физико-технический институт им. Е.К.Завойского»

Кронберг Дмитрий Анатольевич

кандидат физико-математических наук, старший научный сотрудник отдела математических методов квантовых технологий Федерального государственного бюджетного учреждение науки «Математический институт им. В.А. Стеклова Российской Академии Наук»

Ведущая организация:

Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», научно-исследовательская лаборатория Казанский квантовый центр («КАИ-КВАНТ»)

Защита состоится «26» декабря 2019 г. в ____ на заседании на заседании объединенного совета по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Д 999.069.02, созданного на базе Российского государственного педагогического университета им. А.И. Герцена, Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, по адресу: 191186, Санкт-Петербург, наб. реки Мойки, 48, корп. 3, ауд. 52.

С диссертацией можно ознакомиться в фундаментальной библиотеке Российского государственного педагогического университета им. А.И. Герцена (191186, Санкт-Петербург, наб. реки Мойки, 48, корп. 5) и на сайте университета по адресу:
https://disser.herzen.spb.ru/Preview/Karta/karta_000000573.html

Автореферат разослан «__» октября 2019 года.

Учёный секретарь
диссертационного совета Анисимова Надежда Ивановна

Общая характеристика работы

Актуальность темы. На сегодняшний день квантовая теория информации является краеугольным камнем во многих областях современной науки, находясь на пересечении разделов современной физики, информатики и математики, таких как квантовая физика, квантовая оптика, теория информации, а также теория групп и алгебр, что позволяет ей активно развиваться в современном мире. Помимо фундаментальной важности данного направления, существует ряд прикладных аспектов, важнейшими из которых являются квантовая информатика и квантовая коммуникация. Глубокое понимание "квантовости"процессов, в свою очередь, невозможно без их детального теоретического анализа и дальнейшего развития теории функционирования ключевых элементов систем квантовой информатики и коммуникаций.

Область квантовой коммуникации на сегодняшний день вызывает неподдельный интерес уже не только с научной, но и с практической точки зрения. Большое число исследований проводится как в теоретической, так и экспериментальной области уже более 30 лет. Однако, несмотря на большое число имеющихся подходов к оценке стойкости, на сегодняшний день далеко не все существующие (что лабораторные, что коммерческие) системы квантового распределения ключа (КРК) имеют строгое безусловное доказательство стойкости. Главной причиной тому является тот факт, что до сих пор не существует универсального подхода к доказательству стойкости подобных систем. Это вызвано как и различной структурой используемых квантовых состояний, так и различными возможными реализациями систем КРК.

Большая часть используемых протоколов КРК строится на использовании ослабленных когерентных состояний. Важным свойством ослабленных когерентных состояний является то, что внутри любого конечного набора они неортогональны и линейно независимы. В начале этого века был проведен ряд работ, в которых доказывалась стойкость протокола на неортогональных состояниях. В качестве основной идеи данных работ можно выделить утверждение, что рассмотрение протокола на неортогональных состояниях (например, B92) можно свести к рассмотрения протокола дистилляции запутанности (EDP) или же к анализу только однофотонной части аналогичному оригинальному BB84. В общепринятых подходах показана эквивалентность выбранных методов по аналогии с анализом протокола BB84. Авторы работы,

предполагают, что любое вмешательство злоумышленника в канал будет приводить к ошибкам. Однако, стоит отметить, что авторы работы пользуются рядом сильных допущений при доказательстве. Первое из них – применения неразрушающих измерений и выделение однофотонной на стороне получателя. Подобное допущение справедливо в случае использования кодирования информации по поляризации, однако абсолютно недопустимо для состояний с кодированием по фазе. В ряде работ показана техника доказательства для конечного набора когерентных состояний с кодированием по поляризации. Тем не менее, авторы также используют одно существенное допущение, а именно, – отбрасывание многофотонной части когерентных состояний, тем самым переходя к пространству меньшей размерности, где состояния становятся линейно зависимыми. Подобное допущение не может считаться физичными, потому что значительно изменяет структуру формируемых состояний, не имея на то должных оснований.

В связи с этим, становится очевидно, что необходимо расширение имеющихся теорий, основанное на отказе от вышеперечисленных допущений.

Целью данной работы является разработка методов описания квантовой динамики многомодовых фотонных систем для оценки развития различных квантовых состояний (как однофотонных, так и слабых когеретных или набора фоковских состояний) в произвольных (как линейных, так и не линейных) вполне положительных сохраняющих след квантовых каналах.

Для достижения поставленной цели необходимо было решить следующие **задачи**:

1. Разработать модель описания пространства многомодовых квантовых фазомодулированных состояний, реализуемую на основе представлений абелевой группы точечной симметрии и одномерных представлений симметрической группы Sn.
2. Разработать описание как линейных, так и нелинейных вполне положительных сохраняющих след отображения, соответствующих атакам общего типа на систему квантового распределения ключа, использующих слабые когеретные состояния.
3. Доказать стойкость протоколов, использующих многомодовые неортогональные состояния, с учетом атак, не вносящих ошибок в квантовый канал, а также конечной длины кодовых слов.

4. Разработать модель динамики многочастотных однофотонных состояний с учетом декогеренции в поляризационной области в квантовом канале, и проанализировать ее влияние на пропускную способность канала.

Основные положения, выносимые на защиту:

1. Пространство многомодовых квантовых фазомодулированных состояний может быть описано на основе представлений абелевой группы точечной симметрии и одномерных представлений симметрической группы S_n, построенных на принципах теории электро-оптического модулятора, использующей образующие $SU(2)$ алгебры Ли.
2. Условие ограничения снизу границей Деветака-Винтера скорости генерации стойкого ключа для протоколов, использующих дискретные переменные, в асимптотическом приближении бесконечного числа бит при наличии коллективных атак, является недостаточным для случая рассмотрения протоколов, использующих линейно независимые состояния
3. Найдены условия, обеспечивающие стойкость протоколов, использующих многомодовые неортогональные состояния, к атакам, не вносящим ошибок в квантовый канал, а также с учетом конечной длины кодовых слов.
4. Декогеренция в поляризационной области однофотонного излучения в оптическом волоконном канале приводит к появлению ошибок, а также снижает пропускную способность квантового канала.

