



МОНИТОРИНГ

ЦНТИБ – филиал ОАО «РЖД»

КВАНТОВЫЕ СЕТИ

№ 4/АПРЕЛЬ 2020

СОДЕРЖАНИЕ

В мае Samsung выпустит первый в мире смартфон с квантовой криптографией.....	2
Квантовая запутанность помогла улучшить геолокацию	3
Создатель квантового компьютера Google покинул корпорацию.....	4
«Квантовый интернет» все ближе: физики нашли новый метод генерации квантово-запутанных фотонов.....	4
Квантовые вычисления для анализа данных LHC	6
Intel и QuTech создали квантовый компьютер, работающий при температурах выше одного кельвина.....	8
Microsoft и PsiQuantum объединят усилия для создания отказоустойчивого квантового компьютера.....	9
Загадочные майорановские фермионы: их обнаружение на золоте готовит квантовый компьютерный прорыв.....	10
Оптический резонатор поможет создать квантовый интернет.....	11
Редкоземельные металлы помогут физикам построить большие квантовые сети	13
Коронавирус попробуют победить квантовыми компьютерами.....	15
Алмаз станет основой квантового интернета: новая система управляет субатомными частицами.....	16
Ученые России повысили безопасность квантовой криптографии.....	17
РКЦ: квантовый компьютер и блокчейн. Наука России и ее ученые.....	19
Ученые создали квантовые точки, расстреляв графен потоком ионов	22

В мае Samsung выпустит первый в мире смартфон с квантовой криптографией

Традиционно квантовая криптография ассоциируется с оптическими линиями связи, поскольку она основана на переносе информации одиночными фотонами. А как же быть со смартфонами? Неужели мобильную связь нельзя защитить от потенциально любого вторжения? В мае компания Samsung и оператор SK Telecom сметут это ограничение и представят первый в мире смартфон с квантовой криптографией.

Как сообщают южнокорейские источники, компания Samsung готовит смартфон с рабочим названием GALAXY Quantum с беспрецедентным уровнем защиты от прослушивания и взлома. Это будет модификация серийной модели Samsung A71 5G, которая ранее в этом году уже поступила в международную продажу. Но только в отличие от своих обычных собратьев модель GALAXY Quantum будет нести в себе квантово-криптографический чип QRNG.

Чип QRNG – это генератор случайных квантовых чисел или, по-английски, Quantum Random Number Generator. Вероятно, это решение швейцарской компании ID Quantique (IDQ), в которую оператор SK Telecom инвестировал два года назад. Чип QRNG в составе смартфона генерирует последовательность чисел, которые затем ложатся в основу сильных паролей. Утверждается, что числа настолько случайны, что ни один алгоритм в мире не сможет подстроиться под работу генератора.

Генератор QRNG как и положено квантовой криптографии работает с фотонами, но только не с одиночными, а со среднестатистической выборкой из массива фотонов. По словам разработчиков, надёжность шифрования с использованием QRNG будет так же высока, как и в случае классического распределения квантовых ключей шифрования с помощью одиночных фотонов. Кроме защиты чип QRNG позволит также реализовать другой эффект квантовой криптографии, а именно уведомление о попытке перехвата сообщения.

Смартфон Samsung GALAXY Quantum будет продаваться только в Южной Корее (это ограничение юрисдикции оператора, надо полагать). Цена вопроса на местном рынке составит от 500 до 600 тыс. вон, или от 400 до 500 долларов. В международной продаже обычная версия Samsung A71 5G стоит 600 долларов, так что с ценой за пределами страны ясности пока нет. Теоретически, «квантовая криптография» должна потянуть цену аппарата вверх.

Квантовая запутанность помогла улучшить геолокацию

Исследователи из Аризонского университета продемонстрировали, что комбинация радиофотонного зондирования и квантовой метрологии может позволить создать радары с невиданной до сих пор точностью позиционирования. О своей разработке исследователи рассказали в журнале *Physical Review Letters*.

Традиционные радары преобразуют информацию из радиочастотных сигналов в электрический ток. Однако оптическое зондирование, которое использует фотоны – кванты света – для передачи информации, гораздо более эффективно. Мало того, что фотоны позволяют получить больше данных, чем электроны, что дает большую полосу пропускания сигнала, зондирование на основе фотоники может передавать этот сигнал на гораздо большие расстояния, чем зондирование на основе электроники, и с меньшим количеством помех. Поскольку оптические сигналы имеют так много преимуществ, авторы новой работы решили использовать электрооптический преобразователь для преобразования радиоволн в оптическую область с помощью метода радиофотонного зондирования.

После преобразования геолокационных данных в оптический диапазон исследователи применили метод, называемый квантовой метрологией. Обычно точность датчика ограничивается стандартным квантовым пределом – например, GPS-системы смартфона точны в масштабе 5 метров. Квантовая метрология использует запутанные частицы, чтобы преодолеть стандартный квантовый предел и провести сверхчувствительные измерения.

Как это работает? Запутанные частицы связаны друг с другом, поэтому все, что происходит с одной частицей, влияет на запутанные с ней, пока проводятся соответствующие измерения. Представьте себе руководителя и сотрудника, работающих вместе над проектом. Поскольку для сотрудника требуется время, чтобы поделиться информацией со своим руководителем с помощью таких методов, как электронная почта и встречи, эффективность их партнерства ограничена. Но если бы эти двое могли объединить свои мозги, сотрудник и руководитель мгновенно обменивались бы информацией и могли работать более эффективно.

Почти во всех предыдущих примерах квантовой метрологии, включая интерферометр LIGO, использовался только один датчик. Авторы новой работы впервые продемонстрировали, что сеть из трех датчиков можно запутать друг с другом. Все они при этом получают информацию от зондов и обрабатывают ее одновременно, сохраняя связь друг с другом.

Хотя в эксперименте использовались только три датчика, метод может быть применим к сетям из сотен датчиков. Этот метод может быть применен к любому применению, которое требует наличия массива или сети датчиков».

Источник: indicator.ru, 21.04.2020

Создатель квантового компьютера Google покинул корпорацию

Профессор Джон Мартинис, создатель квантового компьютера Sycamore, покинул корпорацию Google. Специалист работал в лаборатории искусственного интеллекта, его считают лидером в данном сегменте инновационных разработок.

