ЛАБОРАТОРИЯ *КВАНТОВОЙ ИНФОРМАЦИИ*

Научный отчет за 2004 г.

1. Наиболее значимые результаты за 2004 г.

Проанализирована микроскопическая структура физических преобразований, соответствующих введённому ранее классу супероператоров перепутывающего квантового измерения, и специфика их физической реализации. Предложена простейшая трёхкубитовая модель, позволяющая минимальными средствами реализовать квантовое измерение с произвольной степенью перепутанности. Рассмотрен специальный класс нечётких квантовых измерений как реалистичная модель широко представленных в физике измерений мягкого типа и проанализированы их информационные характеристики. Показано, что модель отбора квантовой информации с помощью невозмущающего измерения, обобщённого с учётом эффектов перепутанности, в наиболее явной форме суммирует фундаментальные отличия квантовой информации от классической. В частности, в задачах квантовой криптографии возможность рассмотрения регулируемой степени вмешательства Евы при использовании нечёткого измерения с целью получения секретной информации, передаваемой по каналу Алиса–Боб, позволяет использовать данную модель квантового измерения как наиболее простую физически содержательную модель взаимодействия потоков квантовой информации.

2. Наиболее значимые результаты за последние 5 лет

На основе неселективной информации предложен новый криптографический квантовый протокол с континуальным алфавитом, превосходящий по эффективности предложенные ранее.

Теоретически описаны полученные в ФИАН экспериментальные данные по КПН в атомах самария.

Теоретически разработана экспериментальная схема управления хиральным состоянием изотопомера перекиси водорода

3. Список статей и препринтов за 2004 г.

1. Б. А. Гришанин, В. Н. Задков, “Перепутывающие квантовые измерения”, Оптика и спектроскопия 96, №5, 751–759 (2004).

2. Denis V. Sych, Boris A. Grishanin, Victor N. Zadkov, “Unselected quantum information as an effective tool for quantum cryptography”, Proc. SPIE Vol. 5161, p. 341–351, Quantum Communications and Quantum Imaging; Ronald E. Meyers, Yanhua Shih; Eds. (2004).

3. D. Sych, B. Grishanin, and V. Zadkov, “Quantum Key Distribution with a Continuous Alphabet”, Laser Physics 14 (10), 1314–1321 (2004).

4. Boris A. Grishanin, Denis V. Sych, Victor N. Zadkov, “Noise-resistant quantum key distribution protocol”, Proc. SPIE Vol. 5401, p. 714–724, Micro- and Nanoelectronics 2003; Kamil A. Valiev, Alexander A. Orlikovsky; Eds (2004).

5. D. V. Sych, B. A. Grishanin, and V. N. Zadkov, “Critical error rate of QKD protocols versus the size and dimensionality of the quantum alphabet”, Phys. Rev. A 70, No. 5, 052331–8 (2004).

6. B. A. Grishanin and V. N. Zadkov, “Physical implementation of entangling quantum measurements”, Laser Phys. Lett., DOI 0.1002/lapl.200410001, accessible at http://www.interscience.wiley.com; e-print arXiv:quant-ph/0410220 v1.

4. Участие в конференциях в 2004 г.

1. **Int. Conf. Quantum informatics – 2004, October 4-8, 2004, Moscow, Russia (100 участников)**

D. V. Sych, B. A. Grishanin, and V. N. Zadkov, “Optimal alphabets for noise-resistant quantum cryptography”, in International Symposium “, Int. Conf. Quantum informatics – 2004, October 4-8, 2004, Moscow, Russia [ORAL].

