И.И. БЕТЕРОВ

# Некоторые элементы КВАНТОВОЙ ИНФОРМАТИКИ

*Ключевые слова:* квантовая информатика, квантовая криптография, ридберговские атомы
*Key words:* quantum informatics, quantum cryptography, Rydberg atoms



*Создание экспериментальных методов управления отдельными квантовыми системами привело к появлению новой и необычной области науки – квантовой информатики. Отдельные атомы, азотные вакансии, одиночные фотоны могут выступать в роли логических ячеек, но подчиняются особой квантовой логике. Это позволяет создавать невычислимые системы, способные решить невычисляемые с помощью обычных компьютеров задачи. Синтез информатики и квантовой физики рождает новые технологии в передаче и кодировании информации – квантовую криптографию, позволяющую создать абсолютно защищенный канал передачи данных*



БЕТЕРОВ Илья Игоревич – кандидат физико-математических наук, младший научный сотрудник лаборатории нелинейных резонансных процессов и лазерной диагностики Института физики полупроводников СО РАН (Новосибирск). Сфера научных интересов: квантовая информатика, квантовая оптика. Автор и соавтор более 30 научных работ

Исследование отдельных квантовых систем, ставшее возможным благодаря развитию и совершенствованию тонких экспериментальных методов, является принципиально новым и многообещающим подходом к изучению природы. Эксперименты с отдельными ионами и нейтральными атомами, взаимодействующими с одиночными фотонами, в 2012 г. были отмечены Нобелевской премией по физике.

Квантовый характер таких объектов проявляется в том, что они обладают дискретным набором возможных состояний, которые можно «переключать», воздействуя на них электромагнитным излучением. И, фактически, они могут выступать в роли своеобразных логических элементов, на основе которых может быть создана вычислительная система.

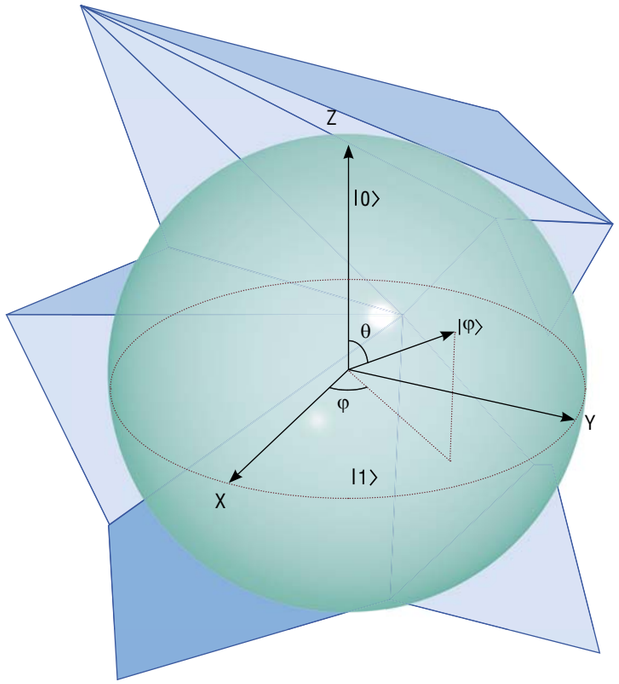
## Вычислить невычислимое

Зачем же нужны квантовые компьютеры? Ведь, казалось бы, обычные вычислительные системы сегодня достаточно мощны, а развитие методов параллельных вычислений позволяет увеличивать скорость расчетов в тысячи раз.

Однако есть ряд задач, решить которые с помощью классических компьютеров в разумные сроки невозможно. Это, в первую очередь, все точные (неэмпирические) квантово-механические расчеты атомов и молекул – если в интересующей нас молекуле содержится $N$ электронов, то необходимое для последовательных вычислений время пропорционально некоторому числу в степени $N$, и уже для нескольких десятков электронов становится больше времени существования Вселенной. Эти трудности обсуждались в 1981 г. Ричардом Фейнманом в лекции «Моделирование физики с использованием компьютеров».

Но еще в 1980 г. в пионерной работе Юрия Манина «Вычислить невычислимое» (Манин, 1980), выдвигалась идея создания «квантовых автоматов» для расчета процесса разворачивания двойной спирали

**Юрий Иванович Манин – российский математик, член-корреспондент РАН, один из основоположников квантовой информатики. С 1960 по 1992 г. работал в отделе алгебры Математического института им. В. А. Стеклова АН СССР. С 2002 г. по настоящее время – профессор Северо-западного университета, США. Является прототипом математика Вечеровского в книге братьев Стругацких «За миллиард лет до конца света»** ***Фото: Archives of the Mathematisches Forschungsinstitut Oberwolfach***




*Кубит* или элемент квантового компьютера представляет собой квантово-механический объект, обладающий двумя возможными состояниями. Например, это может быть атом в магнитном поле с двумя возможными направлениями собственного магнитного момента (спина). Промежуточных направлений спина в квантовом случае нет, измерение будет всегда показывать спин, направленный либо вверх, либо вниз – в зависимости от состояния.

