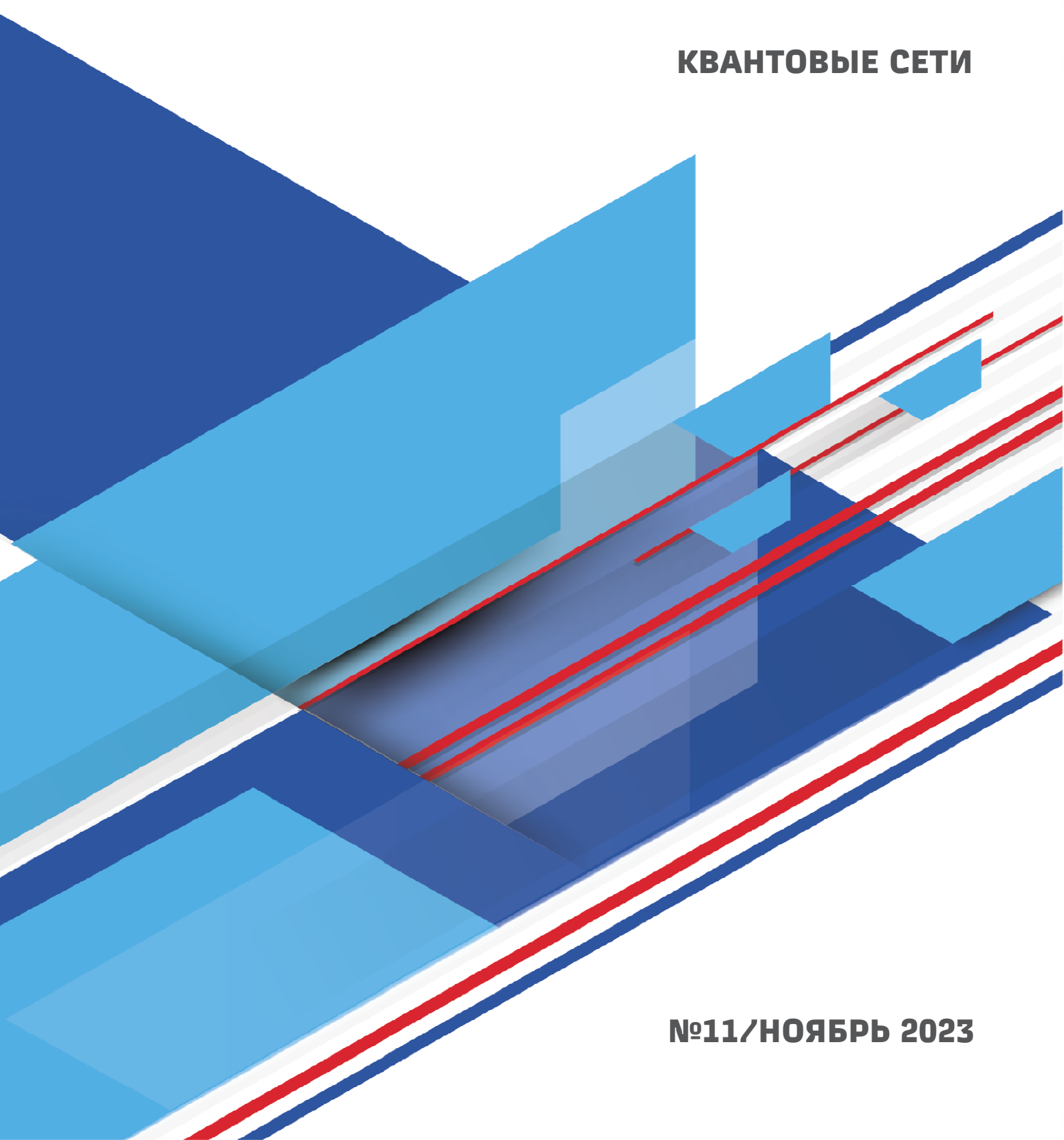
МОНИТОРИНГ

ЦНТИБ ОАО «РЖД»

КВАНТОВЫЕ СЕТИ



№11/НОЯБРЬ 2023

СОДЕРЖАНИЕ

В космос запущен «невозможный» квантовый привод, не подчиняющийся известным законам физики

Новая спорная электрическая двигательная установка, которая, по мнению физиков, противоречит законам движения Ньютона, была запущена в космос на борту ракеты SpaceX.

Квантовый привод, разработанный компанией IVO Ltd., занимающейся разработкой прототипов электроники, отправился в полет утром 11 ноября 2023 года на ракете-носителе SpaceX Transporter 9. Этот полет включал в себя более 80 отдельных полезных нагрузок, предназначенных для вывода на низкую околоземную орбиту (НОО).

«Запуск и выведение прошли успешно!» сообщил владелец и основатель компании IVO Ричард Мэнселл. «Мы слышим «сердцебиение» спутника. Следующий шаг – установление связи с ним».

Мэнселл также сообщил, что после установления связи со спутником «Barry-1» компании Rogue Space Systems, на котором установлена пара квантовых приводов, начнет проходить несколько этапов, прежде чем квантовые приводы будут подвергнуты окончательному испытанию. Это включает в себя сбор данных на низкой околоземной орбите в течение нескольких недель, чтобы установить базовую линию для включения приводов.

«Rogue Space Systems и IVO тесно сотрудничают друг с другом, чтобы собрать надежную базу орбитальных данных перед первым включением приводов», – сказал Мэнселл. «Это поможет подтвердить результаты тяги квантовых приводов».

13 ноября компания Rogue Space Systems официально заявила, что связь со спутником Barry-1 установлена.

«Rogue Space Systems установила положительный контакт со спутником!» сообщил Мэнселл. «Мы благодарны за то, что они позволили нам стать полезной нагрузкой на их первом спутнике, нам было приятно работать с ними».

Изобретение квантового привода

Мэнселл до запуска на орбиту его квантового привода, рассказывал о том, какие споры вызывает технология, на которой основаны его двигатель, и что именно побудило его заняться созданием того, что, по мнению почти всех ученых, не должно работать:

«Мы начали играть с идеей «что такое гравитация» и «что такое инерция». Затем я наткнулся на работу профессора Майка Маккаллоха из Плимутского университета».

На своем сайте Маккаллох отмечает, что первый закон Ньютона определяет инерцию следующим образом: «Объекты движутся по прямым линиям с постоянной скоростью, если их не толкать». Далее Маккалох отмечает, что, хотя Ньютон определяет инерцию в таких простых терминах, гений XVII века так и не объяснил, что именно представляет собой инерция.