2. **European Workshop on “Optical parametric processes and periodical structures”, September 26-29, 2004, Vilnius, Lithuania (100 участников)**

B.A. Grishanin, J.V.Vladimirova, V.N. Zadkov, D.Zhdanov, and H.Takahashi, "Controlling molecular chiral states with light", European Workshop on “Optical parametric processes and periodical structures”, September 26-29, 2004, Vilnius, Lithuania. [INVITED]

3. **IV International Symposium on Modern Problems of Laser Physics, August 22-27, 2004, Novosibirsk, Russia (200 участников)**

D. V. Sych, B. A. Grishanin, and V. N. Zadkov, “Six-state protocol critical error rate can be exceeded”, IV International Symposium on Modern Problems of Laser Physics, August 22-27, 2004, Novosibirsk, Russia (Digest, p.78) [INVITED].

4. **IV International Symposium on Modern Problems of Laser Physics, August 22-27, 2004, Novosibirsk, Russia (200 участников)**

J.Vladimirova, B.Grishanin, D. Zhdanov, V.Zadkov, "Laser coherent control of an ensemble of randomly oriented chiral molecules", IV International Symposium on Modern Problems of Laser Physics, August 22-27, 2004, Novosibirsk, Russia (Digest, p.281) [POSTER].

5. **International Conf. on Distributed calculations and GRID-technologies in science and educartion, 29 June -- 2 July, 2004, Dubna, Russia (200 участников)**

Vl.V.Voevodin, A.V.Gulyaev, A.P.Demichev, V.N.Zadkov, V.A.Il'in, A.P.Kryukov, and N.A.Soukhareva, "Studies of distrinuted data processing technologies on a gigabit network at Moscow State University", International Conf. on Distributed calculations and GRID-technologies in science and educartion, 29 June -- 2 July, 2004, Dubna, Russia. [INVITED]

6. **Международная научная конференция студентов, аспирантов и молодых ученых «Ломоносов-2004», 12-15 апреля 2004, Москва, Россия (200 участников)**

D.V.Sych, B.A.Grishanin, V.N.Zadkov, "Investigation of the QKD-protocols efficacy versus the parameters of the quantum alphabet", International conference of students and researchers Lomonosov-2004, 12-15 April 2004, Moscow, Russia [Сыч Д. В., Гришанин Б. А. и Задков В. Н., “Исследование зависимости эффективности протоколов квантовой криптографии от параметров квантового алфавита”, Международная научная конференция студентов, аспирантов и молодых ученых «Ломоносов-2004», 12-15 апреля 2004, Москва, Россия] [ORAL]

7. **X Int. Conference on Quantum Optics, Minsk, Belarus, June 2-6 (500 участников)**

D.N.Sych, B.A.Grishanin, and V.N.Zadkov, "Comparative characteristics of quantum key distribution protocols with alphabets corresponding to the regular polyhedrons on the Bloch sphere", Int. Conference on Quantum Optics, Minsk, Belarus, June 2-6, 2004 [POSTER].

8. **X Int. Conference on Quantum Optics, Minsk, Belarus, June 2-6 (500 участников)**

B.A.Grishanin, and V.N.Zadkov, "Entangling measurement as a basic operation of quantum information processing", X Int. Conference on Quantum Optics (ICQO 2004), Book of Abstracts, p. 46, Minsk, Belarus, June 2-6, 2004 [INVITED].

9. **Russian-French Workshop on Laser Physics for Young Scientists, July 6-10, 2004, St. Petersburg, Russia (100 участников)**

D.N.Yanyshev, B.A.Grishanin, and V.N.Zadkov, "Resonance dipole–dipole interactions between atoms in an optical dipole trap", Russian-French Workshop on Laser Physics for Young Scientists, July 6-10, 2004, St. Petersburg, Russia [ORAL].

5. Информация о грантах, договорах, контрактах

1. Грант Российского министерства науки и технологий “Научная школа Р. В. Хохлова и С. А. Ахманова по когерентной и нелинейной оптике”
2. Номер, шифры (УДК, ГАСНТИ), номер госрегистрации (если есть)
3. Руководитель
4. Объём финансирования

5. Аннотационный отчет:

Два предельных типа квантового измерения – полностью деквантующее, т.е. порождающее некогерентный набор ортогональных (классически совместимых) состояний в системе объект–прибор, и полностью квантовое, т.е. порождающее полностью когерентное состояние, обобщены в форме единого преобразования *перепутывающего* измерения, которое характеризуется соответствующей матрицей перепутанности R. Выявлены общие соотношения между различными типами измерения, проанализированы динамические характеристики соответствующих супероператоров и конкретизирована общая структура реализующих их физических систем.

