На правах рукописи

Сыч Денис Васильевич

Совместимая информация как инструмент анализа квантовых информационных каналов

Специальность 01.04.02 — теоретическая физика

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2005

Работа выполнена на кафедре общей физики и волновых процессов физического факультета Московского государственного университета им. М.В. Ломоносова.

Научный руководитель:	кандидат физико-математических наук, доцент Виктор Николаевич Задков;
Официальные оппоненты:	доктор физико-математических наук, профессор Дмитрий Васильевич Куприянов,
	доктор физико-математических наук, профессор Фарид Явдатович Халили;
Ведущая организация:	Санкт-Петербургский государственный университет.

Защита состоится "____"_____ 2005 г. в _____ на заседании диссертационного совета К 501.001.17 в МГУ им. М.В. Ломоносова по адресу: 119992, Москва, ГСП-2, Ленинские горы, МГУ, физический факультет, аудитория _____.

С диссертацией можно ознакомиться в библиотеке физического факультета МГУ им М.В. Ломоносова.

Автореферат разослан "____"_____ 2005 г.

Ученый секретарь диссертационного совета К 501.001.17
доктор физико-математических наук, профессор

Петр Александрович Поляков

1. Общая характеристика работы

1.1. Актуальность темы

Одним из наиболее значительных научных событий XX века в области физики стало, несомненно, создание квантовой теории. Основные ее положения настолько сильно отличаются от привычных представлений о мире, что вызывали не только споры у основоположников квантовой теории (достаточно вспомнить известную дискуссию Эйнштейн — Бор), но и все новые и новые попытки интерпретации её оснований, продолжающиеся до сих пор. Другим значительным научным событием XX века стало создание теории информации. На стыке квантовой теории и теории информации в последнее время начала активно развиваться *теория квантовой информации*, которая, возможно, станет одной из самых интересных областей науки XXI века. Ее предметом является создание, передача и обработка информации, с той особенностью, что носителями информации выступают не классические, а сугубо квантовые объекты с присущей им квантовой спецификой.

Первые теоретические исследования в данном направлении были начаты еще в 60–70-х годах прошлого века, но настоящий всплеск интереса к теории квантовой информации начался в 90-е годы и был связан, с одной стороны, с открытием практически важных приложений теории (квантовые вычисления, квантовая криптография, квантовая телепортация), и, с другой стороны, — с возросшими возможностями экспериментальных методов в таких областях, как квантовая оптика, атомная физика, физика твердого тела, с помощью которых уже экспериментально продемонстрированы новые возможности практического использования специфических особенностей квантовой информации.

Особый интерес научного сообщества к теории квантовой информации обуславливает тот факт, что классическая теория информации находится с теорией квантовой информации приблизительно в том же соотношении, что и классическая ньютоновская механика с квантовой — некоторые объекты и результаты квантовой теории в частном случае дают классическую теорию, а некоторые совсем не имеют классического аналога, и, помимо интереснейших фундаментальных результатов, дают принципиально новые возможности решения важных прикладных задач. Так, например, в квантовых вычислени-

ях переход к квантовому носителю информации — кубиту (от английского qubit — quantum bit) дает возможность построения квантовых алгоритмов, решающих некоторые математические задачи за значительно меньшее число шагов, чем лучшие классические алгоритмы. В квантовой криптографии появляется возможность *абсолютно секретной* передачи данных по квантовым каналам, в то время как секретность передачи информации по классическим каналам не абсолютна, а основана лишь на сложности решения ряда математических задач. В квантовой телепортации с использованием перепутанных состояний можно мгновенно передавать произвольное квантовое состояние с одного объекта на другой.