Однако квантовый объект может находиться и в особом состоянии, называемом *суперпозицией*, являющемся суммой основных состояний. В этом случае измерение может дать как спин, направленный вверх (|0⟩), так и направленный вниз (|0⟩) – с определенной вероятностью. *Сфера Блоха* – удобный способ изображать квантовые состояния и их суперпозиции. Суперпозиция двух состояний может быть также записана в следующей форме:

$$\left|\Psi_1\right\rangle = \cos\theta\left|0\right\rangle + e^{i\varphi}\sin\theta\left|1\right\rangle$$

Графически, такое состояние кубита может быть изображено точкой на сфере Блоха. Положение точки задано углами θ и ψ

ДНК – предлагалось использовать для моделирования квантово-механических явлений системы, обладающие не классическими, а квантовыми свойствами.

В те времена, когда были опубликованы работы Манина и Фейнмана, возможность использовать в компьютерах квантовые объекты была лишь гипотетической. Но в последнее время благодаря развитию экспериментальных методик появилась технологическая возможность создавать вычислительные системы, использующие квантовые свойства микроскопических объектов. Естественно, это вызывает огромный интерес у научного сообщества.

## Вроде бы ноль, но немного единица

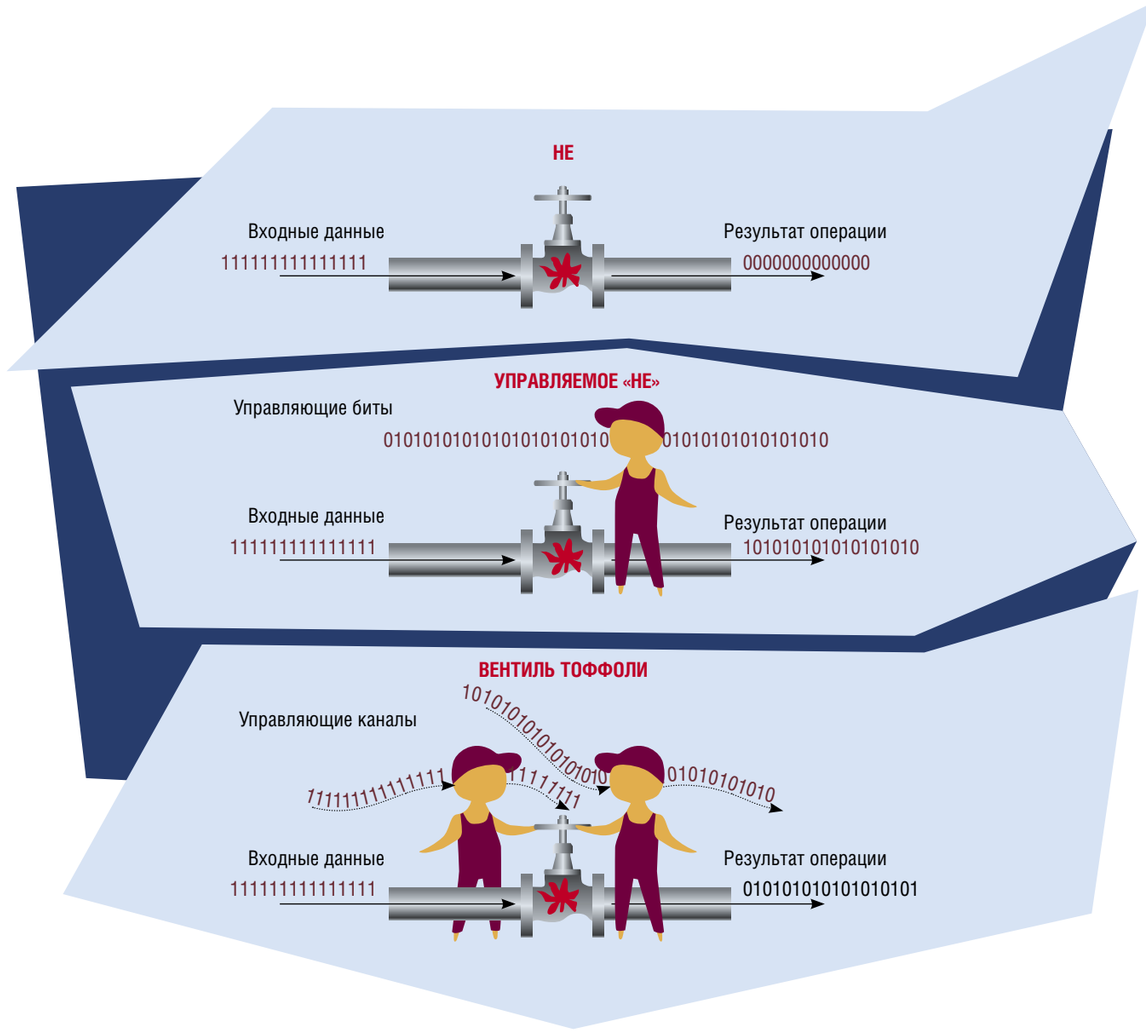
Обычные компьютеры производят математические операции над числами, представленными в двоичном виде, то есть в виде последовательностей нулей и единиц. Двоичная система удобна с точки зрения аппаратной реализации – ячейки памяти, в которых записаны числа, должны иметь всего два состояния – есть напряжение или нет напряжения, есть намагниченность или нет намагниченности и т. д. Процесс вычислений в двоичном счислении сводится к последовательности операций над нулями и единицами, а фактически – к изменению по определенным правилам состояний хранящих их ячеек памяти, регистров.