Учёный в интервью изданию The Wired рассказал, что его целью стало создание компьютера новой генерации, причём сам проект реализовывался не целенаправленно. Уход из корпорации специалист считает оптимальным решением, причём для обеих сторон. О Мартинисе стали говорить в 2014 году, когда он начал работать в лаборатории квантового интеллекта Google. Специалист тогда приступил к созданию инновационной ЭВМ, предназначенной для различных вычислений. Через три года профессор объявил, что достиг так называемого «квантового превосходства». Речь шла о разработке машины, работу которой невозможно просчитать, используя актуальные компьютеры. Профессор преодолел названный уровень в 2019 году, когда Sycamore успешно справился с «нерешаемой» задачей по выработке случайных чисел. Вскоре учёного отстранили от должности и перевели в ранг консультанта. Далее появились разногласия с Хартмутом Невеном – основателем названного проекта в Google, вслед за этим Джон Мартинис покинул корпорацию.

Источник: actualnews.org , 23.04.2020

«Квантовый интернет» все ближе: физики нашли новый метод генерации квантово-запутанных фотонов

Ученые нашли очень полезный новый способ генерации квантово-запутанных фотонов, совершенно необходимых для создания сверхбезопасного, супербыстрого «квантового интернета».

Квантовая запутанность – это явление, когда две частицы (например, фотоны) связаны друг с другом, независимо от физического расстояния между

ними. Если что-то происходит с одной из частиц, что-то должно случиться и с другой.

Хотя физики до сих пор не до конца понимают, как именно происходит запутывание, это явление открывает возможность для связи на больших расстояниях с квантовым питанием – где сдвиги в частицах в одном месте приводят к сдвигам в запутанных частицах на огромном расстоянии.

Это конкретное исследование предполагает, что квантово-запутанные фотоны используются в качестве квантового распределения ключей (QKD), своего рода низкоуровневого квантового Интернета, где классические данные в форме единиц и нулей получают дополнительный уровень конфиденциальности и безопасности благодаря квантовой физике.

До сих пор запутанные фотоны, используемые для этих методов шифрования, были ограничены диапазоном длин волн ближнего инфракрасного излучения от 700 до 1550 нм, что делает их уязвимыми для помех от поглощающих свет газов и солнечного излучения.

Другими словами, подключение для передачи данных работает только ночью, что само по себе не идеально для того, что предположительно является интернет-инфраструктурой следующего поколения.

Новое исследование показывает, как генерировать и обнаруживать запутанные фотоны на более длинной волне 2,1 микрометра, которая защищена от таких помех. Конечный результат – гораздо более надежный и стабильный канал связи.

«Мы продемонстрировали, что запутанные поляризацией пары фотонов могут генерироваться, управляться и обнаруживаться с помощью нашего подхода», – пишут исследователи в своей опубликованной статье.

«Эта работа предоставляет новую платформу для квантовой оптики и прокладывает путь технологическим приложениям для квантового зондирования и квантовой защищенной связи на большие расстояния в этом режиме длин волн».

Для достижения этой цели исследователи использовали нелинейный кристалл из ниобата лития: запутанные пары фотонов создавались с помощью ультракоротких световых импульсов от лазера, направленного в кристалл.

Квантовый интернет, если мы сможем понять, как его создать, обещает быть во много раз более мощным, более безопасным и более приватным, чем все, что мы имеем сегодня. Например, любые попытки взлома мгновенно разорвали бы соответствующее соединение – неплохая сеть безопасности.

Мы все еще далеки от реализации этой мечты, но инновации, подобные описанным, неуклонно сближают нас и превращают квантовые вычисления из гипотезы в реальность.

«Следующим важным шагом будет миниатюризация этой системы путем преобразования ее в интегрированные фотонные устройства, что сделает ее пригодной для массового производства и для использования в других прикладных сценариях», – говорит квантовый физик Майкл Куес из Ганноверского университета им. Лейбница в Германии.

Источник: rwspace.ru, 19.04.2020

Квантовые вычисления для анализа данных LHC

Международное сотрудничество изучает, как квантовые вычисления могут быть использованы для анализа огромного количества данных, полученных в результате экспериментов на Большом адронном коллайдере (LHC) в ЦЕРН. Исследователи показали, что «машина квантовых опорных векторов» может помочь физикам разобраться в огромном количестве данных, генерируемой в ЦЕРН.

Эксперименты на LHC могут дать ошеломляющий один петабайт в секунду данных из примерно одного миллиарда столкновений частиц в секунду. Многие из этих данных должны быть отброшены, потому что эксперименты могут сосредоточиться только на подмножестве событий столкновения. Тем не менее, анализ данных CERN в настоящее время опирается на около миллиона процессорных ядер, работающих в 170 компьютерных центрах по всему миру.

LHC в настоящее время проходит модернизацию, которая увеличит частоту столкновений. Ожидается, что вычислительная мощность, необходимая для обработки и анализа дополнительных данных, к 2027 году возрастет в 50-100 раз. В то время как усовершенствования в современных технологиях устранят небольшую часть этого разрыва, исследователям в ЦЕРН придется искать новые и более разумные способы, для решения вычислительных задач – вот где приходят квантовые вычисления.

В 2001 году лаборатория создала государственно-частное партнерство под названием CERN openlab, чтобы ускорить разработку новых компьютерных технологий, необходимых исследовательскому сообществу CERN. Одной из нескольких ведущих технологических компаний, вовлеченных в это сотрудничество, является IBM, которая также является крупным игроком в области исследований и разработок в области квантовых вычислений. Квантовые компьютеры могут, в принципе, решать определенные проблемы гораздо быстрее, чем обычные компьютеры. Хотя для создания практических квантовых компьютеров необходимо преодолеть значительные

технологические проблемы, IBM и несколько других компаний создали коммерческие квантовые компьютеры, которые уже могут выполнять вычисления.

Федерико Карминати (Federico Carminati), физик-компьютерщик в CERN и главный директор по инновациям CERN openlab, объясняет интерес лаборатории к квантовому решению: «Мы смотрим на квантовые вычисления, поскольку они могут обеспечить возможное решение нашей проблемы вычислительной мощности». Он рассказал Physics World, что CERN openlab не хочет завтра пытаться внедрить мощный квантовый компьютер, а скорее играет в «игру средней продолжительности», чтобы увидеть, что возможно. «Мы можем попытаться смоделировать ядерную физику, рассеяние ядер, возможно, даже смоделировать кварки и фундаментальные взаимодействия», – объясняет он.

CERN openlab и IBM начали совместную работу над квантовыми вычислениями в 2018 году. Теперь физики из Университета Висконсина во главе с Сау Лань Ву (Sau Lan Wu), CERN, IBM Research в Цюрихе и Fermilab около Чикаго, изучают, как можно использовать машинное обучение квантовой машины для идентификации события бозона Хиггса в данных столкновения LHC.

Используя квантовые компьютеры и квантовые компьютерные симуляторы IBM, команда решила применить метод квантовых опорных векторов к этой задаче. Это квантовая версия управляемой системы машинного обучения, которая используется для классификации данных.