Несмотря на значительные как теоретические, так и экспериментальные успехи различных приложений, общая теория квантовой информации пока не создана. С фундаментальной точки зрения одной из центральных проблем в теории информации является определение количественной меры информации и связанной с ней пропускной способности информационного канала. В классической теории объем информации определяется информационным функционалом Шеннона, имеющим смысл логарифма числа сообщений, передаваемых безошибочно при оптимальном кодировании в асимптотическом пределе больших последовательностей сообщений. По сравнению с теорией информации Шеннона в приложении к физике роль квантовой информации представляется значительно более существенной, не позволяющей выделить её в качестве независимой от физики чисто математической дисциплины. В отличие от классических систем, в квантовом случае проблема введения количественной меры квантовой информации не допускает единого решения, а зависит от физического содержания квантового информационного канала.

Наиболее общее деление типов квантовых каналов и соответствующих информационных мер основано на коммутативности/некоммутативности проекторов–индикаторов событий на входе и выходе информационного канала, или, другими словами, внутренней и взаимной совместимости/несовместимости элементарных событий на входе и выходе информационного канала. В результате такого деления можно выделить четыре основных типа информационных каналов:

- классический (элементарные события на входе и выходе канала внутренне и взаимно совместимы);
- полуклассический (элементарные события на входе канала внутренне

совместимы и автоматически взаимно совместимы с элементарными событиями на выходе канала, но, в отличие от предыдущего случая, элементарные события на выходе канала внутренне несовместимы);

- некоммутативный (элементарные события на входе и выходе канала внутренне и взаимно несовместимы);

- коммутативный (элементарные события на входе и выходе канала внутренне несовместимы, но, в отличие от предыдущего случая, взаимно совместимы).

В то время как три первых типа информационных каналов и соответствующих им информационных мер хорошо известны и в той или иной степени исследованы, коммутативный канал, как особый тип квантового канала, и его информационная мера — *совместимая информация* — в явной форме введены лишь относительно недавно. В связи с этим представляется весьма актуальным анализ общих свойств совместимой информации, разработка математических методов информационного анализа коммутативных каналов и применение анализа, основанного на расчете совместимой информации, к общеупотребительным моделям реальных физических систем.

1.2. Цель работы

Цель диссертации состоит в анализе общих свойств совместимой информации и применении разработанного формализма к информационному анализу ряда важных типов коммутативных информационных каналов.

1.3. Научная новизна работы

В диссертационной работе впервые проведен систематический анализ общих свойств совместимой информации. Детально проанализированы информационные свойства наиболее важных двухчастичных состояний. Исследованы возможности применения совместимой информации к анализу фундаментальных процессов передачи информации на квантовом уровне в реальных физических задачах. Показана ее эффективность для анализа проблем, связанных с таким практически важным приложением теории квантовой информации, как квантовая криптография.

1.4. Практическая ценность работы

Полученные теоретические результаты и методы наряду с комплексом написанных программ могут быть использованы для исследования различных коммутативных информационных каналов. Результаты анализа совместимой информации в задаче Дике представляют интерес для физического обсуждения процессов передачи информации на уровне отдельных атомов и могут быть использованы, например, в задачах физической реализации квантовых вычислений. Предложенные в работе протоколы квантовой криптографии обеспечивают больший уровень помехозащищенности, чем существовавшие ранее протоколы, и могут быть реализованы в реальных системах квантовой криптографии.

1.5. Защищаемые положения

1. На ряде практически важных квантовых информационных каналов продемонстрирована эффективность использования понятия совместимой информации как адекватной информационной меры.

2. Показано, что максимально перепутанные двухчастичные состояния обеспечивают бóльшую информативность чем любые другие двухчастичные состояния. Выявлено соответствие между энтропией чистого квантового состояния в N–мерном гильбертовом пространстве и энтропией классической системы с N элементарными событиями. Выявлена качественная специфика описания динамики физических систем на языке совместимой и когерентной информации.

3. Выявлено соответствие между неклонируемостью квантовых состояний и некопируемостью квантовой информации. Предложены и проанализированы несколько протоколов квантовой криптографии, алфавиты которых образуют правильные многогранники на сфере Блоха. Показано, что они могут обеспечивать больший уровень помехозащищенности, чем существовавшие раннее протоколы с двумерными алфавитами. Рассчитана верхняя оценка помехозащищенности для протоколов квантовой криптографии с многомерными алфавитами. Показана принципиальная возможность создания секретного сообщения при произвольном уровне помех в квантовом канале связи.