Научная новизна:

1. Впервые была разработана и предложена модель описания многомодовых квантовых фазомодулированных состояний на основе представлений абелевой группы точечной симметрии и одномерных представлений симметрической группы S_n, построенная на принципах теории электро-оптического модулятора, использующей образующие $SU(2)$ алгебры Ли.
2. Впервые были проанализированы различные линейные вполне положительные сохраняющие след отображения, описывающие атаки общего вида на системы квантового распределения ключа, исполь-

зующие многомодовые когерентные состояния, а также разработана модель нелинейного вполне положительного сохраняющего след развития состояний в квантовом канале с обратной связью на основе метода унитарной декомпозиции, описывающая динамику развития произвольных квантовых состояний в канале, зависящую от измерения одной из подстистем и позволяющая учитывать атаку с засветкой детектора в теоретическом рассмотрении протокола.

3. Впервые была доказана стойкость протоколов, использующих многомодовые неортогональные состояния к атакам, не вносящих ошибок в квантовый канал, а также с учетом конечной длины кодовых слов.
4. Впервые разработана модель неунитарной динамики многомодовых однофотонных состояний с учетом декогеренции в поляризационной области в квантовом канале и проанализировать ее влияние на пропускную способность канала.

Практическая значимость Данная работа является значимой как с научной, так и с практической точки зрения, в виду того, что разработанные в диссертации подходы, модели и доказательства были представлены впервые и уже используются для реализации в реально существующих образцах систем квантового распределения ключей, использующих многомодовые состояний.

Достоверность полученных результатов обеспечивается хорошим совпадением построенных моделей с полученными экспериментальными данными. Кроме того, работы представлялись на различных ведущих международных конференциях, а также опубликованы в рецензируемых научных журналах, входящих в первый квартиль. Результаты находятся в соответствии с результатами, полученными другими авторами.

Апробация работы. Основные результаты работы докладывались на:

– Kozubov A.V. Quantum control attack on quantum key distribution systems, Quantum model of decoherence in the polarization domain for the fiber channel // 9th International Conference on Quantum Cryptography, Montreal, Canada, 26.08.2018–30.08.2018

– Kozubov A.V. Dynamics of non-orthogonal states in quantum channels // QKD Security Workshop 2019, Toronto, Canada, 01.08.2019 - 02.08.2019
– Kozubov A.V. Analysis of quantum dynamics of multimode weak coherent states and their information properties // ICQOQI 2019, Minsk, Belarus, 13.05.2019 - 17.09.2019
– Козубов А.В. Квантовая динамика многомодовых фотонных систем и их анализ в качестве информационного ресурса // XLVIII научная и учебно-методическая конференция Университета ИТМО, Санкт-Петербург, Россия, 29.01.2019 - 1.02.2019.
– Kozubov A.V. Finite-key analysis for subcarrier wave quantum key distribution // 8th International Conference on Quantum Cryptography, Shanghai, China, 27.08.2018–31.08.2018
– Kozubov A.V. Subcarrier wave quantum networking for free space communications// 18th International Conference on Laser Optics ICLO 2018, Санкт-Петербург, Россия, 4 - 8 июня 2018
– Козубов А.В. Исследование неравенства параметров модуляции в системах квантовой коммуникации на боковых частотах и его применение для обнаружения атаки с полным различением состояний // VII Всероссийский конгресс молодых ученых, Санкт-Петербург, Россия, 17.04.2018 - 20.04.2018
– Козубов А.В. Устойчивость протокола с четырьмя неортогональными когерентными состояниями для системы квантовой коммуникации на боковых частотах к коллективным атакам // XLVII научная и учебно-методическая конференция Университета ИТМО, Санкт-Петербург, Россия, 30.01.2018-02.02.2018
– Kozubov A.V. Practical security for subcarrier wave quantum key distribution against collective beam-splitting attack // 7th International Conference on Quantum Cryptography, Cambridge, UK, 18.09.2017-22.09.2017.

Объем и структура работы. Диссертация состоит из введения, шести глав и заключения. Полный объём диссертации составляет 150 страниц с 16 рисунками и 1 таблицей. Список литературы содержит 115 наименований.

Публикации. Основные результаты по теме диссертации изложены в 7 статьях, из них 6 работ издано в журналах, рекомендованных Перечнем ВАК и входящих в списки Web of Science/Scopus, 1 — в прочих изданиях.

Содержание работы

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель, ставятся задачи работы, сформулированы научная новизна и практическая значимость представляемой работы.

Первая глава «Литературный обзор» посвящена более детальному обзору научной литературы по изучаемой проблеме. Кроме того, в первой главе представлены основные проблемы, на решение которых направлена данная диссертация, а также методы, позволяющие решать поставленные задачи.

Во **второй главе «Основные определения»** представленные основные определения из различных разделов физики, математики и теории информации, которые будут использоваться в дальнейшем.

Третья глава «Анализ многомодовых состояний с поляризационным и фазовым кодирование» посвящена оценке пространства многомодовых фазомодулированных состояний, а также сравнению многомодовых состояний с фазовым и поляризационным кодированием информации.

В первой части данной главы рассмотрена возможность представления подобных состояний с помощью абелевой группы точечной симметрии в базисе конечного числа слабых когерентных состояний с различной фазой, элементы которой могут быть образованы следующим образом:

$$\mathcal{G}_i|\alpha_j\rangle = \exp\left(\frac{i2\pi}{M}a^\dagger a\right)|\alpha_j\rangle = \left|\alpha_j \exp\left(\frac{i2\pi}{M}\right)\right\rangle,$$

где a – оператор уничтожения фотона, а M – число реализуемых состояний.