«Мы проанализировали смоделированные данные экспериментов Хиггса с целью определения наиболее подходящего алгоритма обучения квантовой машины для выбора интересующих событий, который можно в дальнейшем проанализировать с использованием традиционных, классических алгоритмов», – объясняет Панагиотис Баркауцос (Panagiotis Barkoutsos) из IBM Research.

Предварительные результаты эксперимента были очень многообещающими. Пять квантовых битов (кубитов) на квантовом компьютере IBM и квантовых симуляторах были применены к данным. «С нашей квантовой машиной опорных векторов, мы проанализировали маленький образец обучения с более чем 40 функциями и пятью тренировочными переменными. Результаты очень близки, а иногда даже лучше, чем результаты, полученные с использованием самых известных эквивалентных классических классификаторов, и были получены эффективно и в короткие сроки», – говорит Баркауцос.

Обнаружение бозона Хиггса в данных LHC часто сравнивают с «поиском иголки в стоге сена», учитывая его очень слабый сигнал. Действительно,

большая часть вычислительного времени, использованного физиками LHC, до сих пор уходила на анализ бозона Хиггса.

Важной целью LHC является проверка Стандартной модели физики элементарных частиц до предела в поисках новой физики – и квантовые вычисления могут сыграть важную роль. «Это именно то, к чему мы стремимся, очень точный анализ сложных данных, которые могут привести к аномалиям, которые помогут нам улучшить Стандартную модель или выйти за ее пределы», – заключает Карминати.

Работа ведется с использованием большего числа кубитов, большего количества обучающих переменных и больших размеров выборки.

Источник: ko.com.ua, 18.04.2020

Intel и QuTech создали квантовый компьютер, работающий при температурах выше одного кельвина

Компания Intel совместно со специалистами нидерландского научно-исследовательского института QuTech успешно продемонстрировали возможность использования спиновых кубитов (их состояние определяется спином атомных ядер) на основе кремниевых квантовых точек при температурах выше одного кельвина.

Квантовые компьютеры способны превзойти свои классические аналоги во многих задачах. Однако для возможности практического применения квантовых вычислительных систем необходимо обладать возможностью контролировать миллионы кубитов, в которых содержится информация.

Современные конструкции квантовых систем ограничены общим размером, надёжностью (точностью) кубитных операций, а также невероятной сложностью и дороговизной электроники, необходимой для управления квантовыми вычислениями в больших масштабах.

Для возможности хранения информации кубиты должны охлаждаться до температуры близкой к абсолютному нулю (-273°C или 0 кельвинов). Тем не менее, возможность повышения температуры, при которой смогут работать кубиты, имеет решающее значение для масштабирования квантовых вычислений. Ранее было показано, что квантовый компьютер работает только в диапазоне температур милликельвинов, то есть не более чем на долю градуса выше абсолютного нуля.

Учёные и инженеры Intel вместе с нидерландскими коллегами из QuTech смогли впервые продемонстрировать возможность работы кубитов на основе

кремниевых квантовых точек при температурах выше 1 кельвина с сохранением высокого уровня надёжности и когерентности (рис. 1).

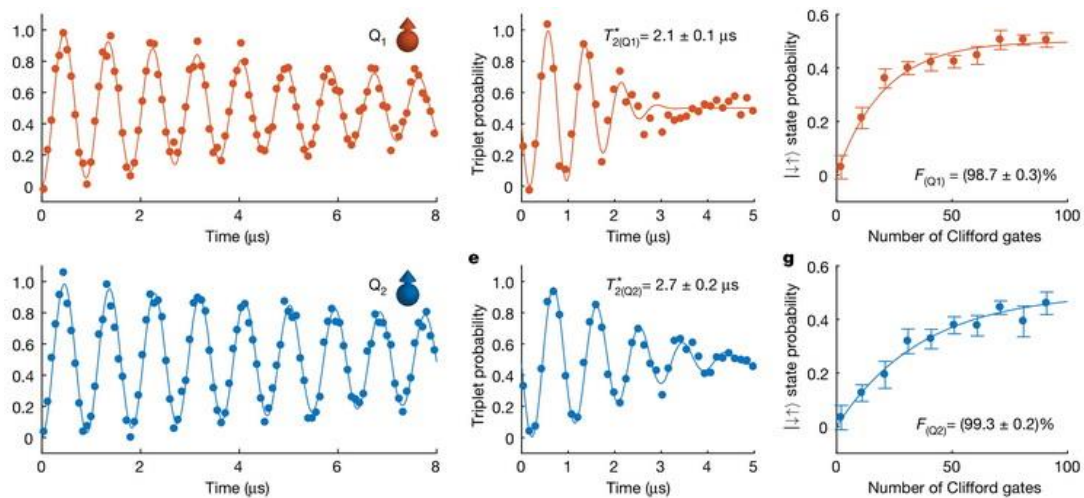


Рис. 1. Время когерентности и надёжность однокубитной операции для двух кубитов (красный и синий) при температуре 1,1 кельвин

Более того, исследователи реализовали универсальную квантовую логику на основе двухкубитного процессора и продемонстрировали возможность её работы при температуре 1,1 кельвин с уровнем надёжности однокубитной операции в 99,3% и временем когеренции 2 микросекунды. Ранее подобное было возможно только при температуре 40 милликельвинов.

Результат Intel и QuTech показывает, что квантовые вычисления обладают потенциалом масштабируемости, могут стать более простыми и, главное, более доступными.

Источник: *3dnews.ru*, 15.04.2020

Microsoft и PsiQuantum объединят усилия для создания отказоустойчивого квантового компьютера

Microsoft уже на протяжении нескольких лет работает над развитием квантовых вычислений и созданием квантовых компьютеров.

В прошлом году Microsoft анонсировала создание Azure Quantum – полнофункциональной открытой облачной экосистемы по теме квантовых вычислений. Второе направление – поддержка становления Quantum Network – глобального сообщества для продвижения квантовых вычислений и разработки специального набора программных инструментов Quantum Development Kit, с помощью которого планируется предоставлять доступ к службам Azure и средствам квантового программирования и разработки алгоритмов.

Новое направление на «квантовом» пути, который показало Microsoft – это совместные работы со стартапом PsiQuantum по созданию квантового компьютера на обычных кремниевых чипах. Ожидается, что на его базе будет вестись обработка информации с использованием фотонной техники и традиционной электроники. Инвестиции в поддержку PsiQuantum были сделаны через M12, специальное венчурное подразделение Microsoft.