Чтобы объяснить истинную природу инерции, Маккаллох разработал теорию квантованной инерции (КИ), обращающуюся за ответом к странным и загадочным свойствам квантового мира. Неудивительно, что попытки объяснить инерцию вызвали широкомасштабную критику, поскольку его предложение, как представляется, противоречит законам движения, впервые установленным много веков назад, законам, которые оказались весьма надежными для ракетчиков и инженеров.

Тем не менее, по словам Мэнселла, работа Маккаллоха его заинтриговала. В отличие от других, кто считал, что профессор Плимутского университета всё придумал, он обладал уникальными возможностями действовать в этом направлении.

Квантовый привод компании IVO

Получив патент на конденсатор, используемый для беспроводной передачи энергии – основного рынка для коммерческой деятельности компании IVO, включающей систему беспроводной передачи CBAT, которая в настоящее время проходит строгие испытания на безопасность и сертификацию, Мэнселл понял, что его оборудование вполне подходит для создания первых прототипов приводов, построенных с использованием теорий Маккаллоха:

«Что, если мы начнем с того, что попробуем повторить работу других людей и посмотрим, есть ли в ней какие-то плюсы?»

Вскоре Мэнселл и его команда уже работали в штаб-квартире в Северной Дакоте и на предприятии в Вирджинии, которое он назвал «IVO East», тестируя и совершенствуя способы использования возможностей квантовой инерции. За этой работой последовало более 100 часов испытаний прототипа в имитируемой космической среде, в результате которых была создана модель, создающая тягу. Недавно команда также успешно завершила 1000-часовой «стресс-тест», который «Квантовый привод» прошел с блеском.

Таким образом, хотя наука говорит, что это не должно работать, в лабораторных испытаниях привод IVO, похоже, создал предсказанную тягу. На этом этапе, по словам Мэнселла, они поняли, что осталось сделать только одно:

«Привод просто нужно отправить в космос. Это действительно нужно сделать».

Мэнселл отметил важность успешного полета «Квантового привода» в космос, что делает его первым в своем классе, перешедшим от лабораторных экспериментов к реальным орбитальным испытаниям.

«Я не знаю других чисто электрических приводов, которые когда-либо испытывались в космосе», – сказал Мэнселл. Включая спорный EMDrive, который, как он отметил, основан на совершенно другой технологии, но также претендует на создание тяги без топлива. «Если это так, то это будет первый случай испытания чисто электрического, «нетрадиционного» привода в космосе!»

Мэнселл также считает, что, что бы ни случилось, его команда показала своим клиентам и коллегам, что они могут в рекордно короткие сроки перевести потенциально революционные идеи из разряда концепций в разряд продуктов.

«Независимо от того, создадут ли «Квантовые приводы» ожидаемую тягу или нет, IVO еще раз продемонстрирует, что мы способны не только проводить сложные эксперименты, но и делать это эффективно и в рекордно короткие сроки», – сказал Мэнселл.

Как наука и техника могут совершить большой скачок вперед

После успешного запуска, до начала испытаний осталось всего несколько недель. После этого, когда приводы будут включены, они либо успешно изменят орбиту спутника Barry-1, переписав учебники физики, либо потерпят неудачу, и сэр Исаак Ньютон сможет спать спокойно.

«Наша цель – поднять орбиту», – говорит Мэнселл. «Мы хотели бы провести несколько демонстраций. Мы собираемся сделать несколько орбит без тяги, чтобы получить базовый набор данных и понять, что такое фоновый шум. Затем мы включим двигатели, квантовые приводы, и поднимем орбиту. Затем цель состоит в том, чтобы опустить орбиту и иметь возможность делать это предсказуемо, туда и обратно, и посмотреть, сможем ли мы изменить наклон орбиты. Это было бы фантастично».

В любом случае, по словам Мэнселла, он гордится тем, что его команде удалось провести реальные испытания своего спорного привода. Он также отмечает, что в этом деле наступает момент, когда теория заканчивается, и на смену ей приходят практические испытания:

«Мы не боимся пробовать сложные эксперименты, потому что именно так наука и техника могут сделать большой скачок вперед. Важно опираться не на догадки и гипотезы, а на реальные, достоверные данные. Именно поэтому мы отправили в космос квантовые накопители».

Источник: etm-club.site, 19.11.2023

ORCA Computing предоставит Польше две квантовые вычислительные системы

Британский разработчик квантовых систем ORCA Computing выбран Познаньским центром суперкомпьютерных и сетевых технологий (PSNC) в Польше в качестве поставщика двух квантовых компьютеров. Эти системы призваны ускорить решение задач в ряде научных и прикладных областей, включая биологию, химию и машинное обучение.

Речь идёт о квантовых фотонных компьютерах ORCA Computing PT-1. Они будут установлены в центре высокопроизводительных вычислений PSNC в Познане в ноябре и декабре нынешнего года и интегрированы в существующую HPC-инфраструктуру. Ситсемы закуплены в рамках проекта EuroHPC-PL.

Квантовые компьютеры PT-1 используют источник одиночных фотонов и программируемые сети светоделителей для реализации квантовой памяти. Результаты вычислений представляют собой сложную статистику, где количество фотонов отражает вероятность распределения. Система может быть интегрирована с классическими HPC-платформами. Доступен специализированный комплект для разработки, который поддерживает гибридные квантово-классические алгоритмы с QPU и GPU.

Технология ORCA Computing предусматривает использование одиночных фотонов в качестве носителя. Это не только позволяет системе естественным образом взаимодействовать с оптическими сетями, но также обеспечивает модульность и гибкость архитектуры с возможностью последующего обновления. Задействована проприетарная технология мультиплексирования для управления синхронизацией, частотой и маршрутизацией одиночных фотонов: данная методика позволяет достигать высокой плотности данных, что даёт возможность осуществлять полномасштабные квантовые вычисления с гораздо меньшим количеством компонентов.

Источник: servernews.ru, 12.11.2023

Квантовый телескоп способный закрыть инопланетный вопрос

В 2021 году, появилась любопытная новость о том что группа австралийских астрономов из Сиднейского университета предложила идею создания гигантского интерферометра из оптических телескопов, разбросанных по Земле, наподобие виртуальной антенны телескопа EHT, или SKA. Такой оптический интерферометр со сверхдлинной базой, был бы основан на технологии квантового жесткого диска, который не записывал бы, а сохранял квантовую информацию о полученных фотонах, дабы оптом объединить ее

в одну картинку. Таким образом, теоретически можно было бы получить телескоп с настолько мощной разрешающей способностью, что это было бы сравнимо с телескопом диаметром с Землю. Такой телескоп в принципе, мог бы получать прямые снимки экзопланет, сравнимых по размеру с Землей, закрыв инопланетный вопрос.