1.6. Апробация работы

Результаты работы докладывались и обсуждались на следующих российских и международных конференциях и семинарах:

1. Международная конференция “International Quantum Electronics Conference — 2002”, 22 — 27 июня 2002 г., Москва, Россия.

2. Международная конференция “Quantum Informatics — 2002”, 1 — 4 октября 2002 г., Звенигород, Россия.

3. Санкт–Петербургский городской семинар по квантовой оптике, 18 декабря, 2002 г., Санкт–Петербург, Россия.

4. Международная научная конференция студентов, аспирантов и молодых ученых “Ломоносов — 2003”, 15 — 18 апреля 2003 г., Москва, Россия.

5. Московский городской семинар по квантовой оптике, 23 апреля 2003 г., Москва, Россия.

6. Международная конференция “8th International Conference on Squeezed States and Uncertainty Relations”, 9 — 13 июня 2003 г., Puebla, Mexico.

7. Международная конференция “International Symposium on Optical Science and Technology, SPIE’s 48th Annual Meeting”, 3 — 8 августа 2003 г., San Diego, USA.

8. Международная конференция “Micro– and nanoelectronics — 2003”. 6 — 10 октября 2003 г., Звенигород, Россия.

9. Международная конференция “304. WE–Heraeus–Seminar: Elementary Quantum Processors”, 13 — 15 октября 2003 г., Physikzentrum Bad Honnef, Germany.

10. Международная конференция “2nd Asia–Pacific Workshop on Quantum Information Science”, 15 — 19 декабря 2003 г., Singapore.

11. Международная научная конференция студентов, аспирантов и молодых ученых “Ломоносов — 2004”, 12 — 15 апреля 2004 г., Москва, Россия.

12. Международная конференция “X International Conference on Quantum Optics — 2004”, 30 мая — 3 июня 2004 г., Минск, Беларусь.

13. Международная конференция “IV International Symposium on Modern Problems of Laser Physics”, 22 — 27 августа 2004 г., Новосибирск, Россия.

14. Международная конференция “Quantum informatics — 2004”, 4 — 8 октября 2004 г., Москва, Россия.

По теме диссертации опубликовано 18 работ, список которых приведен в конце настоящего автореферата.

1.7. Объем и структура работы

Диссертация состоит из введения, трех частей, заключения, двух приложений и списка литературы. Диссертация содержит 115 страниц текста, 13 рисунков и 4 таблицы. Список литературы содержит 97 наименований.

1.8. Личный вклад автора

Автор внес определяющий вклад в исследования по теме диссератции. Все результаты, выносимые как защищаемые положения, получены лично автором.

2. Краткое содержание диссертации

Во **введении** дан исторический и литературный обзор работ по теории квантовой информации. Обсуждена проблема определения количественной меры квантовой информации, осложненная по сравнению с классическим случаем наличием классически несовместимых квантовых событий. Обоснована актуальность изучения совместимой информации, связанной с множествами совместимых событий на входе и выходе квантового канала. Сформулированы цели диссертационной работы.

В первой главе **“Передача классической информации по квантовым каналам”** изучены базовые понятия и соотношения теории квантовой информации, введено понятие совместимой информации, изучены общие

свойства совместимой информации и проанализированы абстрактные двухкубитные каналы.