Известно, что в PsiQuantum в настоящее время работает команда из более 100 инженеров. Они имеют богатый опыт производства кремневых систем и ведения квантовых вычислений.

Подход PsiQuantum отличается от того, чем до сих пор занималась Microsoft по топологическим кубитам. Подход Microsoft связан с развитием технологии коррекции ошибок при использовании оборудования для квантовых вычислений с топологической защитой от локальных помех.

Как отметил Самир Кумар из M12, до сих пор PsiQuantum и Microsoft занимались различными инженерными задачами. Теперь компании постараются объединить свои усилия для разработки «масштабируемого, отказоустойчивого квантового компьютера».

Ранее редакция THG.ru опубликовала обзор лучшей материнской платы. Выбрать лучшую материнскую плату непросто – для кого-то лучшей может быть самая доступная материнская плата, для других – самая функциональная. Мы стараемся учитывать все факторы и публикуем регулярно обновляемый материал, в котором стараемся рекомендовать действительно лучшую материнскую плату любой функциональности, под любой процессорный разъем, в любой ценовой категории – от самых дешёвых до топового сегмента.

Источник: thg.ru, 12.04.2020

Загадочные майорановские фермионы: их обнаружение на золоте готовит квантовый компьютерный прорыв

Ученые Массачусетского технологического Университета заявили об удивительном открытии. Ими обнаружены частицы таинственного майорановского фермиона на золоте. Это открытие позволит создать совершенно новый вид надежных кубитов для квантовых вычислений. Ученые наблюдали свидетельства майорановских фермионов на поверхности обычного металла – золота.

Теория гласит, что они являются собственной античастицей. Обнаружить майорановские фермионы на платформе удалось впервые, и она может быть потенциально увеличена. Что такое майорановские частицы? Это своеобразные

элементарные элементы. Впервые они были в теории предсказаны физиком из Италии Этторе Майорана в 1937 году.

Частицы принадлежат к группе фермионов, она также включает в себя электроны, нейтроны и протоны. Фермионы нейтральны, они не имеют электрического заряда. Их называют экзотическими частицами, которые могут выступать в качестве квазичастиц в топологических сверхпроводниках и представлять собой идеальные строительные блоки для топологических квантовых компьютеров.

Их обнаружение на платформе дают совершенно новые возможности. Это важный шаг к изоляции частиц, защищенных от ошибок кубитов, предназначенных для квантовых элементов.

Английский физик Пол Дирак предсказал, что все фермионные фундаментальные частицы должны иметь аналог, или своего двойника, где-то во вселенной в форме античастицы.

Современные ученые из Массачусетского технологического университета обнаружили присутствие свидетельств майорановских фермионов в материальной системе. Она состоит из нанопроволок золота, которые были выращены на сверхпроводящем материале ванадия и сульфиде европия.

Сканируя их поверхность, исследователи обнаружили характерные пики сигнала, свидетельствующие о нулевой энергии, на поверхности золота. Согласно теории, там могут генерироваться только пары майорановских фермионов.

Джагадиш Мудера, старший научный сотрудник физического факультета Массачусетского технологического института, говорит, что майорановские фермионы считались нереальной экзотикой, а теперь наука смогла их увидеть в очень простом материале – в золоте. И это свидетельствует о том, что они есть, они стабильны и они легко масштабируемые.

Источник: ekovolga.com, 10.04.2020

Оптический резонатор поможет создать квантовый интернет

Инженеры из Калифорнийского технологического института показали, что атомы в полостях оптических резонаторов могут стать одной из основных технологий, обеспечивающих функционирование квантового интернета. Свою работу исследователи опубликовали в журнале Nature.

Квантовые сети будут соединять квантовые компьютеры через специальную систему, которая обеспечит соединение между ними. В теории квантовые компьютеры однажды смогут выполнять определенные функции

быстрее, чем классические вычислительные системы, используя свойства квантовой механики, такие как суперпозиция состояний, которая позволяет квантовым битам быть одновременно нулем и единицей.

Как и в случае с классическими компьютерами, ученые хотели бы подключать несколько квантовых компьютеров для обмена данными и совместной работы – создать своего рода «квантовый интернет». Это открыло бы двери для множества применений, включая распределенные квантовые вычисления и зашифрованную передачу информации. Однако такая сеть должна быть способна передавать информацию между двумя устройствами без изменения квантовых свойств передаваемой информации.

Имеющаяся сегодня модель работает следующим образом: один атом или ион действует как кубит и хранит информацию о своем квантовом свойстве, таком как спин. Чтобы прочитать эту информацию и передать ее в другое место, атом нужно возбудить импульсом света, заставляя его испустить фотон, спин которого запутан со спином атома и равен ему. Затем фотон может передавать информацию, связанную с атомом, на большое расстояние по оптоволоконному кабелю. Но сделать это сложнее, чем кажется. Большинство атомов чувствительны к колебаниям магнитного и электрического полей, что приводит к ошибкам при работе основанных на них устройств.

Чтобы преодолеть эту проблему, исследователи из Калтеха построили нанофотонный резонатор – стержень длиной около 10 мкм с вытравленным на его поверхности специальным рисунком, созданный из кристалла ортованадата иттрия. Затем ученые поместили в центр ион редкоземельного металла иттербия Yb^{3+} . При пропускании излучения через такой резонатор он несколько раз проходит вдоль стержня и в конечном итоге, потеряв достаточно энергии, поглощается ионом иттербия. Авторы также показали, что полости в материале изменяют окружающую среду иона, благодаря чему излученный им фотон до 99% времени может находиться в материале, а ученые тем временем могут измерять его свойства.

Кроме того, ионы иттербия способны хранить информацию в своем спине в течение 30 миллисекунд. Этого достаточно, чтобы передавать информацию через всю континентальную часть США. В настоящее время команда сосредоточена на создании строительных блоков квантовой сети. Затем они надеются расширить свои эксперименты и соединить два квантовых бита на большом расстоянии друг от друга.

Редкоземельные металлы помогут физикам построить большие квантовые сети

Американские физики впервые реализовали высококогерентный контроль и считывание одиночных ионов иттербия, помещенных в оптический резонатор. Этот эксперимент открывает дорогу к созданию масштабных квантовых сетей, основанных на ионах. Работа представлена в журнале Nature.

Распределение квантовой запутанности на большие расстояния по оптическим квантовым сетям – это один из ключевых протоколов квантовой криптографии и распределенных квантовых вычислений. Твердотельные источники запутанности, связанные с оптическими резонаторами, являются перспективными кандидатами для реализации масштабируемых квантовых сетей. В частности, физики исследовали такие системы, как квантовые точки и дефекты в алмазе или карбиде кремния.