Во второй части данной главы представлено рассмотрение модели работы электро-оптического модулятора. Решение данной задачи можно свести к анализу эффективного гамильтониана трехбозонного параметрического процесса в приближении вращающейся волны. Другое ключевое приближение, принятое в данной модели, заключается в том, что интенсивность

микроволновой моды достаточно высока, чтобы игнорировать ее квантовые свойства. Таким образом, её можно описать как классическое волновое поле. В этом квазиклассическом приближении оператор рождения (уничтожения) $b^{\dagger}(b)$ заменяется комплескной аплитудой $B\exp\left[-i\Omega_{MW}t\right]$. Кроме того, в данной модели используется приближение конечного (однако достаточно большого) числа взаимодействующих мод, где оптическая несущая (центральная мода) находится в середине интервала.

Кроме того, операторы, входящие в гамильтониан, удовлетворяют хорошо известным коммутационным соотношения $su(2)$ Ли алгебры.

Далее на основе построенной модели квантово-оптически описывается получение многомодовых фазомодулированных состояний. Состояние поля до модуляции имеет следующий вид:

$$|\psi\rangle = |\sqrt{\mu_0}\rangle_0 \otimes |\mathrm{vac}\rangle_{SB},$$

где $|\mathrm{vac}\rangle_{SB}$ – вакуумные состояния на боковых модах, а $|\sqrt{\mu_0}\rangle_0$ – когерентное состояние несущей (центральной) волны с амплитудой, определяемой средним числом фотонов μ_0 в окне передачи, создаваемое когерентным монохроматическим световым пучком с оптической частотой ω. Тогда состояние поля на выходе модулятора (в квантовом канале) является многомодовым когерентным состоянием следующего вида:

$$|\psi(\varphi_A)\rangle = \bigotimes_{k=-S}^{S} |\alpha_k(\varphi_A)\rangle_k,$$

где амплитуды когерентных состояний представлены как

$$\alpha_k(\varphi_A) = \sqrt{\mu_0} d_{0k}^{S}(\beta) e^{-i(\theta_1+\varphi_A)k},$$

где θ_1 – постоянная фаза, а $d_{nk}^{S}(\beta)$ – d-функция Вигнера из квантовой теории углового момента, β определяется индексом модуляции m, без учета дисперсии среды модулятора данную зависимость можно записать в виде

$$\cos\left(\beta\right) = 1 - \frac{1}{2}\left(\frac{m}{S+0.5}\right)^2.$$

В третьей части главы приведено описание пространства генерируемых посылок и его симметризация. Выделение симметрического подпространства основано на работе с симметрической группой перестановок S_n. Для оценки числа классов на симметрической группе S_n (инвариантных подпространств на пространстве $\mathcal{R}$) используется метод схем Юнга. В виду прямого соответствия число диаграмм Юнга, n, равно числу классов на симметрической группе S_n. Схемой Юнга, T, называют диаграмму $\mathcal{F}$ с заполненными соответствующим образом n ячейками диаграммы. Каждая диаграмма $\mathcal{F}$ имеет $n!$ схем T, однако нас интересуют только стандартные схемы. Подобный интерес вызван тем фактом, что число неприводимых представлений равно числу стандартных схем Юнга. Их число можно рассчитать по формуле:

$$f(\mathcal{F}) = n! \frac{\prod_{i<k}(l_i - l_k)}{\prod_i l_i!}$$

Каждой схеме Юнга сопоставим оператор Юнга, выделяющий инвариантное подпространство на пространстве $\mathcal{R}$ и имеющий следующий вид:

$$\hat{\xi}(\lambda_1,\lambda_2,...,\lambda_k) = \sum_q \hat{Q} \sum_{\pi \in S_\lambda} (-1)^{\epsilon(\pi)} \hat{\mathcal{G}}_i,$$

где $\{q\}$ – перестановки номеров в каждой строчке схемы Юнга, $\{\pi\}$ – перестановки номеров в каждом столбце. Таким образом, в каждом инвариантном подпространстве реализуется одно из неприводимых представлений группы перестановок S_n.

В последней части данной главы приведено описание основных различий многомодовых однофотонных и слабых когерентных состояний с фазовым и поляризационном кодированием. Глобально можно выделить два основным различия: размерность образуемого подобными состояниями пространства, а также наличие или отсутствие линейной зависимости между генерируемыми состояниями.

В случае поляризационного кодирования одиночных фотонов, несмотря на количество генерируемых состояний поляризации, размерность пространства остается неизменной и определяется как:

$$\dim \mathcal{H}_{sp} = 2,$$

где $\mathcal{H}_{sp}$ – пространство однофотонных состояний с кодированной по поляризации информацией.

В свою очередь, конечный набор слабых когерентных состояний имеет существенное отличие. Важным моментом является то, что подобные состояния всегда являются неортогональными (векторы, описывающие подобные состояния не формируют ортогональный базис) и линейно независимыми. В связи с этим, размерность такого пространства напрямую зависит от числа используемых состояний и рассчитывается следующим образом:

$$\dim \mathcal{H}_{coh} = n,$$

где $\mathcal{H}_{coh}$ – гильбертово пространство слабых когеретных состояний, а n – число используемых состояний.

Таким образом, можно сделать вывод, что любой конечный набор слабых когерентных состояний (что с поляризационным кодированием информации, что с фазовым) является линейно независимым. В свою очередь, конечный набор однофотонных состояний с поляризационным кодированием информации, в котором присутствует больше двух состояний, является линейно зависимым, благодаря геометрическим свойствам образуемого пространства.