В первом параграфе обсуждаются такие базовые понятия квантовой теории как состояние квантовой системы и элементарное квантовое событие. Обосновывается необходимость рассмотрения квантовой логики событий. Показана естественность разделения всех наборов элементарных событий на два класса: совместимые (подчиняющиеся законам классической логики и отображаемые ортогональным набором волновых функций) и несовместимые (не подчиняюшиеся законам классической логики и отображаемые неортогональным набором волновых функций). Раскрывается физическое содержание обобщенного измерения, математически описываемого неортогональным разложением единичного оператора или, другими словами, ПОМ (положительно определенной операторозначной мерой)

$$\hat{1} = \sum_k \hat{E}(k), \tag{1}$$

Во втором параграфе рассматривается классическая шенноновская информация как основа для введения количественной меры совместимой информации:

$$I_{AB} = S_A + S_B - S_{AB}, \tag{2}$$

где S_X — энтропия распределения вероятностей $P(x)$ элементарных событий x в системе X. Конкретизируется качественный смысл таких базовых понятий, как энтропия и количество взаимной информации. На простом классическом примере угадывания игроком выпадения двусторонней монеты на ту или иную сторону продемонстрирован метод расчета количества взаимной информации в классических системах.

В третьем параграфе выявлено соотношение между энтропией классической системы с N элементарными событиями и энтропией квантового состояния в N–мерном гильбертовом пространстве. Показано, что если в классической системе вероятности ее элементарных событий $p_1, p_2, \ldots p_N$ априори не известны, то средняя энтропия такой системы равна априорной энтропии квантового состояния:

$$\overline{S}_N = \int\limits_{\sum\limits_{i=1}^{N} p_i = 1} S_N(p_1, p_2, \ldots, p_N) dp_1 dp_2 \ldots dp_N = \frac{1}{\ln 2} \sum_{i=2}^{N} \frac{1}{i}. \tag{3}$$

В дальнейшем показывается, что это соотношение тесно связано с борновской вероятностной интерпретацией волновой функции.

В четвертом параграфе вводится формализм совместимой информации. Определяются два предельных типа совместимой информации — селектированная и неселектированная. Селектированная информация

$$I_{AB}(\alpha,\beta)=\sum_{k,l=1}^{2}P_{AB}^{\alpha\beta}(k,l)\log_2\frac{P_{AB}^{\alpha\beta}(k,l)}{P_A^{\alpha}(k)P_B^{\beta}(l)} \tag{4}$$

отражает информационную связь систем A и B посредством двух классических индексов α и β ортогональных информационных базисов $\{|\alpha\rangle \equiv |1\rangle_A^{\alpha}, |\tilde{\alpha}\rangle \equiv |2\rangle_A^{\alpha}\}$ и $\{|\beta\rangle \equiv |1\rangle_B^{\beta}, |\tilde{\beta}\rangle \equiv |2\rangle_B^{\beta}\}$. Здесь составные континуальные индексы α и β определяют ортогональные базисы, а дискретные двузначные индексы $k,l=1,2$ нумеруют в этих базисах состояния $|k\rangle_A^{\alpha}$ и $|l\rangle_B^{\beta}$. Совместное распределение вероятностей есть

$$P_{AB}^{\alpha\beta}(k,l)=\mathrm{Tr_{AB}}\Big[\Big(|k\rangle_A^{\alpha}\langle k|_A^{\alpha}\otimes|l\rangle_B^{\beta}\langle l|_B^{\beta}\Big)\hat{\rho}_{AB}\Big]. \tag{5}$$

Селектированную информацию можно качественно интерпретировать как информацию о состояниях в базисе α системы A, содержащуюся в состояниях базиса β системы B.

Неселектированная информация

$$I_{AB}=\iint\limits_{\alpha\ \beta}P_{AB}(d\alpha,d\beta)\log_2\frac{P_{AB}(d\alpha,d\beta)}{P_A(d\alpha)P_B(d\beta)} \tag{6}$$

отражает информационный обмен сразу через *все* равноправно задействованные квантовые состояния систем с учетом их внутренней квантовой неопределённости, без селекции каких-либо конкретных базисов. Совместное распределение вероятностей $P_{AB}(d\alpha,d\beta)$ задано на элементах дифференциала объема dV_α, dV_β гильбертовых пространств A и B:

$$P_{AB}(d\alpha,d\beta)=\mathrm{Tr_{AB}}\Big[\Big(\hat{E}_A(d\alpha)\otimes\hat{E}_B(d\beta)\Big)\hat{\rho}_{AB}\Big], \tag{7}$$

где $\hat{E}_{A,B}(d\nu)=|\nu\rangle_{A,B}\langle\nu|_{A,B}\,dV_\nu$.