К сожалению, все упирается в то, что все реально созданные прототипы квантовых накопителей, сложны, дорогостоящи, а главное, недолговечны. Идея, тем не менее, была весьма интересная, а потому мне было весьма приятно узнать, что оказывается, тема квантового телескопа получила продолжение.

Для астрономов одной из самых больших проблем является получение изображений объектов и явлений, которые трудно увидеть с помощью оптических телескопов (или в видимом свете). Эта проблема была в значительной степени решена с помощью интерферометрии, метода, при котором несколько телескопов собирают свет, объединяющийся затем для создания более полной картины. Примерами могут служить телескоп Event Horizon, который использует обсерватории со всего мира для получения первых изображений сверхмассивной черной дыры (SMBH) в центре галактики M87 и Стрельца A* в центре Млечного Пути.

При этом классическая интерферометрия требует поддержания оптической связи между обсерваториями, что накладывает ограничения и может привести к резкому увеличению затрат. В недавнем исследовании команда астрофизиков и физиков-теоретиков предложила, как эти ограничения можно преодолеть, полагаясь на квантовую механику. Вместо того чтобы полагаться на оптические каналы связи, они предлагают способ, при котором принцип квантовых запутанностей можно было бы использовать для обмена фотонами между обсерваториями. Этот метод является частью растущей области исследований, которая когда-нибудь может привести к созданию «квантовых телескопов».

Исследование было проведено исследователями из Брукхейвенской национальной лаборатории (BNL) и Университета Стоуни Брук в Нью-Йорке, штат Нью-Йорк. Дополнительную поддержку оказал Стивен Винцкевич, физик-теоретик и независимый исследователь, в настоящее время базирующийся в Объединенных Арабских Эмиратах. Статья, описывающая их выводы, недавно появилась в Интернете и проходит рецензирование для публикации в научном журнале Optica.

В классической интерферометрии Майкельсона пучок света разделяется таким образом, что один луч попадает на неподвижное зеркало, а другой – на подвижное зеркало. Интерференционная картина создается, когда отраженные лучи снова объединяются. Для целей астрономии два луча собираются двумя телескопами, которые разделены некоторым расстоянием (называемым базовой

интерферометрией). Но, несмотря на свою эффективность, классическая интерферометрия подвержена некоторым ограничениям.

Андрей Номероцкий, астрофизик из BNL и соавтор статьи, объяснил Universe Today по электронной почте: «Интерферометрия – это способ увеличить эффективную апертуру телескопов и улучшить угловое разрешение или астрометрическую точность. Главная трудность здесь заключается в поддержании стабильности этого оптического тракта с очень высокой точностью, которая должна быть намного меньше длины волны фотона, чтобы сохранить фазу фотона. Это ограничивает практические исходные линии несколькими сотнями метров».

В последние годы ученые исследовали возможность использования квантовых принципов для создания астрономии следующего поколения. Основная идея заключается в том, что фотоны могут передаваться между обсерваториями без физических соединений, которые являются дорогостоящими в строительстве и обслуживании. Ключ в том, чтобы воспользоваться преимуществами квантовой запутанности – явления, при котором частицы взаимодействуют и находятся в одном и том же квантовом состоянии, несмотря на то, что их разделяет значительное расстояние. Квантовые телескопы были первоначально предложены исследователями Дэниелом Готтесманом, Томасом Дженневейном и Сарой Кроук из Института теоретической физики Периметра и Института квантовых вычислений при Университете Ватерлоо.

«Предложение состояло в том, чтобы использовать источник запутанных фотонов и использовать корреляции количества фотонов на двух станциях и, следовательно, в основном устранить проблему стабильности фазы фотонов. Интерферометры интенсивности используются для измерения диаметров звезд с использованием метода, основанного на эффекте сгущения фотонов Хэнбери Брауна-Твисса. В нашей схеме мы используем тот же эффект, только его фазозависимую часть, для измерения угла раскрытия между двумя звездами, которые теперь могут быть разделены значительным углом. С другой стороны, сказал Номероцкий, вторую звезду также можно рассматривать как источник когерентных фотонов для первой звезды, отсюда и ссылка на предложение Готтесмана-Дженневейна-Кроука».

По словам Номеротски, в настоящее время команда разрабатывает физическое описание, включающее оба варианта. Это можно было бы обобщить на несколько станций и квантовые протоколы для обработки квантовой информации в «зашумленной» среде. Чтобы проверить свою концепцию, команда создала настольную версию двухфотонного интерферометра, который использовал узкую спектральную линию в двух аргоновых лампах (для имитации двух звезд). Как они и предсказывали,

основываясь на предыдущих теоретических исследованиях, команда отметила пики эффекта группировки фотонов Хэнбери-Брауна-Твисса и корреляции каналов и измерила его зависимость от фазы фотона.

Главным преимуществом этого метода является улучшенное угловое разрешение (способность различать детали в объектах) в телескопах. Но, как объяснил Номероцкий, долгосрочные выгоды могут быть неизмеримыми: «Может возникнуть множество научных возможностей, которые выиграют от существенного повышения астрометрической точности. Просто перечислим некоторые из них: проверка теорий гравитации путем прямого отображения аккреционных дисков черных дыр, точного параллакса и лестницы космических расстояний, картирование событий микролинзирования, экзопланет, специфических движений, темной материи и других.

Конечно, все это довольно долгосрочно и потребует демонстраций подтверждения принципа и, что важно, повышения чувствительности по сравнению с тем, что достижимо сейчас. Эти улучшения основаны на прогрессе в разработке квантовых сетей и квантовых ретрансляторов, как в первоначальном предложении GJC. В настоящее время многие из этих разработок осуществляются компаниями для совершенно других целей, и уже достигнут значительный прогресс, так что это может стать реальностью в обозримом будущем».

Это предложение по двухфотонной интерферометрии является одним из многих предложений по квантовым телескопам за последние годы. Другие примеры включают предложение команды Массачусетского технологического института объединить интерферометрию с квантовой телепортацией, чтобы резко увеличить разрешение обсерваторий (без использования зеркал большего размера). Существует также более свежая идея объединения стимулированного рамановского адиабатического прохождения и предварительно распределенной запутанности для создания виртуального телескопа интерферометрии с очень длинной базовой линией размером с планету Земля.