Однако, в слабых когерентных состояниях, усредненных по фазе, можно выделить подпространства (фотонные секторы), где возможно создание линейно зависимых состояний. Интерес к данным состояниям как к объекту исследования вызван тем фактом, что на сегодняшний день они являются наиболее распространенными в системах КРК. Рассмотрим данные состояния. В общем виде их можно представить в следующей форме:

$$\int_0^{2\pi} |\sqrt{\mu}\exp(i\phi)\rangle\langle\sqrt{\mu}\exp(i\phi)|d\phi = \sum_{n=0}^{\infty} p_{n|\mu}|n\rangle_s\langle n|,$$

$$p_{n|\mu} = \exp(-\mu)\frac{\mu^n}{n!},$$

вероятность излучения n фотонов, согласно пуассоновской статистике, $\sqrt{\mu}$ – амплитуда когерентного состояния, $\{|n\rangle\}$ – набор фоковских состояний, где $n = 0...\infty$. Очевидно, что в зависимости от выбранного подпространства число линейно независимых состояний является различным. Общее число

возможных линейно независимых состояний можно определить с помощью биномиального разложения:

$$(\alpha_1 a_H^\dagger + \beta_1 a_V^\dagger)^n = \sum_{k=0}^{n} \binom{n}{k} (\alpha_1 a_H^\dagger)^{n-k} (\beta_1 a_V^\dagger)^k.$$

Легко заметить, что число возможных линейно независимых состояний для каждого из фоковских состояний $|n\rangle$ равняется $n+1$, где n – число фотонов в фоковском состоянии.

В **четвертой главе «Квантовая модель декогеренции в поляризационной области в оптическом волокне»** представлена модель декогренции в поляризационной области для однофотонного излучения в оптическом волокне. Данная глава преследует две цели. Первая цель состоит в исследовании динамики однофотонного состояния в одномодовом волокне, тензор диэлектрической проницаемости которого обладает анизотропией и дихроизмом. Уравнение Лиувилля, описывающее развитие матрицы плотности фотона в шредингеровском представлении, в Марковском приближении предлагается в работе. Уравнение содержит оператор релаксации, зависящий от феноменологических параметров. Эти параметры позволяют учесть явление двулучепреломления и оптической активности, изотропного поглощения и дихроизма. Вторая цель состоит в анализе влияния декогеренции в поляризационной области, описываемой модельным уравнением Лиувилля, на ошибки распределения ключа по протоколу BB84.

Уравнение Лиувилля для матрицы плотности смешанного состояния фотона в квантовом канале, подверженном процессу анизотропной декогеренции в поляризационной области, записывается тогда в виде:

$$\frac{\partial}{\partial t}\rho(t) = -i[\hat{V},\rho(t)] + \hat{\Gamma}\rho(t),$$

где $\hat{\Gamma}$ – супероператор релаксации в Марковском приближении, описывайщий феномен декогеренции, а матрица оператора взаимодействия в пространстве, натянутом на трех базисных векторах $\{|0\rangle, |H\rangle, |V\rangle\}$, где $|0\rangle, |H\rangle, |V\rangle$ – вакуумное состояние, горизонтально и вертикально поляризованные состояния

одиночного фотона соответственно, имеет следующий вид:

$$\hat{V} = \frac{\xi}{2} \begin{pmatrix} 0 & 0 & 0 \\ 0 & n_z & n_x - in_y \\ 0 & n_x + in_y & -n_z \end{pmatrix},$$

где $\boldsymbol{n} = \frac{\boldsymbol{\xi}}{|\boldsymbol{\xi}|}$ – направляющий вектор в системе координат Стокса-Пуанкаре.

Для определения декогеренции в поляризационной области необходимо следить за параметрами Стокса. Тогда, пусть векторный оператор $\hat{\boldsymbol{\sigma}}$ будем называть оператором Стокса. Средние значения этого оператора есть параметры Стокса. Таким образом, пусть $\boldsymbol{P}(t)$ – вектор Стокса, представленный следующим образом:

$$\boldsymbol{P}(t) = (\hat{\boldsymbol{\sigma}}\rho(t)).$$

В силу некоммутативности проекций вектора $\hat{\boldsymbol{\sigma}}$, , не существует квантового состояния фотона, где бы компоненты вектора $\boldsymbol{P}(t)$ не имели бы дисперсии. Определим действие оператора релаксации $\hat{\Gamma}$. Для этого введем два непараллельных единичных вектора $\boldsymbol{\mu^{(1)}}$,$\boldsymbol{\mu^{(2)}}$ и запишем уравнение для оператора $(\boldsymbol{P}(t),\hat{\boldsymbol{\sigma}})$ в следующем виде:

$$\frac{d}{dt}(\boldsymbol{P}(t),\hat{\boldsymbol{\sigma}}) = -i\frac{\xi}{2}[(\boldsymbol{n},\hat{\boldsymbol{\sigma}}),(\boldsymbol{P}(t),\hat{\boldsymbol{\sigma}})] - \varepsilon(\boldsymbol{P}(t),\hat{\boldsymbol{\sigma}}) + \\ + \sum_{j=1}^{2} \frac{\beta_j}{4}\left[(\boldsymbol{\mu}^{(j)},\hat{\boldsymbol{\sigma}}),\left[(\boldsymbol{\mu}^{(j)},\hat{\boldsymbol{\sigma}}),(\boldsymbol{P}(t),\hat{\boldsymbol{\sigma}})\right]\right].$$

По аналогии с терминами кристаллооптики будем называть этот оператор двухосным оператором релаксации. Далее, рассмотрим одноосный оператор релаксации, для этого положим $\boldsymbol{\mu^{(1)}} = \boldsymbol{\mu^{(1)}} = \boldsymbol{\mu}$. Используя свойства оператора $\hat{\boldsymbol{\sigma}}$ получим выражение:

$$\frac{d}{dt}\boldsymbol{P}(t) = \xi[\boldsymbol{n} \times \boldsymbol{P}(t)] - \varepsilon\boldsymbol{P}(t) + \beta[\boldsymbol{\mu} \times [\boldsymbol{\mu} \times \boldsymbol{P}(t)]].$$

Это феноменологическое уравнение (аналог модифицированного уравнения Блоха) будет использовано для описания преобразования состояний фотона в неидеальном ОВ. Первое слагаемое в правой части параметризовано векто-

ром $\boldsymbol{\xi}$ и описывает изменение типа поляризации без изменения длины вектора Стокса $\boldsymbol{P}(t)$. Второе слагаемое описывает процесс изотропной декогеренции со скоростью ε. В этом процессе длина вектора Стокса уменьшается без изменения его направления. Третье слагаемое параметризовано единичным вектором $\boldsymbol{\mu}$ и скоростью β. Это слагаемое описывает неизотропную поляризационную декогеренцию. Данное слагаемое обращает в ноль компоненту вектора Стокса, направленную вдоль вектора $\boldsymbol{\mu}$.