Квантовый компьютер, как и классический, может быть построен на основе двоичной системы исчисления. Некоторые микроскопические объекты, проявляющие квантовые свойства, обладают двумя состояниями, которые могут быть использованы для кодирования нулей и единиц.

Например, это может быть атом, обладающий собственным магнитным моментом – спином. В магнитном поле такой атом может обладать двумя ориентациями спина – в направлении поля и против поля.

Но, если обычная ячейка памяти содержит либо ноль, либо единицу, квантовый объект может находиться в особом состоянии, называемом *суперпозицией*. В этом случае, если измерять ориентацию спина атома в магнитном поле, можно получить как спин, направленный вверх, так и направленный вниз. И если такой объект использовать как ячейку памяти, то результат считывания с него информации даст с некоторой вероятностью ноль, и с некоторой вероятностью – единицу.

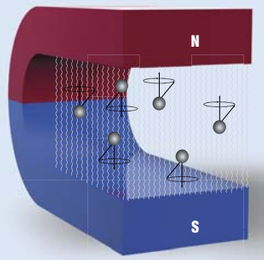
Кроме того, квантовые ячейки памяти, или как их принято называть, *кубиты*, могут взаимодействовать между собой, и находиться в одном общем, коллективном квантовом состоянии. В этом случае состояние нескольких ячеек можно изменять практически мгновенно, воздействуя лишь на одну из них. Этот коллективный характер поведения взаимодействующих кубитов, или *квантового регистра*, как раз и позволяет решать те вычислительные задачи, с которыми не может справиться обычный компьютер.



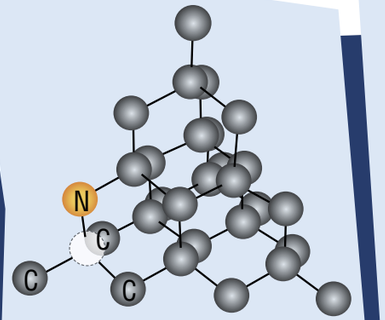

Вычислительная система может быть построена с использованием нескольких типов логических элементов, так называемых вентилей. Наиболее простыми являются вентили «НЕ», которые обращают входное значение, превращая ноль в единицу и наоборот. Результатом работы управляемого «НЕ» будет также обращение входных данных, но только в том случае, если управляющий бит равен 1. Вентиль Тоффоли аналогичен управляемому «НЕ», но у него два управляющих канала. Важной особенностью вентиля Тоффоли является обратимость данных – исходные данные могут быть восстановлены из конечных

Наиболее важные требования к квантовому компьютеру как физической системе – возможность управления состоянием каждого отдельного кубита, и полная изоляция от внешнего окружения. Кубит – объект атомных размеров, и чтобы он помнил свое состояние достаточно долго, необходимо, что бы он был изолирован от внешних воздействий или, как говорят, его состояние сохраняло *когерентность*. Или, по крайней мере, время, за которое происходит разрушение квантовых суперпозиций, должно быть большим, хотя бы в 104 раза превышающим время выполнения одной квантовой логической операции.

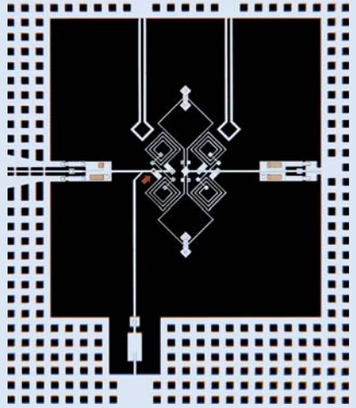
Для реальных вычислений кубиты должны быть объединены в квантовый регистр. Отдельные кубиты регистра должны быть различимы и управляемы извне. Кубиты должны быть строго двухуровневыми и не переходить самопроизвольно на какой-либо третий уровень. Кроме того, должна существовать возможность масштабировать квантовый регистр, т. е. добавлять, если нужно, новые кубиты. Необходимо управлять взаимодействием кубитов друг с другом. Именно взаимодействие, его вид и характеристики влияет на то, какие логические операции сможет выполнять квантовый регистр.




Кубиты могут быть изготовлены на основе ядер атомов. Ядра атомов обладают собственным магнитным моментом – спином.
В магнитном поле спин начинает прецессировать вокруг направления поля, но сохраняет преимущественную ориентацию – вверх или вниз. Два возможных направления спина соответствуют двум состояниям, кодирующим двоичную информацию




Если из структуры алмаза удалить два соседних атома углерода, и на место одного из них поместить атом азота, образуется азотная вакансия, так называемый NV-центр, который благодаря неподеленному электрону атома азота обладает собственным магнитным моментом. Используя спиновое состояние такой вакансии можно кодировать двоичную информацию. А система расположенных рядом вакансий может выступать в роли квантового регистра



Используя сверхпроводящие электрические цепи можно создать «искусственный атом» – *джозефсоновский переход* в центре схемы обладает квантовыми состояниями, и на его основе можно создать кубит – вычислительную ячейку квантового компьютера.
*Courtesy Raymond Simmonds/ National Institute of Standards and Technology (NIST)*

Конечное состояние регистра также должно измеряться достаточно быстро. Немаловажную роль играет эффективность такого измерения – нужно уметь считать информацию с микроскопического объекта атомных размеров.