Предложена простейшая трёхкубитовая модель, позволяющая минимальными средствами реализовать квантовое измерение с произвольной степенью перепутанности. Рассмотрен специальный класс нечётких квантовых измерений как реалистичная модель широко представленных в физике измерений мягкого типа и проанализированы их информационные характеристики. Показано, что модель отбора квантовой информации с помощью невозмущающего измерения, обобщённого с учётом эффектов перепутанности, в наиболее явной форме суммирует фундаментальные отличия квантовой информации от классической. В частности, в задачах квантовой криптографии возможность рассмотрения регулируемой степени вмешательства Евы при использовании нечёткого измерения с целью получения секретной информации, передаваемой по каналу Алиса–Боб, позволяет использовать данную модель квантового измерения как наиболее простую физически содержательную модель взаимодействия потоков квантовой информации.

Показано, что применение ранее развитой в наших работах концепции совместимой квантовой информации к описанию общей криптографической схемы квантовой передачи (распределения) секретного ключа (QKD) приводит не только к более прозрачному описанию механизмов, лежащих в основе квантовой криптографии, но и к новым протоколам QKD и новым методам их анализа, прямо вытекающим из самых общих принципов описания совместимой квантовой информации. В дополнение к известным протоколам с дискретным конечным алфавитом предложен качественно новый протокол, в котором алфавит, в отличие, например, от BB84 и B92, состоит не из некоторого дискретного набора букв, а из всего гильбертова пространства состояний, т.е. из бесконечного числа букв, представленных произвольными суперпозициями ортогональных базисных состояний гильбертова пространства.

Исследован вопрос об увеличении критического уровня допустимых ошибок протоколов квантовой криптографии за счёт варьирования набора букв квантового алфавита при фиксированной размерности пространства. Рассмотрены квантовые алфавиты, образующие правильные многогранники на сфере Блоха, и континуальный алфавит, равноправно включающий все квантовые состояния. Показано, что даже при использовании двумерного пространства квантовых состояний можно с помощью варьирования используемого алфавита превзойти критический уровень ошибок протокола six-state.

6. Нет

7.

1. Грант Российского фонда фундаментальных исследований “Разработка оптических методов управления хиральностью молекул”, МЛЦ МГУ

2. № 02-03-32200

3. Задков В. Н.

4. Объём финансирования

5. Аннотационный отчет:

Конкретизированы общие требования к набору коротких лазерных импульсов, вызывающих цепочку резонансных дипольных переходов, когерентно связывающую симметричное и антисимметричное хиральные состояния. Анализ выполнен для молекул, у которых дублетное расщепление состояний пренебрежимо по сравнению со всеми характерными частотами. На основе того факта, что при изменении на фазы импульса, отвечающего за любой из переходов в рассматриваемой цепочке, индуцируемая хиральность должна изменять знак, для используемых импульсов конкретизированы специфические ограничения на их число, фазы и поляризации, при которых возможно селективное возбуждение одного из энантиомеров. Для молекул с хиральностью динамического типа это автоматически приводит к индуцированию хиральности, а для стабильных молекул может являться первым этапом сценария индуцирования хиральности с последующим использованием одного из сценариев стереомутации.