Выявлено базовое соотношение между селектированной и неселектированной информацией: неселектированная информация равна селектированной, усредненной по всем ориентациям её информационных базисов.

В последнем параграфе первой главы дается развернутый информационный анализ наиболее важных типов двухкубитных каналов, образованных парами кубитов, находящихся в чистых максимально перепутанных и сепарабельных состояниях. Показано, что максимально перепутанные состояния обеспечивают наибольший уровень информативности среди всех остальных двухчастичных состояний. Рассчитан объем неселектированной информации I_{AB} для максимально перепутанных ($I_{AB} = 1 - 1/\ln 4 \simeq 0,279$ бит) и сепарабельных состояний ($I_{AB} = 1 - (20 - \pi^2)/(16 \ln 2) \simeq 0,087$ бит).

Результаты, представленные в этой главе, опубликованы в работе [8].

Во второй главе **"Информационный анализ двухкубитного канала в модели Дике"** показан пример анализа динамики реальной физической системы на языке неселектированной совместимой информации. Рассматривается система из двух двухуровневых атомов, взаимодействующих посредством диполь–дипольного взаимодействия, включающего обмен излучаемыми фотонами.

В первом параграфе дается математическая модель рассматриваемой физической системы. Решение задачи зависит от ряда безразмерных параметров: расстояния между атомами $\varphi = kr$, где k — модуль волнового вектора, соответствующего частоте перехода изолированного атома, а r — расстояние между атомами; времени взаимодействия γt, где γ — скорость радиационного распада изолированного атома, а t — время взаимодействия атомов; начального состояния атомов, заданного начальной разностью населенностей n_A и n_B каждого атома.

Во втором параграфе матрица плотности рассматриваемой двухчастичной системы, зависящая от этих параметров, анализируется в терминах неселектированной совместимой информации. Сначала изучается зависимость неселектированной информации I от времени взаимодействия и расстояния между атомами при их фиксированном начальном состоянии. Эта зависимость, приведенная на рис. 1, качественно аналогична зависимости разности населенностей атомов и отражает динамику процесса излучения одного атома в присутствии другого. Количественно она отражает тип двухчастичного возбуждения системы. Так, при малых межатомных расстояниях и больших временах взаимодействия основной вклад в информацию вносит долгоживущее антисимметричное состояние.

Далее изучается зависимость неселектированной информации от началь-

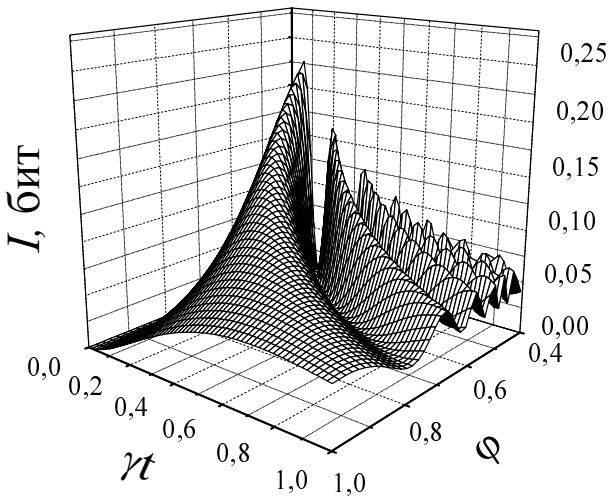

Рис. 1: Зависимость неселектированной информации I в двухатомной системе от безразмерных времени взаимодействия атомов γt и межатомного расстояния φ.