## Фотонные кубиты

В настоящее время для реализации квантовых вычислений изучаются различные физические системы (Ladd, 2010). Например, в качестве состояний кубита можно использовать направление поляризации фотонов, которое практически не подвержено декогеренции. Логические операции с помощью фотонов можно выполнять, используя пластины из двулучепреломляющих материалов, вращающих поляризацию света. Основная трудность – реализовать взаимодействие отдельных фотонов, что требует оптических сред с очень высокой нелинейностью. Для этого могут быть использованы эффекты электромагнитно-индуцированной прозрачности или взаимодействие атомов с фотонами в микроволновом резонаторе.

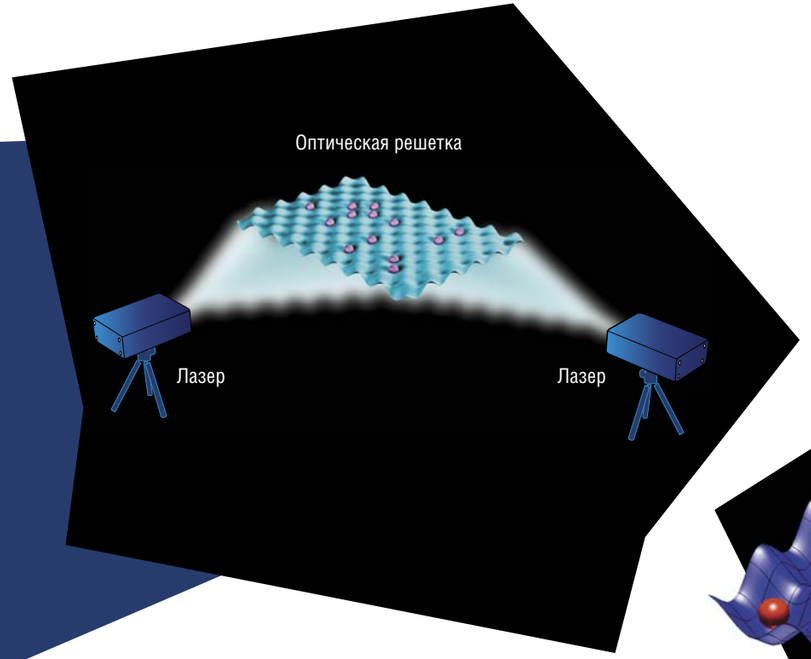
В 2001 г. было показано, что квантовые вычисления могут быть реализованы на основе однофотонных источников, а также детекторов и линейных оптических схем с делителями пучка и интерферирующими одиночными фотонами (Knill, 2001).

Для считывания информации с фотонных кубитов могут быть использованы кремниевые однофотонные детекторы, достигающие квантовой эффективности при комнатной температуре в 70 %. Если же применять сверхпроводящие детекторы, их квантовая эффективность может достигать 95 %, но для этого необходимо охлаждение до 100 мК. Быстродействие сверхпроводящих детекторов может быть радикально увеличено путем использования нанопроволок.

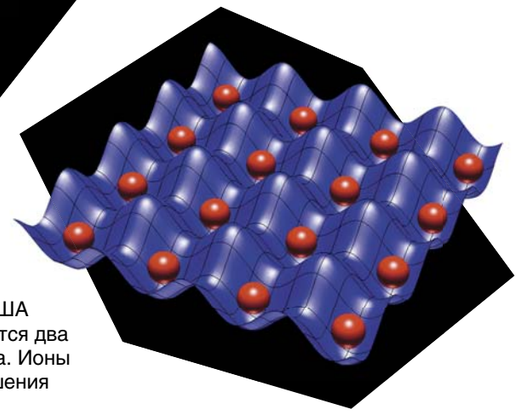
Однако, главный недостаток схем квантовых вычислений, основанных на поляризации фотонов, – большая скорость потерь фотонов, сопоставимая со скоростью декогеренции в альтернативных реализациях квантового компьютера.

Для записи квантовой информации можно использовать сверхтонкие состояния нейтральных атомов, время жизни которых составляет секунды.