Подобная модель позволяет более точно следить за изменением параметров Стокса, и их зависимостью от параметров волокна. В свою очередь, в виду процессов подобной декогеренции, может существенно измениться пропускная способность квантового канала. Основываясь на параметрах модели, вероятности обнаружения правильного квантового бита и бита с ошибкой определяются соответственно следующим образом:

$$\mathcal{P}_{0,0} = \mathcal{P}_{1,1} = \frac{1+B}{4}, \mathcal{P}_{0,1} = \mathcal{P}_{1,0} = \frac{1-B}{4},$$
$$B = \frac{1}{2}(1+\exp(-\beta t))\exp(-\varepsilon t).$$

Следует отметить, что в модели предполагается идеальный однофотонный источник и детектор для изучения влияния только деполяризации на процесс генерации квантового ключа.

Пятая глава «Атаки на квантовые состояния в канале» посвящена исследованию возможных атак на фазомодулированные многомодовые состояния в квантовых каналах. Рассматриваемые в работе протоколы относятся к классу однопроходных протоколов квантового распределения ключей (КРК) с независимыми равнораспределенными носителями информации. Скорость генерации стойкого ключа для протоколов этого класса в асимптотическом приближении бесконечного числа бит при наличии коллективных атак ограничена снизу границей Деветака-Винтера:

$$K = \nu_S P_B \left[1 - \mathrm{leak}_{EC}(Q) - \max_E \chi(A:E)\right],$$

где ν_S – частота повторения посылок, P_B – вероятность успешного декодирования и детектирования бита в одном временном окне, Q – квантовый коэффициент ошибок (QBER), $\mathrm{leak}_{EC}(Q)$ – количество информации, раскры-

той Алисой по открытому каналу для исправления ошибок, которое зависит от квантового коэффициента ошибок и ограничено границей Шеннона $\mathrm{leak}_{EC}(Q) \geq h(Q)$, где $h(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q)$ – бинарная энтропия Шеннона. Величина $\chi(A:E)$ – граница Холево, определяющая верхнюю границы количества информации, доступной для нарушителя в данной коллективной атаке.

В первой части главы приводится описание квантового канала общего вида как линейного вполне положительного сохраняющего след отображения. Кроме того, показано, что классическая пропускная способность квантового канала в приближении бесконечного числа посылок имеет следующий вид:

$$C(\mathcal{Q}) = \lim_{n\to\infty} \frac{1}{n}\chi((\mathcal{Q})^{\otimes n}) = \chi(\mathcal{Q}),$$

$$\chi(\mathcal{Q}) = S\left(\sum_x p_x \mathcal{Q}(\rho_x)\right) - \sum_x p_x S(\mathcal{Q}(\rho_x)),$$

где $S(\rho) = -\mathrm{Tr}\{\rho\log\rho\}$ – энтропия фон Неймана, $\mathcal{Q}$ – квантовый канал, n – число отправленных кубитов, ρ – безусловный оператор плотности канала.

Во второй части главы представлена общая классификация различного типа атак на состояния в квантовом канале.

В третьей части приведено подробное описание протокола, использующего многомодовые фазомодулированные состояния.

В четвертом разделе приведен анализ атаки со светоделителем и квантовой памятью на системы КРК, использующие фазомодулированные многомодовые состояния. Для подобного анализа приведен расчет ключевых параметров, влияющих на работу системы. В частности, в работе представлено квантово-оптическое описание всех элементов установки, а также расчет вероятности детектирования $(1-G)$, вероятности ошибки (E) и квантовый коэффициент ошибок QBER (Q), используя следующие обозначения:

$$E = P_{det}(0, \pi + \Delta\varphi),$$
$$1 - G = P_{det}(0, \Delta\varphi) + P_{det}(0, \pi + \Delta\varphi),$$
$$Q = \frac{E}{1-G},$$

где $\Delta\varphi$ – небольшая фазовая нестабильность, вызванная, например, дрожанием или несовершенной синхронизацией в системе КРК, а P_{det} – вероятность детектирования.

В свою очередь, расчет оценки границы Холево производится, используя бинарную энтропийную функцию Шеннона $h(x) = -x\log x - (1-x)\log(1-x)$ от собственных значений энтропии фон Неймана:

$$\chi(A:E) = h\left(\frac{1}{2}(1-\exp\left[-\mu_0(1-d_{00}^{\bar{S}}(2\beta))\right]\right).$$

Кроме того, приведены расчетные графики для реальной системы КРК, использующей подобные состояния, и экспериментальное подтверждение полученных результатов.