Однако, до сих пор масштабирование твердотельных систем остается под вопросом – центральной проблемой является поиск систем с контролируруемыми когерентными оптическими и спиновыми переходами. Не так давно было обнаружено, что редкоземельные металлы в кристалле обладают достаточно когерентностью и, теоретически, могут быть связаны с оптическим резонатором.

Однако, до сих пор масштабирование твердотельных систем остается под вопросом – центральной проблемой является поиск систем с контролируруемыми когерентными оптическими и спиновыми переходами. Не так давно было обнаружено, что редкоземельные металлы в кристалле обладают достаточно когерентностью и, теоретически, могут быть связаны с оптическим резонатором.

Группа американских физиков под руководством профессора Андрея Фараона (Andrei Faraon) использовала ионы иттербия, изготовленные в кристалле, для демонстрации высокой когерентности спинового состояния и быстрого считывания состояния в оптическом резонаторе.

В качестве кубитного состояния, на основе которого строилась запутанность, ученые использовали связанные состояния электрона с ядром иона. Возбуждение кубита происходило с помощью микроволнового излучения, а измерения производились с помощью дополнительного импульса, приложенного к возбужденному состоянию кубита, которое приводило к флюоресценции иона, только если кубит находился в возбужденном состоянии. Измерения проводились с помощью сверхпроводящего детектора фотонов в криостате растворения на температуре 40 милликельвин (рис. 2, 3).

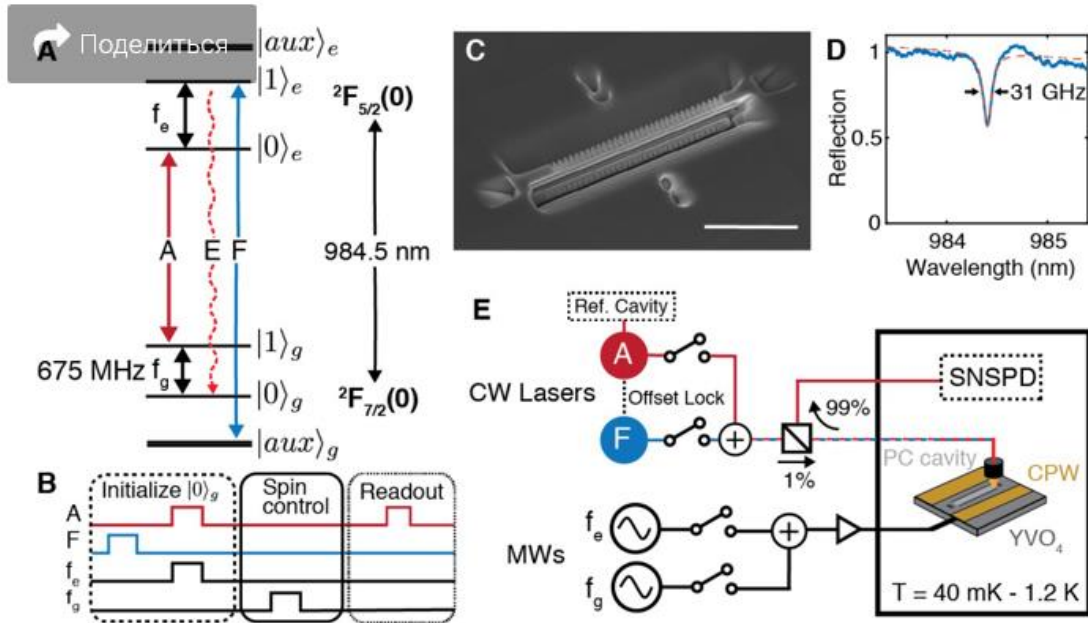


Рис. 2. А. Схема оптических переходов в ионе, связанном с резонатором. В. Характерная последовательность микроволновых импульсов. С. Фотография кристалла с ионами иттербия. D. Спектр отражения резонатора. Е. Экспериментальная схема.

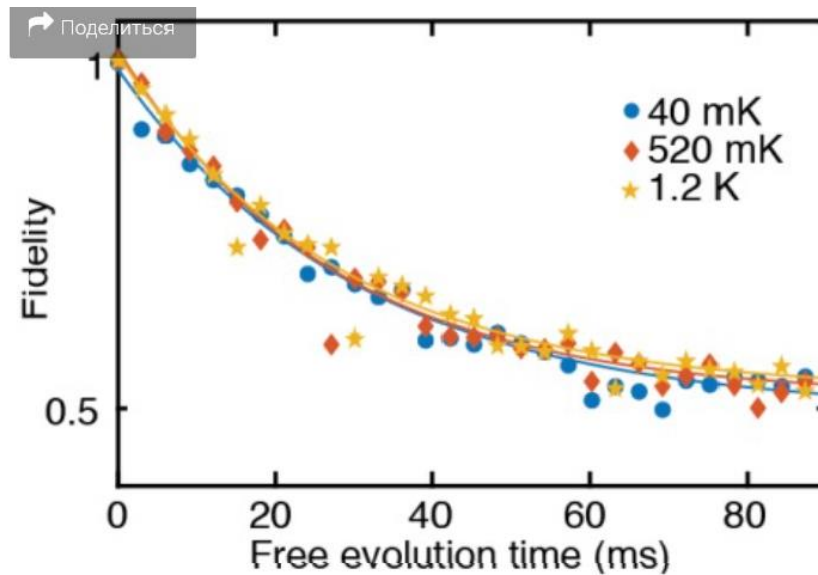


Рис. 3. Измерения времени когерентности при разной температуре детектора.

Оптический резонатор, в которой был помещен ион, позволяет когерентно контролировать квантовое состояние иона, что было экспериментально подтверждено с помощью оптических осцилляций Раби.

Построенная система обладает временем когерентности 30 миллисекунд – за это время фотоны могут пролететь тысячи километров по оптоволокну, что достаточно для создания масштабных квантовых сетей. Также ученые показали, что когерентность сохраняется и при температуре детектора 1,2 кельвина, что позволяет использовать дешевые гелиевые криостаты.

В последнее время физики много работают над созданием квантовой коммуникации. Недавно мы писали о том, что ученым из Китая впервые удалось запутать два узла квантовой памяти через оптоволокно длиной 50 километров, а группе из Швейцарии удалось построить рекордно длинную микроволновую квантовую связь.

Источник: nplus1.ru, 01.04.2020

Коронавирус попробуют победить квантовыми компьютерами

Канадский разработчик квантовых компьютеров D-Wave откроет всем желающим бесплатный доступ к своим вычислительным мощностям. Подключившись к системам облачного сервиса Leap 2, задействующим достижения квантовой физики, энтузиасты смогут заняться поиском мер по ликвидации последствий пандемии коронавируса COVID-19.