Эти квантовые методы могли бы позволить проводить наблюдения на ранее недоступных длинах волн и более детально изучать черные дыры, экзопланеты, Солнечную систему и поверхности далеких звезд. И по мере продолжения усилий по совершенствованию технологии, лежащей в основе квантовых вычислений, приложения, несомненно, будут распространяться на другие области исследований (например, квантовую астрономию).

Источник: blackpill.usite.pro, 11.11.2023

Японские квантовые компьютеры научат работать

Японцы до сего дня не в состоянии овладеть квантовыми компьютерами. Поэтому специалисты «RIKEN» – Центра квантовых вычислений, решили применить метод машинного обучения, посредством которого попытаться создать механизм исправления ошибок. Квантовые компьютеры, как выясняется, попросту не будут работать без автономной системы коррекции. Но на текущий момент такая система даёт лишь приблизительные поправки.

Уже давно набили оскомину утверждения о том, что классика жанра операций битами – это работа с базовыми величинами «0» и «1». В свою очередь квантовые компьютеры делают работу «кубитами» через суперпозицию состояний вычислительного алгоритма.

Соответственно, техника такого рода способна выполнять принципиально новые вычислительные операции, что сопровождается явными преимуществами. Особенно важными видятся такие свойства для операций:

– трудоёмкого поиска;

– оптимизации сложных процессов;

– чтения алгоритмов криптографии.

Однако природа квантовых суперпозиций, по словам японских специалистов, это очень хрупкий мир. Даже незначительные изменения окружающей среды способны приводить к ошибкам, способствующим разрушению такого типа суперпозиций. Результат очевиден – все японские квантовые компьютеры рискуют превратиться в кусок железа.

Эти риски заставляют японцев прибегнуть к разработке сложных методов коррекции ошибок суперкомпьютеров. Теоретически эти методы обещают действенно исключать влияние ошибок на процессы. Но практически эти же методы несут массу издержек в виде сложности устройств. А высокая степень сложности – это неизбежность дополнительных ошибок. Вывод тут очевиден: полноценная коррекция ошибок недостижима.

И всё же японскими специалистами решено обратиться к машинному обучению в самом, так сказать, передовом варианте. Здесь агентом исследуется своего рода абстрактная среда с целью понять и оптимизировать политику действий. Как выяснилось, достаточно простое кодирование кубита приводит к значительному снижению сложности устройства. Более того, здесь возрастают способности исправления ошибок.

Так что, проделанная японцами работа демонстрирует серьёзный потенциал машинного обучения в деле коррекции ошибок суперкомпьютеров. Кроме того, по словам японских учёных-физиков, этот подход приближает на шаг к реализации качественной системы коррекции ошибок, пусть даже пока что только в экспериментах. Машинное обучение, как утверждается,

непременно сыграет ключевую роль в деле исполнения крупномасштабных задач более продвинутых вычислений и оптимизации.

Источник: zetsila.ru, 10.11.2023

Китайские исследователи представили уникальное квантовое решение для защиты данных

Китайская компания QuantumCTek Co, специализирующаяся на квантовых информационных технологиях, предложила новаторский подход к обеспечению кибербезопасности данных в облаке. Исследователи использовали квантовые случайные числа в качестве ключей шифрования, что повышает уровень защиты данных от квантовых компьютеров.

Основой метода служит алгоритм распределения ключей Шамира, позволяющий разделять частную информацию между определённой группой лиц. Эта информация остаётся в секрете до тех пор, пока большинство участников группы не объединят свои знания.

Для повышения эффективности и снижения затрат исследователи применили дополнительный этап кодирования стирания внутри шифротекста перед передачей данных с помощью алгоритмов квантового распределения ключей (QKD). Это позволило обеспечить не только квантовую безопасность, но и повысить устойчивость к сбоям.

Вице-президент QuantumCTek Co., Юн Чжао, заявил, что их решение обеспечивает квантовую безопасность и является практичным применением синтеза квантовых технологий и криптографии. «Ключи, сгенерированные с помощью QKD, обеспечивают безопасность как загрузки пользовательских данных на серверы, так и передачи данных на распределенные узлы облачного хранения», – добавил он.

Исследователи также проверили, может ли их подход быть использован не только для передачи данных, но и для их хранения. Они провели ряд тестов, включая шифрование/дешифрование, сохранение ключевой информации и хранение данных, и подтвердили его эффективность.

Это решение является жизнеспособным как с технологической, так и с инженерной точки зрения, соответствует стандартам квантовой криптографии и способно противостоять вызовам, представленным квантовыми вычислениями. С учётом возможностей квантовых компьютеров решать задачи на порядки быстрее современных компьютеров, разработка кибербезопасности нового поколения является более, чем актуальной.

Источник: securitylab.ru, 15.11.2023

Nature: в трехмерном кристалле обнаружены плоские зоны проводимости

Американские физики сделали важное открытие в области квантовой физики и новых материалов, создав кристалл из сплава кальция и никеля с особенной структурой решетки, похожей на японский орнамент кагоме (рис. 1).

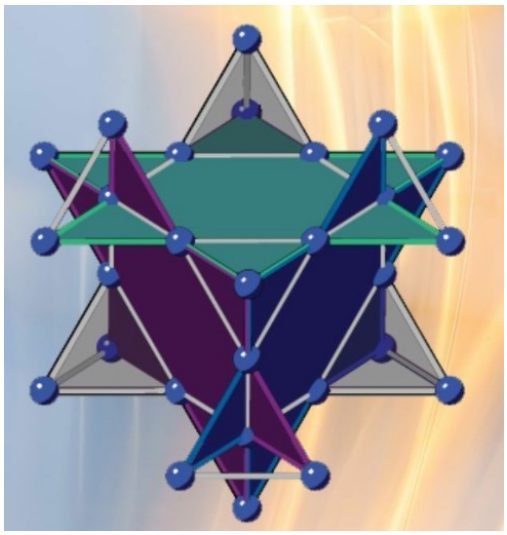


Рис. 1. Японский орнамент кагоме

Исследование, опубликованное в Nature, показало, что в этом кристалле существуют трехмерные плоские зоны проводимости, где электроны имеют низкую кинетическую энергию и не могут выйти из трех измерений. Это явление может породить разнообразные квантовые фазы вещества и расширить наше понимание квантовых явлений.

Источник: nnovpost.ru, 17.11.2023

Huawei создала «квантовый» смартфон

Квантовый смартфон создали совместно с китайской компанией China Telecom Quantum Group. За основу взяли ранее анонсированный Mate 60 Pro, пишет Sparrows News.