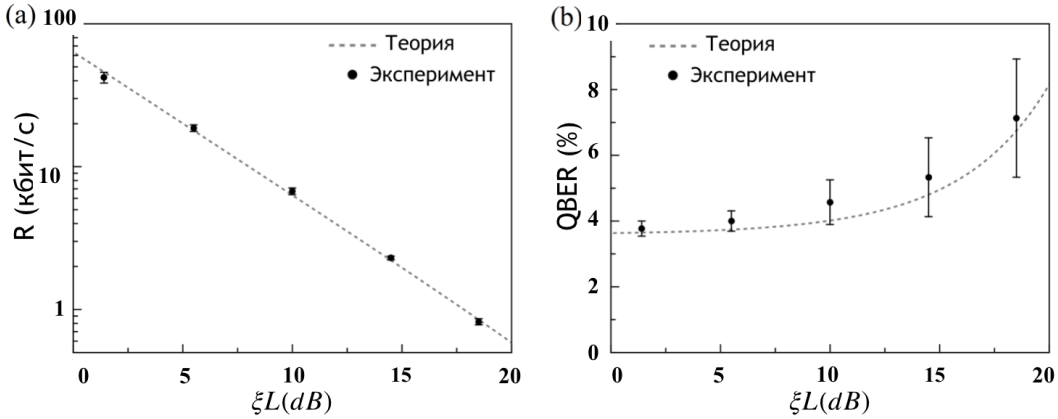

Рис. 1 — Экспериментальная скорость генерации просеянного ключа (a) и квантовый коэффициент ошибок (b) как функция от от потерь в канале в системе КРКБЧ с лавинным фотодиодом, реализующей протокол с четырьмя состояниями.

В пятой части доказывается невозможность проведения атаки с разделением числа фотонов на многомодовые фазомодулированные состояния.

В шестом разделе рассмотрена коллективная атака общего вида на слабые когерентные состояния. Для этого рассматривается действие квантового канала как результат произвольной изометрии. Ева выполняет унитарную операцию (описываемую изометрией) между состояниями в канале и своими вспомогательными модами, чтобы произвольным образом запутать их (в общем случае)

$$\begin{cases} |u\rangle \longrightarrow a|\tilde{u}\rangle \otimes |\psi_{\mathcal{E}}^{\tilde{u}}\rangle + b|\tilde{v}\rangle \otimes |\psi_{\mathcal{E}}^{\tilde{v}}\rangle \\ |v\rangle \longrightarrow b|\tilde{u}\rangle \otimes |\psi_{\mathcal{E}}^{\tilde{u}}\rangle + a|\tilde{v}\rangle \otimes |\psi_{\mathcal{E}}^{\tilde{v}}\rangle, \end{cases}$$

где a, b – произвольные коэффициенты, удовлетворяющие норме и условиям унитарности, $\{|u\rangle,|v\rangle\}$ – пространство состояний, приготовленных Алисой, $\{|\tilde{u}\rangle,|\tilde{v}\rangle\}$ – пространство состояний в квантовом канале после применения Евой унитарного преобразования, $\{|\psi_{\mathcal{E}}^{\tilde{u}}\rangle,|\psi_{\mathcal{E}}^{\tilde{v}}\rangle\}$ – пространство состояний Евы в комплементарном квантовом канале (без потери общности можно предположить , что у Евы было начальное состояние $|\psi_{\mathcal{E}}\rangle$, описывающее её вспомогательную моду, учитывая унитарную эволюцию сведенного к чистому состояния).

Информационную оценку используемых фазовых многомодовых квантовых состояний в произвольном квантовом канале можно получить по средствам расчета пропускной способности Холево. Можно показать, что максимальная пропускная способность Холево для подобных состояний достигается при $a = 1$ и $b = 0$ (или же наоброт), используя распутанные (но взаимодействующие) состояния:

$$\begin{cases} |u\rangle \longrightarrow |\tilde{u}\rangle \otimes |\psi_{\mathcal{E}}^{\tilde{u}}\rangle \\ |v\rangle \longrightarrow |\tilde{v}\rangle \otimes |\psi_{\mathcal{E}}^{\tilde{v}}\rangle. \end{cases}$$

Благодаря свойствам сохранения перекрытий неортогональных состояний в результате действия изометрии и тому факту, что пропускная способность Холево является убывающей функцией от перекрытий состояний нетрудно показать, что любая пропускная способность Холево ограничены сверху границей Холево, что позволяет учесть произваольные коллективные атаки на состояния в квантовом канале с помощью границы Холево.

В седьмой разделе главы производится оценка получаемой информации в результате измерения различного типа посылок. Кроме того, доказывается, что перепутывание посылок между собой не дает преимущества при измерении по сравнению с распутанным случаем.

В восьмой, девятой и десятой частях данной главы показано, что несмотря на общепринятый подход к оценке стойкости систем КРК, его при-

менение в случае когерентных состояний с кодировкой информации по фазе является недостаточным. Это происходит благодаря тому, что атаки на квантовый канал не всегда описываются линейными сохраняющими след отображениями.

Например, квантовые каналы, включающие в себя измерение посередине, не могут быть рассмотрены как линейные вполне положительные сохраняющие след отображения. Рассмотрим случай, когда измерение происходит внутри квантового канала. Тогда такой канал может быть описан следующим образом:

$$\mathcal{Q}^i_{\mathcal{E}}\rho_j(0) = \tilde{\rho}(t) = \frac{U\sqrt{A^i_{\mathcal{E}}}\rho_j(0)\sqrt{A^i_{\mathcal{E}}}U^*}{(\mathcal{A}^i_{\mathcal{E}}\rho_j(0))}, \tag{1}$$

где $\rho_j(0)$ – состояние на входе в квантовый канал, а $\tilde{\rho}_j(t)$ – состояние после действия отображения, индексы $i = 1$ и $j = 1{,}2$ обозначают соответствующий оператор ПОМа и возможные начальные состояния соответственно. Рассмотрим случай, когда начальное состояние описывается линейной комбинацией состояний:

$$\rho(0) = \frac{\rho_1(0) + \rho_2(0)}{2}. \tag{2}$$

Согласно определению квантового канала, описывающее его отображение должно переводить линейную комбинацию в соответствующую линейную комбинацию (чтобы удовлетворять свойству линейности), а следовательно, иметь следующий вид:

$$\mathcal{V}\rho(0) = \mathcal{V}\frac{\rho_1(0) + \rho_2(0)}{2} = \frac{\tilde{\rho}_1(t) + \tilde{\rho}_2(t)}{2}. \tag{3}$$