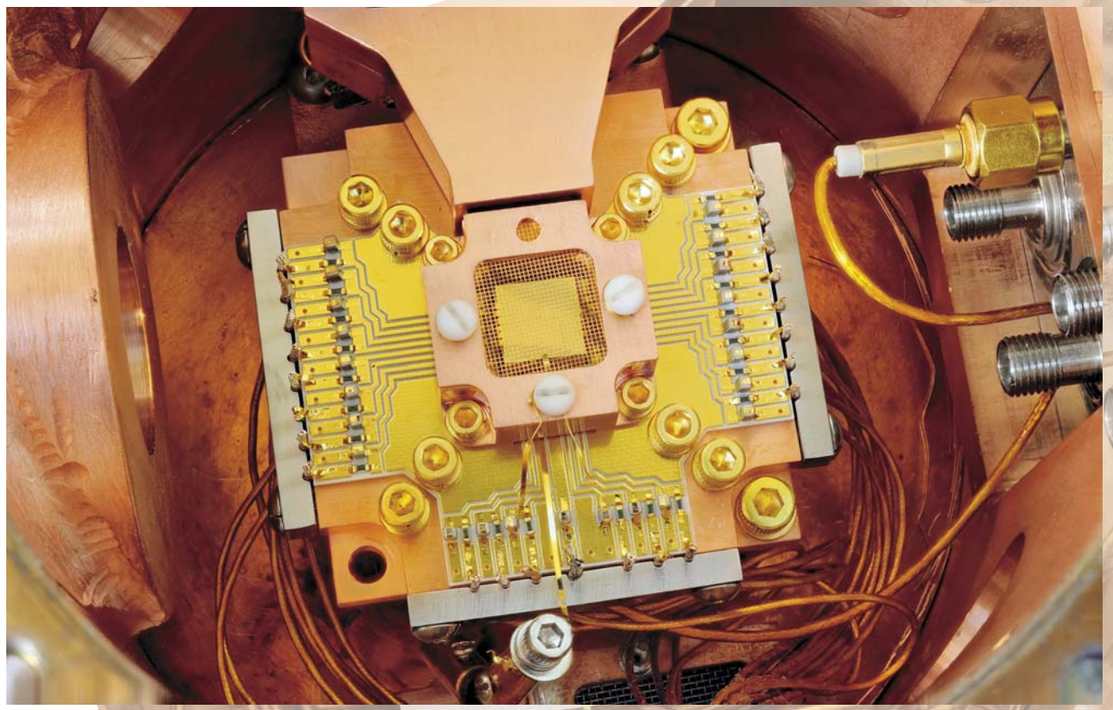





Для захвата и удержания нейтральных атомов можно использовать двумерную оптическую решетку: стоячие волны, образуемые лучами двух лазеров, создают двумерную интерференционную картину.
*Credit: NIST*



Ученые из Национального института стандартов и технологии США (NIST) разработали специальную ловушку, в которой удерживается два иона бериллия, находящиеся на расстоянии 40 мкм друг от друга. Ионы располагаются над золотой пластинкой, окруженной для уменьшения электростатических помех золотой сеткой и медным корпусом.
*Credit: Y. Colombe/NIST*



Дальнодействующие взаимодействия между атомами позволяют выполнять двухкубитовые логические операции, а точность измерения конечного состояния кубита близка к 100 %.

Для создания квантового регистра нейтральные атомы можно захватывать в оптические решетки, образуемые стоячими световыми волнами. Пересечение лучей двух лазеров создает стоячую электромагнитную волну, к пучностям которой притягиваются атомы. Таким образом, из них можно создать пространственно упорядоченные структуры.

В 2010 г. ученым из университета Висконсин-Мэдисон (США) удалось осуществить квантовые логические операции с нейтральными холодными атомами (Isenhower, 2010).

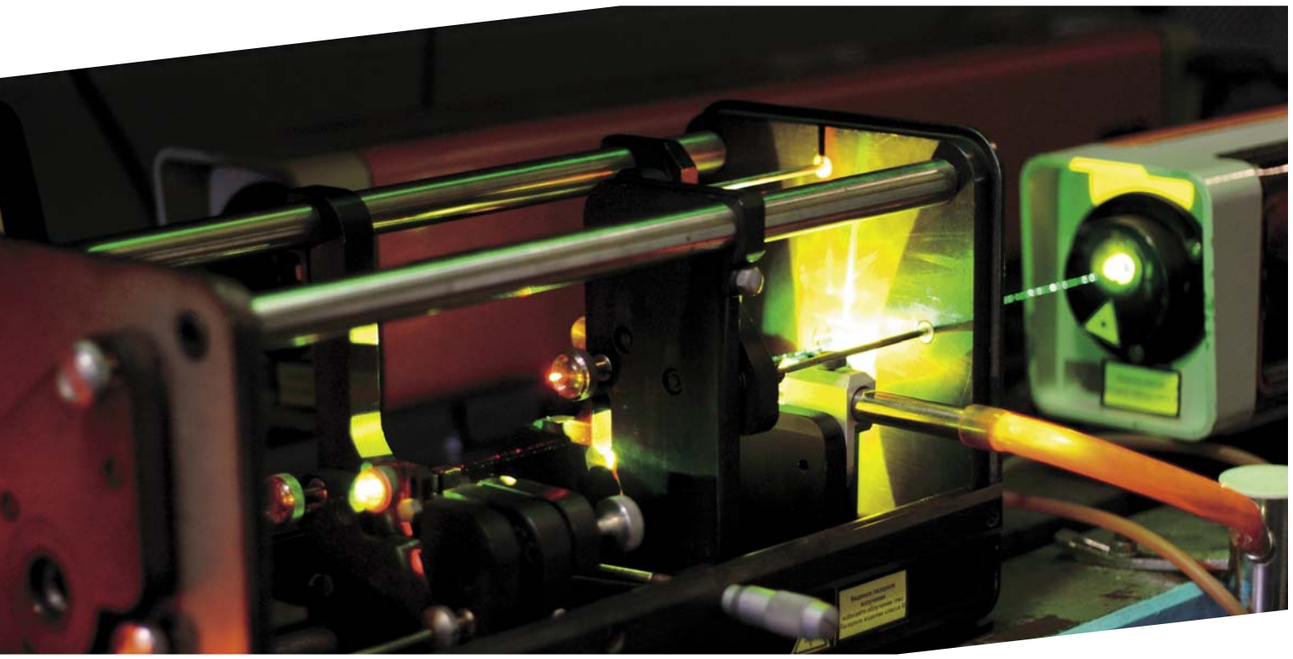
Близкий подход – применение ионов, охлажденных лазерным излучением за счет сил резонансного светового давления и удерживаемых электрическим полем.