Речь идет не только о поиске препарата для лечения инфекции, пояснил TechCrunch Алан Барац. По его словам, мощности Leap 2 будут открыты всем научно-исследовательским командам, которые так или иначе работают над решением сложившейся ситуации – это также могут быть оптимизации управления логистикой или построения математических моделей распространения коронавируса.

Тем, кто пожелает участвовать в проекте, экспертизу предоставят партнеры D-Wave: Volkswagen, DENSO, Юлихский исследовательский центр, Sigma-i при Университете Тохоку, MDR, Menten AI, Мюнхенский университет Людвиг-Максимилиана и OTI Lumionics.

Бесплатно подключиться к Leap 2 можно будет из любой точки, где доступен сервис – США, Канады, Японии и 32 стран Европы. По словам Бараца, на энтузиастов не будет распространяться стандартное ограничение в одну минуту вычислений в месяц, и при этом они получают коммерческую лицензию, которая позволит не раскрывать исходный код разработок.

Впрочем, нет никаких гарантий, что при помощи Leap 2 будут найдены какие-либо приемлемые решения, признал Барац. «Но мы отлично знаем, что станет большим упущением не открыть этот инструмент», – добавил он.

Напомним, что главной особенностью квантовых компьютеров является способность находиться в двух состояниях одновременно. Если «обычные» ПК записывают биты информации последовательно, в состояниях ноль или единица, то квантовые компьютеры могут выполнять несколько вычислений параллельно, кодируя два значения сразу. За это отвечают квантовые биты (кубиты), которые могут одновременно находиться в нескольких состояниях.

Квантовые компьютеры можно применять, где угодно: для поиска лекарств и препаратов, построения наиболее эффективных логистических цепей и каналов поставок, поиска новых способов моделирования финансовых данных, защиты облачных вычислений с помощью законов квантовой физики.

Источник: vesti.ru, 31.03.2020

Алмаз станет основой квантового интернета: новая система управляет субатомными частицами

Ученые создали уникальную систему, которая способна улучшить квантовую связь на большие расстояния. Оказывается, алмаз может стать частью квантового интернета. Устройство, в которое он встроено, способно значительно улучшить квантовую проходимость и приблизить квантовый бум. Современные ученые буквально в одном шаге от создания доступных вычислительных и коммуникационных возможностей будущего. Это совершенно новый класс систем, использующих нетрадиционную математику, а она, в свою очередь, управляет субатомными частицами.

Главная цель, которую преследуют исследователи, заключается в создании сети, способной передавать квантовую информацию на большие расстояния, что, по мнению ученых, может привести к успехам в криптографии, распознавании или даже распределенных квантовых вычислениях. Но эксперты считают, что это не более, чем фантазия, потому что создать такую сеть невозможно без соответствующих компонентов.

Самый главный из них — квантовый повторитель, он увеличивает расстояние передачи, которое минует квантовая информация. Их же еще можно называть преобразователями, которые могут преобразовывать квантовую информацию в передаваемые фотоны. Михир Бхаскар, физик Гарвардского университета, заявил, что классические ретрансляционные станции измеряют этот сигнал и усиливают его копию.

И таким образом информация может быстро и доступно распространяться по всему миру. Все имеющиеся сети отправляют и получают информационные потоки в виде битов. Некоторые природные системы, такие как фотоны или электроны, хранят огромный набор информации в своих свойствах.

Эти системы имеют свойство запутывания, и повторные измерения становятся более коррелированными, чем могла бы позволить обычная вероятность. Физики уверены, что однажды будет создана сеть, которая использует все эти атрибуты.

Вся передаваемая информация кодируется как одиночные фотоны, но на расстоянии в несколько километров оптово-волоконного кабеля одиночные фотоны могут быть потеряны. Любая сеть, которая желает иметь узлы передачи дальше городских пределов, нуждается в повторителях, чтобы обеспечить передачу информации из точки А в отдаленную точку Б.

Ученым из Гарварда и Массачусетского технологического института удалось разработать центральный узел, и он эффективно сокращает половину маршрута. При этом вся система удерживается при нулевом градусе Кельвина. А основная часть этой системы состоит из алмаза, свойства которого работают путем замены двух атомов углерода одним атомом кремния.

В итоге таким образом создается область, которая одновременно хранит квантовое состояние и передает фотон. После достаточной синхронизации и запутывания фотонов центральный узел создает безопасный ключ, коррелированный между двумя сторонами. Затем этот ключ используется для шифрования и дешифрования сообщений между ними.

Источник: ekovolga.com, 27.03.2020

Ученые России повысили безопасность квантовой криптографии

Ученые консорциума Центра компетенций НТИ «Квантовые коммуникации» разработали способ повысить уровень защищенности квантовой криптографии.

Благодаря особому алгоритму проверки, выделяются и удаляются посторонние «шумы», которые могут повлиять на процесс работы генератора случайных чисел. Это на 100% исключает возможность внешнего воздействия на процесс шифрования. Статья о разработке опубликована в журнале *Optics Express*.

За каждым процессом отправки и получения информации в современном мире стоит криптография – система шифрования данных, обеспечивающая их безопасность. Наиболее часто встречается так называемое асимметричное шифрование, в котором используются не один секретный ключ, а два: открытый и закрытый. Закрытый (секретный) ключ хранится только у одного из участников криптографической системы, который хочет получить зашифрованное сообщение. Для этого он отправляет по обычному (незасекреченному) информационному каналу открытый ключ, который используется для того, чтобы зашифровать сообщение. Чтобы расшифровать сообщение недостаточно иметь только открытый ключ – нужно знать еще и закрытый ключ.

Эта ситуация аналогична тому, как если бы человек, желая получить секретное послание, раздавал всем желающим небольшие замки, но не давал бы никому ключи к этим замкам. Каждый, кто захотел бы поделиться с ним своим секретом, мог бы положить секретное послание в шкатулку и запереть ее этим замком. Очевидно, что теперь никто, кроме него, не сможет открыть шкатулку и прочитать секретное сообщение, даже если шкатулка попадет в руки злоумышленника.

Система асимметричного шифрования, опирается на недоказанное математическое утверждение о невозможности за полиномиальное время разложить целое число на простые сомножители. Поэтому считается, что мощности современного компьютера не хватит для взлома такой системы, однако такие возможности могут в ближайшем будущем появиться у квантового компьютера. Это ставит под сомнение безопасность классических методов криптографии в приближающуюся эпоху квантового превосходства.