Телефон оснастили квантовыми информационными технологиями с сетями передачи голоса по LTE (VoLTE). В устройстве используется технология «тройной защиты», включающая чип отечественного производства, секретные алгоритмы и SIM-карту квантовой безопасности. По данным источника, этот тройной комплекс мер безопасности обеспечивает комплексную защиту от потенциальных угроз.

Одна из выдающихся особенностей квантового устройства – способность совершать телефонные звонки с квантовым шифрованием непосредственно

через встроенную панель набора номера. Передача зашифрованных файлов и сообщений доступна в предварительно установленном приложении Quantum Secure Messaging.

В устройстве используется технология тройной защиты.

Шифрование и дешифрование голосовых данных VoLTE осуществляется локально на мобильном телефоне с использованием чипа отечественного производства и промежуточного программного обеспечения квантовой безопасности собственной разработки Huawei. Этот инновационный подход эффективно предотвращает потенциальные попытки подслушивания при передаче данных по сети.

Напомним, обычную версию Huawei Mate 60 Pro представили в конце августа.

Характеристики Huawei Mate 60 Pro:

– Экран: 6,82 дюйма, LTPO, Full HD+, адаптивные 120 Гц, шим 1440 Гц, стекло Kunlun glass;

– Процессор: Kirin 9000s;

– Память: 12 ГБ ОПГ, до 1 ТБ ПЗУ;

– Камеры: основная 50 Мп, телевизор 48 Мп, широкоугольная 12 Мп, передняя 13 Мп;

– ОС: HarmonyOS 4.0.

Источник: china-review.com.ua, 14.11.2023

Новые достижения в квантовой физике: возможности и принципы квантовой телепортации.

Квантовая телепортация – впечатляющее явление, которое позволяет передавать информацию, состояния и даже частицы на огромное расстояние мгновенно. Этот удивительный процесс основан на принципах квантовой механики и открывает перед научным сообществом большие возможности для развития передачи информации.

Одной из ключевых особенностей квантовой телепортации является то, что при ее использовании передаваемые данные никогда не переносятся через промежуточное пространство. Вместо этого, состояние одной частицы кодируется и передается на другую частицу, находящуюся на большом расстоянии. При этом, состояние первой частицы, оказавшись взаимно согласованным с состоянием второй частицы, как бы «телепортируется» на вторую частицу.

Квантовая телепортация базируется на понятии квантовой связи или взаимовлиянии между частицами. Как известно из квантовой механики, частицы могут быть не только в отдельных состояниях, но и в «связанных» состояниях, так называемых квантовых состояниях, которые становятся взаимообусловленными. Используя эту особенность, ученые могут создавать особые квантовые пары частиц, такие как квантово-связанные фотоны.

Основное преимущество квантовой телепортации заключается в том, что она позволяет передавать информацию сразу, мгновенно, на любое расстояние. Это отличается от классической информационной передачи, основанной на использовании электромагнитных волн, где передача данных ограничена скоростью света.

Квантовая телепортация имеет огромный потенциал применения в различных областях науки и технологий. Например, она может быть использована для создания высокоскоростных коммуникационных систем, где передача информации происходит мгновенно и без задержек.

Кроме того, квантовая телепортация может использоваться в криптографии для обеспечения безопасной передачи данных. В классической криптографии секретный ключ передается по открытому каналу, что может предоставить возможность злоумышленнику перехватить ключ и расшифровать сообщение. С использованием квантовой телепортации можно достичь абсолютной безопасности, поскольку любая попытка перехвата и измерения состояния переданной частицы будет приводить к ее немедленной деструкции.

Квантовая телепортация также может иметь применение в квантовых компьютерах. Она может быть использована для передачи кубитов – квантовых битов, которые являются основными элементами квантовой информации. Квантовая телепортация позволит передавать кубиты между различными частями квантового компьютера, что увеличит его вычислительные возможности и поможет решать сложные задачи с высокой эффективностью.

Таким образом, квантовая телепортация на расстоянии дает возможность передавать квантовое состояние частиц мгновенно и на любые расстояния. Это открывает новые перспективы для развития коммуникационных систем, криптографии и квантовой вычислительной технологии.

Возможность передачи информации на расстояние с использованием квантовой телепортации обеспечивает бесперебойный и быстрый обмен данных между удаленными точками.

Одной из главных проблем в сфере коммуникаций является задержка в передаче данных, особенно при использовании современных сетей. Квантовая телепортация решает эту проблему, предоставляя возможность мгновенной передачи информации.

Квантовая телепортация основана на явлении квантовой связи между двумя частицами, которое называется квантовой запутанностью. При этом информация о состоянии одной частицы передается на другую частицу мгновенно, не зависимо от расстояния между ними.

Это позволяет использовать квантовую телепортацию для создания сетей, способных передавать информацию с высокой скоростью и без задержек. Например, такие сети могут быть полезны в сферах финансов, телекоммуникаций, научных исследований и многих других.

Кроме того, использование квантовой телепортации позволяет обезопасить передаваемую информацию. В современных системах шифрования данные передаются в зашифрованном виде по открытым каналам, что делает их уязвимыми для взлома. При использовании квантовой телепортации, с помощью принципа Ножницы-Бумага-Камень реализуется криптографическая защита. Это значит, что перехватчик не сможет получить информацию о передаваемых данных без непосредственного участия участников связи.

Таким образом, квантовая телепортация позволяет обеспечить бесперебойный и быстрый обмен информацией на расстоянии, а также обезопасить передаваемую информацию от несанкционированного доступа.

Процесс квантовой телепортации состоит из нескольких этапов. Вначале необходимо создать состояние взаимной связи между двумя частицами – той, которую необходимо телепортировать (называемой объектной частицей) и той, которая будет использоваться для передачи информации (называемой квантовым каналом). Для этого используется явление квантовой связи или «связь квантового состояния».

Далее, с помощью определенных операций и измерений на объектной частице, ее состояние взаимного взаимодействия с квантовым каналом измеряется и регистрируется. Полученная информация отправляется по классическому каналу связи (обычной проводной или беспроводной связи) на другой конец, где производится восстановление состояния объектной частицы.

Восстановление состояния частицы – это процесс, обратный созданию состояния взаимной связи. На этом этапе используется информация, полученная по классическому каналу связи, для изменения квантового состояния квантового канала таким образом, чтобы оно точно соответствовало состоянию объектной частицы. В результате, состояние объектной частицы «телепортируется» на расстояние без прямого перемещения самой частицы.

Основой для возможности передачи состояния частицы на расстояние является понятие квантовой связи и принципы квантовой механики. Это позволяет устанавливать взаимосвязь между частицами на фундаментальном уровне, не зависящем от пространственного разделения. Таким образом,

квантовая телепортация открывает новые перспективы для передачи информации и создания квантовых сетей связи.