Квантовые регистры, составленные из нескольких кубитов, были успешно реализованы в молекулах с использованием ядерного магнитного резонанса (ЯМР). В магнитном поле ядерные спины начинают прецессировать, ориентируясь параллельно или антипараллельно относительно направления магнитного поля. Этим двум возможным направлениям соответствуют логические состояния кубитов. В молекулах частота прецессии для различных атомов будет отличаться. Это позволяет индивидуально адресоваться к отдельным атомам в молекуле, используя резонансное электромагнитное излучение. Простейшие квантовые алгоритмы были продемонстрированы в квантовых ЯМР-компьютерах на основе органических молекул, но масштабирование таких систем пока невозможно.

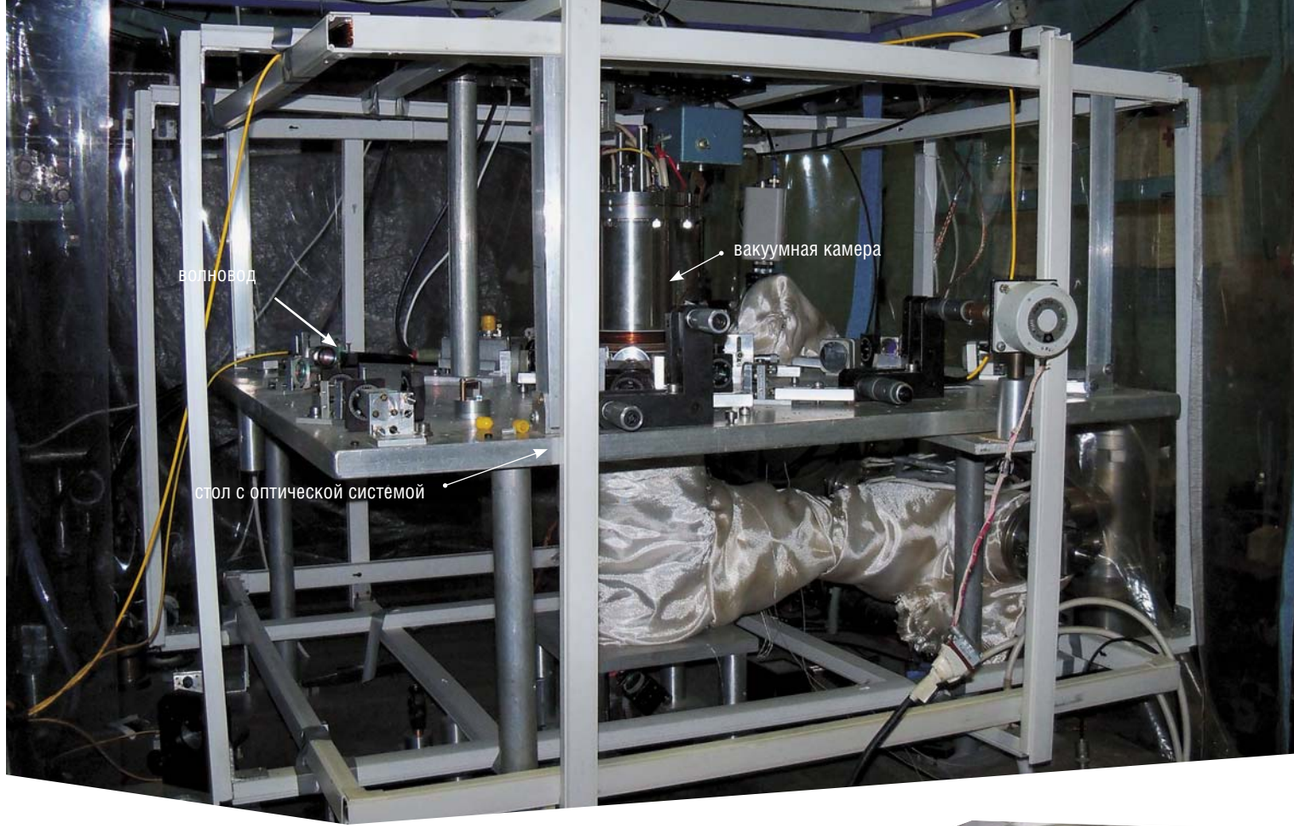
Вместо массивов нейтральных атомов, удерживаемых лазерным излучением, можно использовать массивы «искусственных атомов», например, квантовых точек в полупроводниках (Валиев, 2001). Логические состояния кубита в этом случае представляются двумя состояниями спина электрона в квантовой точке. Также для создания кубитов можно использовать донорные атомы фосфора в полупроводниках или азотные вакансии в алмазах. Спиновые состояния таких кубитов легко управляются внешними электромагнитными полями, время жизни спинового состояния достигает миллисекунд, а спин-спиновые взаимодействия позволяют получить когерентные суперпозиции состояний и реализовать двухкубитовые и более операции.