В противовес возможным технологиям квантового взлома учеными активно разрабатываются и внедряются методы квантовой криптографии – шифрования, основанного не на компьютерных алгоритмах, а на законах квантовой механики. Системы квантовой криптографии решают задачу безопасного распределения секретного ключа между участниками криптографической системы. Секретный ключ передается по оптическому каналу с помощью одиночных фотонов. Согласно законам квантовой механики, злоумышленник не сможет незаметно перехватить отдельные фотоны, так что при любой его попытке узнать секретный ключ, система будет сигнализировать об опасности.

Ученые консорциума Центра компетенций НТИ «Квантовые коммуникации» (НИТУ «МИСиС», компания QRate и Российский квантовый центр) разработали способ повысить уровень защищенности систем квантовой криптографии при помощи особого алгоритма, позволяющего обнаруживать атаки именно на квантовый генератор случайных чисел.

Для генерации случайных битовых последовательностей ученые предложили использовать шумы, возникающие в полупроводниковом лазере и связанные со спонтанным излучением. Поскольку спонтанное излучение обусловлено так называемыми нулевыми колебаниями электромагнитного поля, то можно утверждать, что такие шумы в лазере имеют чисто квантовую природу, а поэтому их принципиально невозможно научиться предсказывать и, что самое главное, они оказываются невосприимчивы к любым попыткам «подчинить» их внешнему контролю.

Ученые из компании QRate и НИТУ «МИСиС» разработали протокол, который позволяет «на лету» оценивать вклад классических шумов и определять таким образом уровень потенциальной угрозы. Более того,

предложенный ими протокол позволяет преобразовывать выходную случайную битовую последовательность в «истинно квантовую» без использования сложных алгоритмов постобработки, таких как хеширование, которые обычно применяются для этих целей.

По словам разработчиков, их алгоритм уже сейчас можно применять в существующих и проектируемых квантовых генераторах случайных чисел для установок квантовой криптографии.

Источник: rusplt.ru, 06.04.2020

РКЦ: квантовый компьютер и блокчейн. Наука России и ее ученые (интервью с Алексеем Федоровым – создателем квантового блокчейна и руководителем одной из научных групп)

– *Квантовый генератор случайных чисел, квантовый блокчейн – это все здорово, отлично. А квантовый компьютер-то где?*

– На самом деле, квантовый компьютер уже существует на сегодняшний день, есть прототипы в мире, в России. Но они пока не могут решать индустриальные, коммерчески востребованные задачи. Они относятся к так называемой «эре NISQ (Noisy Intermediate-Scale Quantum)». То есть они шумные и промежуточного масштаба, но уже квантовые.

– *Промежуточного масштаба – это как?*

– Мощность квантового компьютера меряется количеством кубитов. Кубит – это квантовый аналог бита, это суперпозиция 0 и 1. Считается, что маленький квантовый компьютер – это 0-5 кубитов. В России есть двухкубитный квантовый компьютер, сейчас работают над пятикубитными. А в мире – это десятки кубитов. Intermediate-Scale – это где-то от 30 до 100.

Самый мощный на сегодняшний день создан компанией Google, в нем 53 кубита, и он может решать некоторую очень специфическую задачу моделирования случайных квантовых цепочек. Пока это единственное, что он может делать нормально, но он решает эту задачу намного быстрее, чем классический суперкомпьютер.

– *Это необходимо для каких-то научных разработок?*

– Это называется «демонстрация квантового превосходства». Квантовое превосходство – это способность квантового компьютера решать задачи, которые неспособен за разумное время решить классический суперкомпьютер. Вот Google в октябре прошлого года нашел специфическую задачу. Хотя она и имеет сомнительное практическое применение, тем не менее, квантовый

компьютер решает её за 200 секунд, а классическому по их оценкам потребовалось бы 10 тысяч лет.

– *Правильно ли я понимаю, что те научные результаты, которые вы получили, лягут в основу создания отечественного квантового компьютера?*

– На самом деле, наша цель достаточно амбициозна – сильно сократить отставание между тем, что происходит сейчас в России и в мире. Россия отстает в создании квантовых вычислений на 5-10 лет. Наша цель – сократить это отставание до 2-3 лет.

Этим в последнее время занимался «Росатом» вместе с экспертным советом при участии нашего центра. Была разработана супер-детализированная дорожная карта развития каждого квантового процессора в отдельности. На данный момент идея состоит в том, что будут поддерживаться 4 базовых технологии создания квантовых процессоров: на сверхпроводниках, ионах, интегральной оптике и на ультрахолодных атомах. При чем помимо хардварной части будет также программная. Я принимаю участие в разработке программного обеспечения для будущих квантовых компьютеров.

– *Что это ПО будет делать?*

– Будет решать индустриальные задачи. Из области квантовой химии или материаловедения, или биоинформатики – моделирование таких систем, как лекарства, например. Вопрос пока тонкий – насколько это будет эффективнее того, что есть сейчас. Возможно, в чем-то более эффективно, но вряд ли за 5 лет удастся достичь прямо индустриального превосходства. Тем не менее, такой фокус есть.

– *А пока в России есть только двухкубитный квантовый компьютер.*

– Да, но двухкубитный – это уже очень важно. Потому что любые алгоритмы, которые есть в квантовом компьютере, раскладываются на однокубитные и двухкубитные операции. То есть один кубит и два кубита – это базовые элементы для того, чтобы потом эту технологию масштабировать.

– *Это все очень круто звучит, но, согласись, чтобы человек думал о науке, вот так вот был в неё погружен, действительно был нацелен на результат, он не просто должен её любить... он еще не должен думать о деньгах, хотя бы о своих базовых потребностях.*

– Да, конечно. РКЦ обеспечивает достойный уровень жизни.

– *Сколько зарабатывают ваши сотрудники?*

– Я знаю только в среднем вилки. Для студентов – это от 30 до 50-60 тысяч, аспирант получает 80-120, и так далее. Но это очень индивидуально, все сильно зависит от человека, его уровня, потребностей и желания вовлекаться. Хорошая сторона квантового центра – это его гибкость.

Действительно выдающемуся сотруднику могут быть обеспечены супер-привлекательные условия для того, чтобы он либо не уехал, а лучше – уехал, поработал там и вернулся.

Но есть и другая сторона. У квантового центра в отличие от института академии наук нет базы финансирования. Он не является строчкой бюджета Российской Федерации. На каждый год это финансирование надо искать и оправдывать. Поэтому иногда помимо получения денег от спонсора мы участвуем в грантах и различных крупных проектах.

– Согласись, что человек не может заниматься наукой, если ему приходится выживать, как сейчас происходит во многих научных институтах.