Однако, в случае наличия измерения внутри квантового канала, подобная операция имеет следующий вид:

$$\mathcal{Q}^1_{\mathcal{E}}\frac{\rho_1(0) + \rho_2(0)}{2} = \frac{(A^1_{\mathcal{E}}\rho_1(0))\tilde{\rho}_1(t) + (A^1_{\mathcal{E}}\rho_2(0))\tilde{\rho}_2(t)}{(A^1_{\mathcal{E}}(\rho_1(0) + \rho_2(0)))}. \tag{4}$$

Очевидно, что правая часть выражения 4 не равна правой части выражения 3. Таким образом, квантовый канал не может рассматриваться исключи-

тельно как линейные отображения из-за наличия перенормировки состояний в результате измерения.

В связи с этим, становится очевидно, что существующие подходы к рассмотрению являются недостаточными. Для этого два утверждения с соответствующими доказательствами. Первое из них – Рассмотрение границы Деветака-Винтера для коллективных атак является недостаточным для оценки стойкости системы КРК, использующих слабые когерентные состояния с кодированием информации по фазе.

Доказательство данного утверждения сводится к описанию предложенной атаки с квантовым управлением, которая не учитывается при подобном анализе. Для описания подобной атаки использован метод полярной (унитарной) декомпозиции операторов, составляющих положительную операторнозначную меру (ПОМ). Подобная атака не включена в общепринятое рассмотрение, так как она не может быть описана линейным вполне положительным сохраняющим след отображением. Иными словами, данную атаку можно описать как нелинейное вполне положительное сохраняющее след отображение с измерением одной из подсистем. В ходе описания атаки показано, что она позволяет узнавать до 100% ключа и требует отдельных контрмер для ее нейтрализации.

Помимо этого, вторым важным утверждением является то, что протокол, использующий слабые когерентные состояния с кодированием информации по фазе, нельзя сводить к дистиляции запутанности как в случае протокола BB84. Доказательство данного утверждения также сводится к описанию применения атаки с квантовым управлением, не вносящей ошибки, к используемым состояниям и доказательству невозможности ее отследить.

Кроме того, приведено обобщение данной атаки с учетом использования различными ПОМов, что позволяет максимизировать взаимную информацию между отправителем и злоумышленником. Помимо этого, представлены различные варианты атаки на протокол, использующий два слабых когерентных состояния с кодированием информации по фазе.

В одиннадцатом разделе приводится рассмотрение подобного квантового канала в терминах теории информации. Доказывается, что подобный канал описывается посредством марковской цепочки. Благодаря этому, можно

утверждать, что случайные переменные X, Y, Z, отвечающие за информацию Алисы, Евы и Боба соответственно, образуют марковскую цепь $X \to Y \to Z$.

Таким образом, благодаря тому факту, что подобный канал представляет собой марковскую цепь, можно воспользоваться хорошо известным неравенством обработки данных и утверждать, что

$$I(X;Y) \geq I(X;Z) \tag{5}$$

Следовательно, очевидно, что наблюдение только за уровнем ошибок (благодаря тому, что неортогональные состояния можно различать без ошибок) и оценке границы Холево недостаточно, как и было показано в предыдущих разделах.

Шестая глава «Математическое доказательство стойкости протоколов на когерентных состояниях» посвящена обощению доказательства стойкости систем КРК на случай использования как одномодовых, так и многомодовых слабых когерентных состояний с кодированием информации по фазе. В первой части производится описание пространства формируемых состояний, а также оценка его размерности. Далее приводятся методы борьбы с атакой с квантовым контролем представленной в предыдущей главе. В работе было показано, что если удовлетворяется следующее условие, Ева не сможет успешно осуществить атаку

$$1 - G > P_{USD},$$

где $1 - G$ – ожидаемая вероятность детектирования (G – предполагаем вероятность «пустого» счета), а P_{USD} - вероятность однозначной различения состояний. Очевидно, что есть две основные стратегии: первая - увеличить $1 - G$, вторая - уменьшить P_{USD}. Вторая стратегия выглядит более удобной с практической точки зрения (неравенство 6 должно выполняться для всех допустимых потерь в канале, где мы можем извлечь секретный ключ). Существует несколько вариантов решения данной задачи:

- Увеличение числа используемых состояний
- Добавление дополнительных неинформационных состояний-ловушек, позволяющих минимизировать (или даже занулить) вероятность различения состояний.

Далее приведен расчет ε-стойкого ключа для случая слабых когерентных состояний с кодированием информации по фазе. Для оценки соответствующей границы скорости генерации безопасного ключа мы рассмотрим обозначения квантовых энтропий Реньи,

$$H_\alpha(X) = \frac{1}{1-\alpha} \log \left(\sum_{i=1}^{n} p_i^\alpha \right),$$

поскольку они описывают наихудший случай, а не усредненный, как это делают энтропии Шеннона и фон Неймана. В данной работе рассматривается энтропия, когда параметр $\alpha \to \infty$, а именно *мин-энтропия*,

$$H_\infty(X) = H_{\min} = -\log \max_i p_i.$$

Для дальнейшего анализа информационных соотношений будет использован подход основанный на квантовом асимптотическом свойстве равнораспределения. Тогда, можно ограничить *ε-гладкую мин-энтропию* следующим образом:

$$H_{\min}^{\varepsilon_S}(\mathbf{A}|\mathbf{E}) \geq n \left(H(\mathbf{A}|\mathbf{E}) - \frac{\delta(\varepsilon_S)}{\sqrt{n}} \right),$$

где

$$\delta(\varepsilon_S) = 4 \log(2+\sqrt{2}) \sqrt{\log \left(\frac{2}{\varepsilon_S^2} \right)},$$

где $H(\mathbf{A}|\mathbf{E})$ – условная энтропия фон Неймана, обозначающая энтропию битов Алисы зависимые от информации, доступной Еве в отдельном раунде.