Широко известным и достаточно перспективным методом реализации квантового компьютера являет-

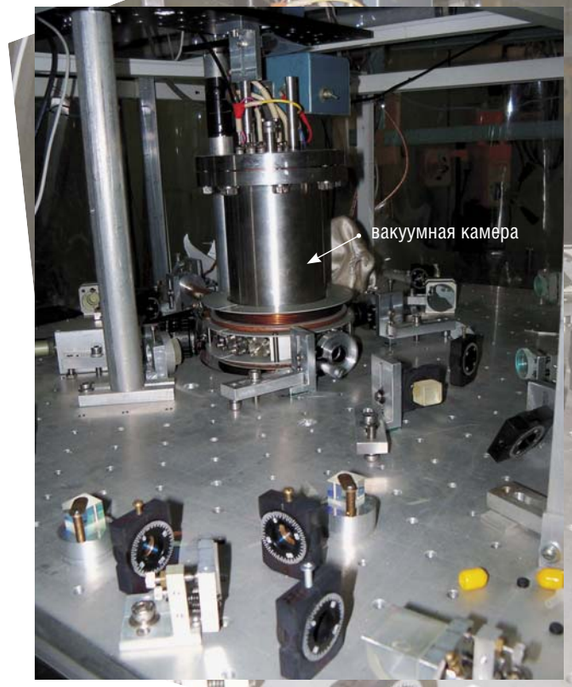
Для возбуждения ридберговских атомов используются перестраиваемые лазеры с частотой повторения импульсов 5 кГц и длительностью импульсов 20—100 нсек








В Институте физики полупроводников СО РАН создана установка для экспериментов с холодными ридберговскими атомами, т. е. атомами, внешний электрон которых находится в высоковозбужденном состоянии. Это позволяет управлять взаимодействием атомов, что необходимо для использования их для создания кубита. В центре установки расположена вакуумная камера, в которой атомы рубидия охлаждаются лазерным излучением до температур в сотни микрокельвин и возбуждаются в ридберговские (высоковозбужденные) состояния. На столе собрана оптическая схема лазерного охлаждения и возбуждения атомов.
Атомы рубидия внутри вакуумной камеры захватываются в магнито-оптическую ловушку, образованную тремя парами ортогональных встречных лазерных пучков и двумя катушками, создающими неоднородное магнитное поле. Затем холодные атомы возбуждаются в ридберговские состояния, с $n$>20, в которых благодаря огромным величинам дипольных моментов они начинают взаимодействовать друг с другом уже на расстояниях порядка 10 мкм. Для регистрации ридберговских атомов используется метод селективной полевой ионизации в момент, когда ридберговский атом, находящийся в данном квантовом состоянии, ионизуется определенным электрическим полем. Этот метод позволяет измерить число возбужденных атомов и определить квантовое состояние, в котором они находятся




В квантовой криптографии передатчик (Алиса) обменивается с приемником (Бобом) информацией по двум каналам – зашифрованному и открытому. Информация кодируется направлением поляризации фотонов, передаваемым в зашифрованный канал. По открытому каналу Боб и Алиса обмениваются информацией о ключе шифрования. Если подслушивающее устройство (Ева) попытается считать информацию, она необратимо исказит ее. Это может быть легко обнаружено Бобом и Алисой

**В криптографии и компьютерной безопасности приняты специальные обозначения для передатчика, приемника и перехватчика сообщений (прослушивающего устройства) – Алиса, Боб и Ева соответственно. Эти обозначения были впервые введены Роном Ривестом в 1978 г. в статье, описывающей криптосистему RSA. Иногда злонамеренного перехватчика называют Мэлори – подразумевается, что Мэлори может не только подслушивать, но и передавать от себя ложную информацию**

ся использование сверхпроводников – в этом случае отдельные кубиты могут иметь мезоскопический характер и содержать до ~$10^{10}$ движущихся квантово коррелированно электронов. Преимущество такого подхода – большие времена декогеренции.

Многие из этих методов в настоящее время развиваются, в частности, в Институте физики полупроводников СО РАН, включая исследование квантовых точек, азотных вакансий в алмазе и взаимодействия ультрахолодных ридберговских атомов.