ного состояния атомов при фиксированном межатомном расстоянии и времени взаимодействии. Показано, что в общем случае эта зависимость немонотонна. Так, например, при максимально возбужденных атомах неселектированная информация не достигает своей максимальной величины. Максимум неселектированной информации зависит также и от характера начального возбуждения атома: при чистом начальном состоянии он несколько больше, чем при некогерентном возбуждении той же разности населенностей.

Результаты, представленные в этой главе, опубликованы в работах [1, 7].

В третьей главе **“Информационный анализ квантовых каналов в задачах квантовой криптографии”** выполняется исследование протоколов квантовой криптографии на основе анализа совместимой информации. Основной результат главы состоит в получении зависимости критического уровня ошибок протоколов квантовой криптографии от квантового алфавита, выбранного для кодирования информации в квантовом канале связи.

В первом параграфе обсуждается принцип неклонируемости квантовых состояний, играющий ключевую роль в квантовой криптографии. Этот принцип заключается в том, что нельзя создать точную копию произвольного заранее неизвестного квантового состояния, т.е. произвольное квантовое состояние нельзя клонировать. Показано, что этот принцип может быть усилен и выражен в принципе некопируемости квантовой информации, состоящем в том, что точную информационную копию квантового состояния не только

нельзя создать, но она вообще не существует.

Во втором параграфе излагаются основные понятия квантовой криптографии (получение сырого ключа, согласование базисов, усиление безопасности, коррекция ошибок, квантовый алфавит, критический уровень ошибок), раскрывается используемая далее терминология (Алиса — передатчик информации, Боб — приемник, Ева — подслушивающая сторона). Вводятся в рассмотрение двумерные квантовые алфавиты, буквы которых в представлении на сфере Блоха образуют вершины правильных многогранников: тетраэдр, октаэдр, куб, икосаэдр и додекаэдр (имеющих 4, 6, 8, 12 и 20 вершин соответственно), и, как предельный случай многогранника с бесконечным числом вершин, — континуальный алфавит. Протоколы, использующие такие алфавиты, повторяют все шаги стандартных протоколов квантовой криптографии.

В третьем параграфе рассматривается особенность континуального алфавита, связанная с невозможностью буквального использования стандартной процедуры согласования базисов. Вместо точного согласования базисов для протокола с континуальным алфавитом предлагается использовать приблизительное согласование базисов. Для этого сфера Блоха разбивается на конечное число одинаковых областей и базисы считаются совпавшими, если они попали в одну область. Понятно, что такая процедура вносит дополнительные (по сравнению с точным согласованием базисов) ошибки в передаваемое сообщение, зависящие от конкретного способа разбивки и размера области. Чем меньше размер одной области, и, соответственно, больше общее число областей, тем меньше будут эти ошибки. В работе предложены два варианта разбивки и рассчитано соответствующее им количество информации в одном сообщении.

Вторая особенность континуального алфавита состоит в неадекватности использования меры ошибок QBER (от англ. “quantum bit error rate”), равной $Q = 1 - N/N_{max}$, где N — число правильно переданных букв, а N_{max} — общее число переданных букв, как количественной меры подслушивания, т.к. в случае приблизительного согласования базисов она дает ненулевой уровень ошибок даже при отсутствии подслушивания. Вместо нее предлагается использовать меру ошибок MIER (от англ. “mutual information error rate”), равную $\tilde{Q} = 1 - I/I_{max}$, где I — реально переданное количество совместимой информации в одном бите, а I_{max} — максимально возможное количе-

ство совместимой информации в одном бите при отсутствии подслушивания. MIER адекватно описывает уровень подслушивания для всех рассматриваемых в работе протоколов.

В четвертом параграфе рассчитывается уровень ошибок для всех рассматриваемых протоколов, вызванный стратегией подслушивания типа перехвата–пересылки. Это самая простая стратегия, состоящая в прямом измерении Евой передаваемого состояния в случайном базисе с последующей пересылкой Бобу результата своего измерения. Уровень ошибок, вызванный такой стратегией, дает верхнюю границу потенциально возможного критического уровня ошибок при любой стратегии подслушивания. Результаты расчетов приведены в табл. 1.