Тогда, с точки зрения общепринятых определений, это означает, что протокол ε_{corr} - корректный с $\varepsilon_{corr} = \varepsilon_{EC}$ (см. определение 1) и ε_{sec} - стойкий с $\varepsilon_{sec} = \varepsilon_s + \varepsilon_{PA}$ (см. определение 2). Если сформулировать это в терминах определения 3, то протокол выглядит так: ε_{QKD} - стойкий и коректный, с $\varepsilon_{\text{QKD}} = \varepsilon_{EC} + \varepsilon_s + \varepsilon_{PA}$ предоставляет стойкую битовую строку с длиной

$$l = n(1-\chi(\rho)) - 4\sqrt{n} \log(2+\sqrt{2}) \sqrt{\log \left(\frac{2}{\varepsilon_S^2} \right)} - \\ -k - code_{EC} - \log \frac{1}{\varepsilon_{EC}} - \log \frac{1}{\varepsilon_{PA}} + 2.$$

В последней части данной главы приведен пример применения данного анализа для случая реальной системы КРК, использующей фазомодулированные многомодовые слабые когерентные состояния.

В **заключении** приведены основные результаты работы, которые заключаются в следующем:

1. На основе теории электро-оптического модулятора, использующей образующие $SU(2)$ алгебры Ли, была разработана модель описания многомодовых квантовых фазомодулированных состояний на основе представлений абелевой группы точечной симметрии, одномерных представлений симметрической группы S_n.
2. Впервые разработана модель неунитарной динамики многомодовых однофотонных состояний с учетом декогеренции (уменьшение длины вектора Стокса без изменения его направления и неизотропную поляризационную декогеренцию) в поляризационной области в квантовом канале и проанализировано ее влияние на пропускную способность канала.
3. Впервые были проанализированы различные атаки общего вида, описываемые линейными вполне положительными сохраняющими след отображения, на системы квантового распределения ключа, использующие многомодовые когерентные состояния.
4. Впервые был представлен формализм вполне положительного сохраняющего след развития состояний в квантовом канале с обратной связью на основе метода унитарной декомпозиции (квантового контроля), описывающая динамику развития произвольных квантовых состояний в канале, зависящую от измерения одной из подстистем, являющийся примером нелинейного отображения.
5. Впервые были найдены условия, при которых стойкость протоколов, использующих многомодовые неортогональные состояния, с учетом атак, не вносящих ошибок в квантовый канал, а также конечной длины кодовых слов может быть доказана.
6. Численное моделирование позволило оценить зависимость скорости генерации стойкого ключа с учетом атака, не вносящих ошибок в канал, а также конечной длины кодовых слов от потерь в канале

Статьи из списков Web of Science/Scopus, ВАК:

- **Kozubov A. Quantum model of decoherence in the polarization domain for the fiber channel / Kozubov A., Gaidash A., Miroshnichenko G. //Physical Review A. – 2019 (5). – Т. 99.(5), май – №. 5. – С. 053842.** (0,31 п.л. / 0,23 п.л.)
- **Kozubov A.V. Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems / Gaidash A.A., Kozubov A.V., Miroshnichenko G.P. // Journal of the Optical Society of America B: Optical Physics. - 2019 (3). - Vol. 36.(3), март - № 3. - Pp. B16-B19** (0, 25 п.л. / 0,18 п.л.)
- **Kozubov A.V. Security of subcarrier wave quantum key distribution against the collective beam-splitting attack / Miroshnichenko G.P., Kozubov A.V., Gaidash A.A., Gleim A.V., Horoshko D.B. // Optics express. - 2018. - Vol. 26. - № 9. - Pp. 11292-11308** (1,1 п.л. / 0,8 п.л.)
- **Kozubov A.V. Subcarrier wave quantum networking for free space communications / Gleim A.V., Kynev S.M., Egorov V.I., Chistyakov V.V., Volkova K.P., Vasilev A.B., Kozubov A.V., Gaidash A.A., Latypov I.Z., Vitkin V.V., Kolyubin S.A., Bespalov V.G., Bobtsov A.A., Kozlov S.A. //Proceedings - International Conference Laser Optics 2018, ICLO 2018, IET - 2018, pp. 281** (0,06 п.л. / 0,03 п.л.)
- **Kozubov A.V. Sideband quantum communication at 1 Mbit/s on a metropolitan area network / Gleim A.V., Chistyakov V.V., Bannik O.I., Egorov V.I., Buldakov N.V., Vasilev A.B., Gaidash A.A., Kozubov A.V., Smirnov S.V., Kynev S.M., Khoruzhnikov S.E., Kozlov S.A., Vasil'ev V.N. //Journal of Optical Technology, IET - 2017, Vol. 84, No. 6, pp. 362-367** (0.37 п.л. / 0,2 п.л.)
- **Kozubov A.V. Security conditions for sub-carrier wave quantum key distribution protocol in errorless channel / Gaidash A.A., Kozubov A.V., Chistyakov V.V., Miroshnichenko G.P., Egorov V.I., Gleim A.V. //Journal of**

Physics: Conference Series, IET - 2017, Vol. 917, No. 6, pp. 062014 (0,12 п.л. / 0,1 п.л.)

Прочие публикации:

– Козубов А.В. Многоузловая квантовая сеть на основе технологии квантовой коммуникации на боковых частотах / Чистяков В.В., Глейм А.В., Банник О.И., Васильев А.Б., Гайдаш А.А., Козубов А.В., Смирнов С.В., Егоров В.И., Козлов С.А //Сборник трудов XI Международного симпозиума по фотонному эхо и когерентной спектроскопии (ФЭКС - 2017) - 2017. - С. 102-103С. 13. (0,06 п.л. / 0,03 п.л.)