Безопасность и защита данных

Квантовая запутанность представляет собой состояние, при котором два или более квантовых объекта становятся неразрывно связанными. Если одно из этих объектов изменяется, то другой объект мгновенно реагирует на это изменение, независимо от расстояния между ними.

Используя квантовую запутанность, при передаче данных по каналу связи, можно обеспечить их безопасность. При попытке несанкционированного просмотра или перехвата данных, состояние квантового объекта-носителя информации изменится, и получатель сможет обнаружить вмешательство.

Кроме того, квантовая телепортация может использоваться для создания квантовых криптографических систем, которые обеспечивают безопасную передачу информации. При использовании квантовой телепортации для передачи ключей шифрования, атакующая сторона не сможет перехватить ключ, так как при любой попытке измерения состояния квантового ключа, его состояние изменится и сторонний наблюдатель будет обнаружен.

Квантовая телепортация, благодаря своим особенностям, обеспечивает высокий уровень безопасности передаваемых данных и может найти применение в различных областях, таких как криптография, финансовые транзакции, связь и прочее.

Кубиты могут находиться в суперпозиции, состоянии, которое представляет собой комбинацию состояний 0 и 1. Это позволяет кубитам выполнять несколько вычислений одновременно, что делает квантовые вычисления намного более мощными и эффективными по сравнению с традиционными вычислениями.

Применение квантовой телепортации в квантовых вычислениях основывается на передаче квантовой информации между кубитами на расстоянии. Это позволяет создавать сети кубитов, которые могут взаимодействовать и эффективно выполнять сложные вычисления.

Применение квантовой телепортации в квантовых вычислениях также позволяет решать проблемы, которые недоступны для традиционных компьютеров. Например, квантовый алгоритм Шора использует квантовую телепортацию для факторизации больших чисел, что может иметь важное значение для криптографии.

Квантовая телепортация и квантовые вычисления в целом представляют собой важное направление исследований, которые могут привести к революции в области информационных технологий. Благодаря квантовой телепортации, кубиты могут быть связаны на расстоянии и взаимодействовать друг с другом,

открывая новые возможности для создания мощных и эффективных квантовых компьютеров.

Развитие технологий в сфере связи и коммуникаций не стоит на месте. Вместе с развитием квантовой телепортации открываются новые перспективы для передачи информации на расстоянии.

Одной из самых заметных проблем существующих коммуникационных сетей является ограничение на скорость передачи данных. Однако квантовая телепортация позволяет преодолеть эту проблему. За счет запутанных состояний и квантового взаимодействия, информация может быть передана сразу для нескольких устройств, что значительно увеличивает пропускную способность и скорость передачи данных.

Кроме того, квантовая телепортация обладает еще одним важным преимуществом – безопасностью. Использование квантовых состояний позволяет создать системы передачи информации, которые невозможно взломать или подменить. Это открывает новые возможности для обеспечения конфиденциальности и защиты данных.

Будущее связи и коммуникаций, безусловно, связано с развитием квантовой телепортации. Эта технология открывает новые горизонты для передачи информации и предлагает решение для таких проблем, как ограничение на скорость и безопасность передачи данных. С развитием квантовых сетей можем ожидать появления новых возможностей и сервисов, которые изменят наше представление о коммуникациях.

Источник: ermakovs.ru, 12.11.2023

Стартап Atom Computing начал тестирование квантового компьютера с 1000+ кубитами

Компания Atom Computing разработала в своей платформе квантовых вычислений следующего поколения атомный массив из 1225 узлов, заполненный 1180 кубитами.

Стартап впервые преодолел показатель в 1000 кубитов для многофункциональной системы с вентилями, выпуск которой планируют начать в следующем году.

Это чрезвычайно важное событие на пути к отказоустойчивым квантовым компьютерам, имеющим способность решать проблемы крупного масштаба.

В ходе тестирования атомный массив продемонстрировал рекордную скорость когерентности – хранение квантовой информации длилось на протяжении 40 секунд.

Также он имеет способность измерять квантовое состояние определенных кубитов во время вычислений и выявлять конкретные типы ошибок, не влияя на активность прочих кубитов.

При этом можно точно и последовательно регулировать работу кубитов для сокращения количества ошибок, возникающих в ходе вычислений, и исправлять их в режиме реального времени.

Стартап интегрировал в массив методы управления и алгоритмы работы, чтобы связать в «логический кубит» множество физических кубитов для получения точных результатов даже в случае возникновения ошибок.

Генеральный директор Atom Computing Роб Хейс заявил, что быстрое масштабирование – главное преимущество инновационной технологии атомных массивов компании.

Стартап, основанный всего 5 лет назад, уже обладает огромными ресурсами и способен конкурировать с более крупными компаниями.

Источник: arstechnica.com, 31.10.2023

Революция вычислительной мощности: квантовые компьютеры и криптовалюты

История последних десятилетий показывает, что технические инновации могут менять мир с невероятной скоростью. Биллу Гейтсу часто приписывают фразу, которую он якобы озвучил в 80-е годы: «640 КБ должно хватить всем». Сегодня это высказывание звучит смешно и уже стало крылатым выражением, описывающим то, как технологический прогресс не соотносится с нашими прогнозами о будущем. На наших глазах развивается технология квантовых компьютеров, которые, по утверждениям разработчиков, за минуты будут решать задачи, требующие от обычных компьютеров годы непрерывных вычислений.

Что такое квантовый компьютер

Если коротко, то это вычислительное устройство, которое работает на основе явлений квантовой суперпозиции и квантовой запутанности из квантовой механики – передовой области физики, описывающей поведение элементарных частиц. Обычные компьютеры работают на двоичной системе – каждый бит содержит строгое значение: либо 0, либо 1. Кубиты (квантовые биты) могут содержать одновременно 0 и 1. Кубиты позволяют настолько ускорить вычисления, что им под силу те задачи, перед которыми обычные компьютеры практически бессильны.

Существует даже термин «квантовое превосходство», характеризующий разницу между обычным и квантовым компьютером. Соответственно, достижение квантового превосходства означает успешное решение квантовым компьютером задачи, непосильной для традиционного компьютера.

Например, алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) считается достаточно стойким для современных вычислительных систем. Если же квантовому компьютеру удастся его взломать – а по оценкам экспертов именно ECDSA наиболее подвержен угрозам со стороны квантового компьютера – это будет значить, что для этой задачи достигнуто квантовое превосходство.