– Безусловно. Но, тем не менее, у нас в стране есть возможность работать. Можно получить грант Российского научного фонда, который по своему объему сопоставим с европейскими, и это замечательно. Ты можешь получить грант, сформировать научную группу, показать, что ты конкурентоспособен в своем научном направлении и работать. И практически все молодые научные сотрудники квантового центра сильно нацелены на то, чтобы создать свой коллектив какой-то маленький, даже в рамках большой научной группы. Они работают над грантами и привлекают их.

– На чем и как ты пишешь программы для квантовых компьютеров?

– Пока железная часть в разработке, мы пишем программы для эмулятора квантового компьютера, который работает на обычном компьютере, но полностью воспроизводит поведение квантового, вплоть до шумов. Это очень интересная деятельность – писать ПО для компьютера, которого еще не существует. Сама постановка задачи мне настолько понравилась, что я понял, что не хочу ничем другим заниматься.

– А на чем, на чем?

– У нас очень много инструментов. Есть профессиональные, квантовые языки программирования типа Q#.

– Подожди, квантовые языки программирования? Где-то можно такому научиться?

– Конечно, можешь прямо сейчас. Помимо Q# есть такая вещь, которая называется Qiskit – это визуальный язык программирования от компании IBM. Ты можешь зайти на их сайт IBM Quantum Experience и запрограммировать квантовый компьютер, который у них располагается в общем доступе. В России тоже будет нечто подобное.

– То есть вам нужны особые программисты для квантовых компьютеров?

– А таких еще нет, поэтому мы их сами делаем. Они приходят как классические программисты, но постепенно меняют свой подход. В какой-то момент такие: «О, о' кей, нужно программировать еще и такую штуку» и начинают программировать квантовый компьютер, разбираться в железе и так далее.

– Я читала, что вы хотите использовать квантовый компьютер для машинного обучения.

– В процессе исследования мы поняли, что машинное обучение – это одно из потенциальных приложений квантового компьютера, где он может показать свою полезность, пока он еще не стал супермощным и суперидеальным. Например, мы поняли, как делать новый класс оптимизационных алгоритмов, которые называются квантововдохновенными. Они являются квантовыми, но при этом моделируют поведение некоторой физической системы. И могут быть более эффективными, чем классические.

И, в частности, такие, квантововдохновенные алгоритмы можно применять в разных задачах машинного обучения. Например, мы нашли, как обнаруживать хаос в многочастичных системах, это давняя задача и одна из краеугольных задач физики вообще.

Источник: vc.ru, 15.04.2020

Ученые создали квантовые точки, расстреляв графен потоком ионов

Ученые Института физики полупроводников им. А. В. Ржанова СО РАН, Института биохимической физики им. Н. М. Эмануэля РАН, Объединенного института ядерных исследований вместе с коллегами из других научных организаций России, Польши и Франции сформировали графеновые островки (квантовые точки) сверхмалого размера – единицы нанометров, – заключенные в непроводящую матрицу. Исследователи добились этого с помощью «бомбардировки» тонких пленок фторированного графена ионами ксенона. Такое наноструктурирование фторграфена было сделано впервые. Полученные структуры могут стать активными элементами наноэлектронных приборов, функционирующих при комнатной температуре.

Квантовая точка – ее иногда называют искусственным атомом – частица полупроводника, в которой электроны находятся в потенциальной яме, то есть «заперты» и не могут свободно двигаться по всему кристаллу. Применение квантовых точек варьируется от использования в качестве флуоресцирующих меток в медицинских и биологических работах до создания одноэлектронных транзисторов и логических элементов квантового компьютера.

Нанoeлектронные (квантовые) устройства чувствительны к влиянию внешних условий и для корректной работы часто требуют охлаждения до температур близких к абсолютному нулю. Однако характеристики графена позволяют создавать нанoeлектронные приборы, действующие в привычных нам условиях.

«Обычно, чтобы получить в графене квантовые точки, его «нарезают» на маленькие фрагменты, но, тогда края последних взаимодействуют с воздухом, окисляются. Это приводит к нестабильности свойств материалов на основе таких квантовых точек: в частности, к уменьшению электропроводности или подвижности носителей заряда. Возникает противоречие: нужны миниатюрные квантовые точки, но у них будет много краевых состояний, которые изменяют (ухудшат) их параметры. В нашей работе мы формировали графеновые квантовые точки внутри матрицы фторографена (FG, диэлектрика на основе графена). Для этого мы облучали пленки фторографена быстрыми ионами ксенона. Создаваемые в результате облучения нанoостровки графена оказываются встроенными во фторированную матрицу, у них нет оборванных связей и нет проблем с появлением краевых состояний», – объясняет научный сотрудник Института физики полупроводников им. А. В. Ржанова СО РАН кандидат физико-математических наук Надежда Александровна Небогатикова.

Облучение высокоэнергетичными ионами ксенона с энергиями от 26 до 167 МэВ происходило в лаборатории ядерных реакций им. Г.Н. Флерова ОИЯИ. Благодаря кратковременному и мощному выделению тепла во время пролета иона, материал фторграфеновой матрицы локально расширился и восстанавливался до графена вблизи треков (траекторий) ионов. Исследовательская группа предложила модель того, как происходил этот процесс.

«По-видимому, облучение разрушает отдельные частицы фторированного графена, из которого состоят пленки, приводя к формированию небольших (20-40 нанометров в диаметре) гранул с квантовыми точками. Интересно, что затем гранулы «слипаются» в более крупные сферические образования. Мы не ожидали увидеть подобный процесс, но пронаблюдали его в эксперименте и подтвердили при помощи моделирования», – комментирует Надежда Небогатикова.

Одно из направлений развития подхода, предложенного в работе, – разработка материалов с заранее заданными электрическими параметрами за счет управления расстояниями между квантовыми точками и формирование из них определенного рисунка. По сути подобные материалы – основа для создания гибких электронных устройств или карт памяти.

«Наноструктурирование пленок фторированного графена значительно расширяет возможные приложения последнего. Например, мы создали

двуслойные структуры, состоящие из фторграфена, нанесенного на гибкую подложку из поливинилового спирта. Степень фторирования графена до облучения была такой, что он практически не проводил электрический ток. Однако после облучения и наноструктурирования за счет формирования электрически активных квантовых точек, мы увидели улучшение параметров резистивных переключений для наших структур на несколько порядков», – отмечает ведущий научный сотрудник ИФП СО РАН доктор физико-математических наук Ирина Вениаминовна Антонова.

Эффект резистивных переключений используется при разработке энергонезависимой памяти на основе мемристоров. Ее характеристики: время хранения, скорость и плотность записи информации существенно превышают аналогичные параметры у традиционно используемых видов памяти.

Источник: portech.ru, 21.04.2020