Таблица 1: Уровень ошибок Q, вызванный стратегией подслушивания типа перехвата–пересылки.

Число букв в алфавите	4	6	8	12	20	∞
Уровень ошибок Q, QBER	0,333	0,333	0,333	0,329	0,329	0,333

В пятом параграфе аналогичный анализ выполняется для стратегии оптимального подслушивания при индивидуальных атаках. Такая стратегия подразумевает, что Ева может выполнять любые преобразования над каждым отдельно передаваемым кубитом, извлекая максимум информации при заданном уровне ошибок, или, другими словами, при извлечении заданного объема информации создает минимальные ошибки в подслушиваемом сообщении. Рассчитан уровень ошибок до и после согласования базисов. Рассматривался случай безопасного согласования базисов, когда считается, что Ева не получает никакой дополнительной информации из процедуры открытого согласования базисов. Результаты расчета приведены в табл. 2

Таблица 2: Критический уровень ошибок $\tilde{Q}_0$ до согласования базисов.

Число букв в алфавите	4	6	8	12	20	∞
$\tilde{Q}_0$ до согл. базисов, MIER	0,650	0,630	0,607	0,597	0,589	0,600
$\tilde{Q}_0$ после согл. базисов, MIER	—	0,806	0,805	0,804	0,805	0,811

Буквы тетраэдрального алфавита ортогональных пар не образуют, поэтому

процедура согласования базисов для него не выполняется, и соответствующего результата в табл. 2 нет.

В шестом параграфе рассматриваются особенности протоколов квантовой криптографии с бесконечномерными алфавитами. Показано, что стратегия подслушивания типа перехвата–пересылки для многомерных алфавитов, состоящих из взаимно–несмещенных базисов, в пределе бесконечной размерности вызывает уровень ошибок $Q = 1$, т.е. принципиальных запретов на увеличение критического уровня ошибок с увеличением размерности пространства состояний алфавита нет. Для протокола с многомерным континуальным алфавитом показано, что при любых стратегиях подслушивания критический уровень ошибок $\tilde{Q}_0$ после безопасного согласования базисов с ростом размерности алфавита может быть сколь угодно близким к 1, т.е. с использованием многомерного континуального алфавита в принципе можно осуществить секретную связь при *любом* наперед заданном уровне ошибок в квантовом канале связи.

В последнем параграфе третьей главы предлагается экспериментальная схема реализации рассмотренных двумерных протоколов с кодированием информации в поляризационной степени свободы фотона. Произвольные двумерные алфавиты могут быть реализованы единообразно на одной экспериментальной установке за счет выбора соответствующего набора углов поворота поляризации с помощью ячеек Поккельса.

Результаты, представленные в этой главе, опубликованы в работах [2–6, 9–18].

В **заключении** обсуждаются результаты работы, делаются выводы и формулируются защищаемые положения, приведенные в пункте 1.5. настоящего автореферата.

В **приложении А** дано описание представления состояния кубита вектором на сфере Блоха. В **приложении Б** приведена программа на языке Mathematica для расчета основных полученных в работе величин.

Список публикаций по теме диссертации

[1] Гришанин Б. А., Сыч Д. В. Совместимая квантовая информация в задаче Дике// Вестник Московского Университета. Серия 3. Физика. Астрономия. — 2002. — 4. — с. 37 — 42.

[2] Sych D. V., Grishanin B. A., Zadkov V. N. Quantum key distribution with continuous alphabet// Laser Physics. — 2004. — 14. — 10. — p. 1314.

[3] Grishanin B. A., Sych D. V., Zadkov V. N. Unselected information as an effective tool for quantum cryptography// SPIE Proc. 5161. Eds: Ronald E. Meyers and Yanhua Shih. 2004. — p. 341 — 351.