Выявленные ограничения применены для построения схем индуцирования динамической хиральности в молекуле перекиси водорода с использованием пикосекундных лазерных импульсов ближнего и среднего ИК-диапазона, настроенных в резонанс с различными колебательно-вращательными переходами. Применительно к задаче локального возбуждения хиральности одной молекулы предложена схема с использованием воздействия трёх когерентных импульсов, которая аналитически исследована для случая модельных начальных условий с нулевой вращательной температурой при оптимальных амплитудах импульсов. Показана возможность индуцирования хиральности, величина которой в предположении неподвижности атомов кислорода при лазерном возбуждении характеризуется степенью хиральности ~0.2, в то время как без этого предположения ~0.1. При ненулевой температуре получаем $\sim 10^{-3}$.

В случае некомпланарных импульсов необходимость их когерентного воздействия делает невозможным прямое использование рассмотренной схемы для индуцирования хиральности в объёме с размерами значительно больше длины волны. Тем не менее, использование вращательной структуры делает возможным также и модификацию данной схемы для индуцирования хиральности в макрообъёме. Предложена четырёхимпульсная схема, в которой в приближении заданного поля требования на когерентность полей накачки выполняются на масштабах порядка нескольких сантиметров.

Согласно проведённым исследованиям, более перспективным представляется подход, упрощающий детектирование результатов лазерного воздействия. Он состоит в индуцировании тремя импульсами пространственного распределения хиральности в виде решётки в объёме ~1 мм^3 и регистрации линейного квадрупольного отклика среды на пробный импульс. Путём соответствующего выбора направлений распространения и поляризации импульсов можно добиться выполнения условия их фазового синхронизма, что позволяет разделить направления распространения пробного импульса и генерируемого им на решетке отклика. Для амплитуды отклика соответствующая оценка ~0.5 В/м позволяет надеяться на его детектирование на фоне шумов.

6. Нет

7. Гришанин Б. А.

6. Особая информация

1. нет
2. нет
3. нет
4. нет
5. нет
6. нет
7. нет
8. нет

7. **Сведения о международном сотрудничестве**

1. Грант INTAS, “Storage of quantum information in trapped neutral atoms"
2. № INFO 00-479
3. V. N. Zadkov
4. Inst. of Applied Physics, University of Bonn, Germany;
Aarhus University, Denmark
5. Объём финансирования
6. Аннотационный отчет:

In accordance with the Tasks 1, 2 of the workprogramme, investigations of the atomic -systems as the most perspective carriers of quantum information have been continued in application to such a physical object like samarium atoms. Thus, applicability of the general methods of the quantum markovian theory to the complete 12-level model of CPT resonance in samarium in the presence of either longitudinal or transversal magnetic field has been established on the base of experimental data obtained in the Institute of General Physics of the Russian Academy of Sciences .

In accordance with the Task 3 of the workprogramme the existing basic quantum information measure, such as *coherent* information, has been bound with such a fundamental physical concept as quantum measurement. It has been shown that there exists the most general type of non-demolition quantum measurement, so called *entangling* measurement that combines in the general form the limiting measurement cases when the result of measurement is represented either in the classical form or in the form of quantum entanglement. It has been shown that for the information channel provided by entangling measurement the coherent information is ever positive, that is well defined. These results show that entangling measurement is a kind of the basic transformations of quantum information, as well as the well known CNOT operation of quantum computing.

The concept of compatible information measure, which had been elaborated at the earlier work on this project, has been applied to information analysis of the problems of quantum cryptography. A new quantum cryptography protocol, based on using of all states of the Hilbert state as the quantum alphabet, and a new measure, *compatible information error rate* (CIER), as a counterpart to the quantum bit error rate (QBER), have been proposed. It has been shown that this protocol has two major advantages with respect to the other known ones. It has a better error rate and additionally poses an essentially new quality – no noise threshold, when applied to systems with the infinite–dimensional Hilbert space.

7. нет
1. Грант Университета Васеда, Токио, Япония, для совместных исследований. Финансируется университетом Васеда

2. Номер -- нет
3. Задков В. Н.
4. нет
5. Финансирование осуществляется принимающей стороной
6. Аннотационный отчет: нет
7. нет

Составители отчета:
Б. А. Гришанин, В. Н. Задков