По ряду задач квантовое превосходство уже достигнуто: так, например, китайский квантовый компьютер Цзючжан в 2020 году выполнил гауссов бозонный сэмплинг за 200 секунд. Самому навороченному суперкомпьютеру потребовалось бы для этого 1,5 млрд лет. Стоит ли криптоэнтузиастам после подобных новостей волноваться за свои кошельки? Пожалуй, пока рано. Разумнее будет чуть глубже разобраться в ситуации.

Вычислительная мощность

Существующие сегодня решения – это, как правило, еще сравнительно слабые машины, заточенные под решение конкретных задач. «Слабые», разумеется, относительно наших завышенных ожиданий и мощностей, которые действительно могли бы изменить мир. Так, британские исследователи подсчитали, что взлом 256-битного шифрования сети Биткоина за час потребовал бы 317 млн кубитов. Уменьшение срока до 10 минут потребует уже 1,9 млрд кубитов. Современные решения колеблются в районе 150 кубитов. Таким образом, рост производительности может быть экспоненциальным, но путь в любом случае предстоит неблизкий. Google прогнозирует, что миллиона кубитов им удастся достичь к концу этого десятилетия.

Перспективы квантового компьютера в криптоиндустрии

Майнинг. Сразу скажем: собрать ферму на основе квантовых машин не получится. Алгоритм SHA-256 показывает себя довольно проблемным для квантовых вычислений, поэтому старые добрые ASIC-майнеры скорее всего пока никуда не пропадут.

Безопасность. Тут все сложнее, поскольку квантовый компьютер вполне может поставить под угрозу безопасность адресов Биткоина, ключей и цифровых подписей.

Эксперты из аудиторской компании Deloitte подсчитали, что, если бы сравнительно мощный квантовый компьютер существовал сегодня, под угрозой оказалось бы примерно 4 млн биткоинов (25% от общего числа). Почему только

четверть, а не все? Для разных типов адресов и для разного поведения пользователя риски квантового взлома будут различны. Так, для адреса P2PK (Pay-to-Public-Key) квантовая машина сможет получить закрытый ключ из открытого. К тому же, для этого нужно будет воспользоваться одним адресом дважды. Если же биткоины совсем не трогать, то и бояться нечего. С P2PKH (Pay-to-Public-Key Hash) все еще сложнее, однако, если такой адрес использовать дважды, то он тоже потенциально может быть взломан.

Во всем этом есть большое «но»: если постоянно менять адреса, то уровень безопасности существенно вырастает и тогда даже квантовые компьютеры теоретически не представляют большой угрозы. Более того, многие кошельки уже запрограммированы таким образом, чтобы максимально избегать повторного использования адресов.

Насколько реальна угроза квантового компьютера

На практике квантовой машине пока далеко до того, чтобы стать полноценной угрозой. Но предположим, что «квантовый мир победил» и «кубит оказался сильней». Погубит ли это феномен криптовалют? Вряд ли.

Во-первых, квантовый компьютер – машина сложная и капризная, требующая для корректной работы идеальных условий. Позволить себе такую роскошь смогут только самые богатые корпорации и процветающие государства. К слову, о последних: государства – не поклонники больших перемен, поэтому легко спрогнозировать, что как только квантовый компьютер станет угрозой текущему порядку вещей, они быстро примут меры. Государства либо монополизируют использование квантовых компьютеров, либо зарегулируют его так, что ни о каких взломах не будет и речи.

Во-вторых, криптовалюты могут защищаться и противостоять квантовой угрозе. Уже сейчас предлагаются решения из области пост-квантовой криптографии, предполагающие повышенную защиту от угроз на этом фронте. Поэтому худшее, что может случиться с Биткоином – это хардфорк и переход на более высокий уровень безопасности, защищающий его от квантовых угроз. Теоретически, может оказаться достаточным простое удлинение размера ключа шифрования или, например, переход на более сложный алгоритм, такой как SHA-512.

В-третьих, не стоит забывать, что у злоумышленников (или, если уж совсем фантазировать, ИИ), завладевших вычислительными возможностями квантового компьютера, будут куда более удобные цели для демонстрации квантового превосходства. Под угрозой окажутся все сферы, в том числе банки, государственные валюты и так далее.

Вывод

Квантовые компьютеры обладают высоким потенциалом в вычислительной мощности, но это крайне дорогое и технически сложное устройство. Для эффективного воздействия на блокчейн Биткоина и других криптовалют потребуются большие ресурсы, тогда как представленные на сегодняшний день устройства обладают ограниченным количеством кубитов. Так же существуют методы, благодаря которым криптовалюты могут стать более устойчивыми к подобному воздействию. Под вопросом остается и процесс законодательного регулирования применения квантовых компьютеров, ведь в руках злоумышленников они могут быть направлены на куда более легкие в сравнении с криптовалютой цели, а именно – банковские и государственные структуры.

Однако сооснователь Эфириума Виталик Бутерин считает, что быстрая эволюция квантовых компьютеров представляет потенциальную опасность, поэтому необходимы надежные решения для защиты безопасности пользователей. По его мнению, абстракция учетных записей (ERC-4337) может сделать пользовательские аккаунты квантово-устойчивыми.

Данный материал и информация в нем не является индивидуальной или иной другой инвестиционной рекомендацией. Мнение редакции может не совпадать с мнениями автора, аналитических порталов и экспертов.

Источник: ru.tradingview.com, 13.11.2023

Квантовая инженерия уже реальность

В этом году Нобелевская премия по химии была присуждена Алексею Екимову, Луису Брюсу и Мунги Бавенди за работы по синтезу нанометровых полупроводниковых кристаллов, – так называемых квантовых точек. Впервые квантовые точки были синтезированы в 1981 году и с тех пор привлекают большой интерес ученых, в том числе и армянских, поскольку эти исследования дают не только фундаментальные результаты, но и приобретают все большее практическое значение. Сегодня эти структуры стали важной элементарной базой для создания приборов нового поколения.

Уникальность этих объектов заключается в том, что этими атомарными структурами, которые часто называют искусственными атомами, можно управлять, меняя их компонентный состав, размеры и геометрические формы, от которых зависят характеристики этих систем. Квантовый мир очень чувствителен к геометрии.

За годы, прошедшие после того, как квантовые точки были синтезированы впервые, для создания этих структур было разработано и сегодня используется множество разных технологий.