[4] Grishanin B. A., Sych D. V., Zadkov V. N. Noise-resistant quantum key distribution protocol// Proc. SPIE 5401 Eds: Kamil A. Valiev, Alexander A. Orlikovsky. — 2004. — p. 714 — 724.

[5] Sych D. V., Grishanin B. A., Zadkov V. N. Critical error rate of QKD protocols versus the size and dimensionality of the quantum alphabet// Phys. Rev. A. — 2004. — 70. — 052331.

[6] Сыч Д. В., Гришанин Б. А., Задков В. Н. Анализ предельно возможных информационных характеристик протоколов квантовой криптографии// Квантовая Электроника. — 2005. — 35. — 1. — с. 80 — 84.

[7] Denis V. Sych, Boris A. Grishanin, Victor N. Zadkov Compatible Information: Properties and application to physical problems// тезисы международной конференции “International Quantum Electronics Conference”. — 22 — 27 июня 2002. — Москва, Россия.

[8] D. V. Sych, B. A. Grishanin, V. N. Zadkov Some applications of compatible information to physical problems// тезисы международной конференции “Quantum Informatics — 2002”. — 1 — 4 октября 2002. — Звенигород, Россия.

[9] Д. В. Сыч, Б. А. Гришанин, В. Н. Задков Квантовая криптография с неселектированной информацией// тезисы международной научной конференции студентов, аспирантов и молодых ученых “Ломоносов — 2003”. — 15 — 18 апреля 2003. — Москва, Россия.

[10] B. A. Grishanin, D. V. Sych, V. N. Zadkov Unselected quantum information as an effective tool for quantum cryptography// тезисы международной конференции "International Symposium on Optical Science and Technology, SPIE's 48th Annual Meeting". — 3 — 8 августа 2003. — San Diego, USA.

[11] D. Sych, B. Grishanin, V. Zadkov, A. Chirkin Noise-threshold-free quantum cryptography// тезисы международной конференции "8th International Conference on Squeezed States and Uncertainty Relations". — 9 — 13 июня 2003. — Puebla, Mexico.

[12] D. V. Sych, B. A. Grishanin, V. N. Zadkov Noise-resistant quantum key distribution protocol// тезисы международной конференции "Micro– and nanoelectronics — 2003". — 6 — 10 октября 2003. — Звенигород, Россия.

[13] D. V. Sych, B. A. Grishanin, V. N. Zadkov Information analysis of the quantum key distribution protocols// тезисы международной конференции "304. WE–Heraeus–Seminar: Elementary Quantum Processors". — 13 — 15 октября 2003. — Physikzentrum Bad Honnef, Germany.

[14] Denis Sych Quantum Cryptography with unselected information// тезисы международной конференции "2nd Asia–Pacific Workshop on Quantum Information Science". — 15 — 19 декабря 2003. — Singapore.

[15] Д. В. Сыч, Б. А. Гришанин, В. Н. Задков Исследование зависимости эффективности протоколов квантовой криптографии от параметров квантового алфавита// тезисы международной научной конференции студентов, аспирантов и молодых ученых "Ломоносов — 2004". — 12 — 15 апреля 2004. — Москва, Россия.

[16] D. V. Sych, B. A. Grishanin, V. N. Zadkov Comparative characteristics of quantum key distribution protocols with alphabets corresponding to the regular polyhedrons on the Bloch sphere// тезисы международной конференции "X International Conference on Quantum Optics — 2004". — 30 мая — 3 июня, 2004. — Минск, Беларусь.

[17] D. V. Sych, B. A. Grishanin, V. N. Zadkov Six–state protocol critical error rate can be exceeded// тезисы международной конференции "IV International Symposium on Modern Problems of Laser Physics". — 22 — 27 августа, 2004. — Новосибирск, Россия.

[18] D. V. Sych, B. A. Grishanin, V. N. Zadkov Optimal alphabets for noise–resistant quantum cryptography// тезисы международной конференции “Quantum informatics — 2004”. — 4 — 8 октября 2004. — Москва, Россия.