## Квантовая криптография

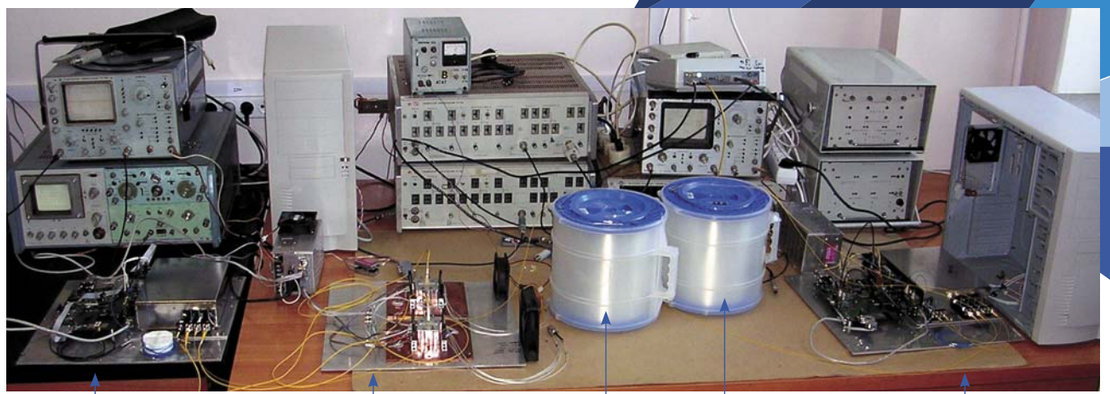
Успехи в создании квантовых логических элементов позволяют перейти к практической реализации принципов квантовой информатики. Хотя квантовые вычислительные системы обладают потенциально огромными возможностями, они, конечно же, не заменят обычные компьютеры. Аналогично, появление лазеров не привело к исчезновению обычных источников света – но они создали возможность решения новых и специфических задач.

К примеру, эксперименты в квантовой оптике позволили продемонстрировать такие фундаментальные физические явления, как квантовая запутанность, – измерение состояния одного квантового объекта может привести к тому, что состояние другого объекта, квантово коррелированного с первым, изменится. Излагаемый далее протокол квантовой криптографии не требует квантовой запутанности – в его основе лежит невозможность копирования квантового состояния.

Передатчик (Алиса) кодирует информацию путем задания той или иной поляризации испускаемых им фотонов, скажем, пропуская их через материал, который вращает плоскость поляризации. Вертикальная поляризация означает «1», а горизонтальная – «0». Приемник (Боб) анализирует полученный фотон с помощью устройства, пропускающего только вертикально поляризованные частицы. И, соответственно, получает «1», когда регистрирует сигнал, или «0», когда сигнала нет.

Допустим, что Алиса испускает также и фотоны, поляризованные по диагонали – под углом в 45 и 135° (в другом базисе). Тогда Боб, анализируя диагонально поляризованный фотон вертикально ориентированным анализатором, будет получать не достоверные значения нулей и единица с некоторой вероятностью ошибется: в 50 % случаев он будет получать «1», в 50 % – «0». Чтобы получить достоверную информацию, приемник






Разработанная в Институте физики полупроводников установка квантовой криптографии. Передатчик (Алиса) передает сигнал по квантовому каналу длиной 25 км приемнику (Боб)

должен знать, какой тип поляризации использовал передатчик при кодировании. Об этом Алиса сообщает Бобу по отдельному, открытому каналу, используя тот или иной протокол.

Если кто-то будет пытаться прослушать канал обмена данными (перехватчик, или Ева), то он заведомо не будет знать базиса. Чтобы остаться незамеченной, Еве необходимо поглотить фотон и испустить такой же точно квант света обратно в канал. Но она не знает, какой был базис поляризации – вертикальный или диагональный, она получила только лишь сигналы «0» или «1». И, соответственно, не может в точности скопировать такой поглощенный фотон, чем вносит дополнительную ошибку в получаемую Бобом информацию. Благодаря этому Алиса и Боб узнают о том, что канал кто-то прослушивает.

Системы секретной передачи данных на основе методов квантовой криптографии производятся компаниями ID Quantique и MagiQ Technologies. Кроме того, исследования в данной области ведутся в интересах органов безопасности ряда стран. В ИФП СО РАН созданы российские прототипы систем квантовой криптографии.

*Литература*

*Валиев К.А., Кокин А.А. Квантовые компьютеры: надежды и реальность. Ижевск: РХД. 2001. 352 с.*

*Манин Ю.И. Вычислимое и невычислимое. М.: Сов. радио, 1980. 128 с.*

*Isenhower L., Urban E., Zhang X.L., et al. // Phys. Rev. Let., 2010. V. 104.*

*Feynman R.P. Engineering and Science/ 1960. P. 22–36 http://www.nobelprize.org/nobel_prizes/physics/laureates/2012/.*

*Feynman R.P. Simulating physics with computers // Int. J. Theor. Phys. 1982. V. 21. P. 467;*

*Feynman R.P. Quantum mechanical computers // Opt. News. 1985. V. 11. P. 11.*

*Knill E., Laflamme R., and Milburn G.J. // Nature. 2001. V. 409. P. 46–52.*

*Ladd T.D., Jelezko F., Laflamme R., et al. // Nature. 2010. V. 464. P. 45.*

*Nature Physics Insight // Quantum Simulation. 2012. V. 8. No 4. Ed. by A. Trabesinger.*

*Nielsen M.A., Chuang I.L. Quantum Computation and Quanum Information. Cambridge, UK: Cambridge University Press. 2010.*

*Vedral V. ,Plenio M.B. Basics of Quantum Computation, Progress in Quantum Electronics. Pergamon. 1998. V. 22. P. 1–39.*

*DiVincenzo D.P. Quantum computation // Science. 1995. V. 270. P. 255;*

*DiVincenzo D.P. The Physical Implementation of Quantum Computation // Fortschr. Phys. 2000. V. 48. P. 771.*

.