Причем в каждой квантовой точке, в зависимости от поставленной практической задачи, ее конкретного применения, электронные оболочки заполняются по-разному. Так, например, в близких к естественным атомам сферических системах возникают свои аналоги тех законов заполнения оболочек, которые действуют в обычной атомной физике, в физике реальных атомов. Получается, что создается новый мир. Массивы квантовых точек могут образовать искусственную решетку. Они могут быть связаны друг с другом, и в этих системах могут возникать интересные коллективные эффекты. В то же время внутрь этой квантовой точки можно имплантировать определенное количество частиц, например, электронов, и они будут проявлять определенные статистические свойства. Таким образом, возникает целое поле абсолютно новых задач, требующих глубокого анализа, дальнейшего приложения в технологиях и, соответственно, в новых приборах.

При уменьшении размера полупроводника до нанометрового диапазона, роль поверхности материала резко возрастает. Важную роль начинают играть квантовые эффекты, возникают совершенно новые свойства, которые можно получить в зависимости от поставленной задачи. И классическая физика уже не в состоянии описать такие системы.

Сегодня стало возможным синтезировать структуры с заданными характеристиками, то есть с управляемыми свойствами. Иначе говоря, возникла уникальная ситуация, когда наряду с реальными атомами, в которых спектр частиц полностью дискетный, в квантовых точках, задавая определенные параметры роста, можно искусственно создать те спектральные характеристики, которые необходимы конкретному прибору. Например, если в данном случае необходим коротковолновый диапазон, то есть чтобы излучение кристалла было ближе к синему, размеры квантовых точек уменьшаются, и технологи синтезируют кристалл под те или иные задачи. Они получают соответствующую структуру, которая используется в конкретном приборе, что очень важно. И, как уже было сказано, эти возможности квантовых точек находят широкое практическое применение. В первую очередь это светодиоды нового поколения, различные чувствительные полупроводниковые датчики. Например, эти возможности нашли конкретное практическое применение при создании экранов телевизоров, поскольку массивы квантовых точек представляют собой излучающие яркие и ясные элементы, что обеспечивает высокое качество изображения.

– Хочу обратить внимание на один интересный факт, – говорит доктор физико-математических наук, профессор Айк Саркисян. – В 1959 году на

ежегодной встрече Американского физического общества в Калифорнийском технологическом институте выдающийся американский физик, лауреат Нобелевской премии Ричард Фейнман, выступил с чрезвычайно интересной лекцией, которая называлась «Внизу много места: приглашение войти в новую область физики». В этой лекции Фейнман говорил о возможностях манипулирования отдельными атомами, как перспективной области синтетической химии и высказал уверенность в том, что придет время, когда люди смогут на уровне атомных решеток конструировать необходимые структуры. А это значит, что возникнет атомно-молекулярная архитектура, благодаря которой человек будет выращивать структуры на квантовом уровне. Прогнозы Фейнмана оказались пророческими, они полностью оправдались. Сегодня квантовая инженерия стала реальностью. Люди научились выращивать квантовые точки, которые находят широкое применение в оптоэлектронных приборах. Причем сами эти приборы – не наноразмерные, но они основаны на наноструктурах.

Исследованиями этих структур занимаются и в Армении. Эти работы начались вскоре после того, как впервые были синтезированы квантовые точки и уже в середине 80-х годов прошлого века научная группа, которую создал академик Эдуард Казарян, начала активно проводить теоретические исследования этого направления, а в 1985 году была опубликована статья по фононному поглощению света квантовыми точками. Тогда эти исследования только начинались. Проводимые в дальнейшем исследования подтвердили, что нанокристаллы обладают уникальными оптическими свойствами, что создает серьезные перспективы их использования, например, в солнечной энергетике.

Созданная академиком Казаряном научная школа, которую он возглавляет и сегодня, продолжает активно работать. «Уже в течение 20 лет мы занимаемся оптикой квантовых точек, вопросами, связанными с кулоновскими комплексами в этих структурах, многочастичными системами и спиновыми свойствами квантовых точек. Для проведения прикладных исследований этого направления необходима дорогостоящая аппаратура, которой у нас, к сожалению, нет. Но именно теоретические исследования способствуют пониманию процессов, происходящих в квантовых точках, и являются той фундаментальной основой, на которой развивается прикладная наука», – сказал профессор Айк Саркисян.

Источник: eenergy.media, 20.11.2023

Новые квантовые эффекты в транспорте электронов обнаружили ученые института физики полупроводников

Ученые Института физики полупроводников им. А.В. Ржанова СО РАН обнаружили новые квантовые явления в транспорте электронов. Эффекты связаны с наблюдением и исследованием мезоскопических флуктуаций проводимости в двумерном полуметалле. Работа выполнялась в рамках крупного научного проекта «Квантовые структуры для посткремниевой электроники», результаты опубликованы в журнале Nanomaterials.

О научном достижении рассказал на Школе молодых ученых «Оптика и фотоэлектрика квантовых систем» один из авторов работы, заведующий лабораторией физики низкоразмерных электронных систем ИФП СО РАН член-корреспондент РАН Дмитрий Харитонович Квон. Школа прошла в ИФП СО РАН при поддержке Российского научного фонда (проект № 23-72-30003).

Мезоскопические системы – промежуточные между микро- и макроскопическими системами. Свойства мезоскопических систем зависят от размеров, входящих в них элементов. Макроскопическими системами считаются те, у которых свойства не меняются при увеличении их размеров. В микроскопических системах размеры элементов сравнимы с размерами атомов.

«Наше наблюдение важно с точки зрения поиска новых квантовых эффектов, и оно свидетельствует о неизвестном до нашего эксперимента проявлении квантово-механических свойств электронов в твердом теле. Ранее мезоскопические флуктуации проводимости наблюдались только в образцах субмикронных размеров. Мы же обнаружили их в большом (макроскопическом) образце, размером более 100 микрон, причем только в двумерном полуметалле. В обычном металле явление отсутствует.

Почему так происходит? Мы предложили качественную интерпретацию: концентрация проводящих дырок в образце во много десятков раз больше концентрации электронов. В такой системе из-за сильного беспорядка появляются области, где электронов нет, и области, где они существуют. Соответственно, возникает сетка электронных каналов в матрице проводящих дырок. Каналы усиливают явление квантовой интерференции, и появление флуктуаций определяется уже не размерами системы, а характерным периодом сетки», – пояснил член-корреспондент РАН заведующий лабораторией физики низкоразмерных электронных систем ИФП СО РАН Дмитрий Харитонович Квон.

Источник: scientificrussia.ru, 14.11.2023

Как «СМАРТС» вышел на рынок квантовых гигантов

Квантовые разработки и уникальные решения на их базе закладывают прочнейший фундамент для формирования безопасного будущего. Передовые ученые, компании и научные институты сегодня работают в единой связке. В их числе и группа «СМАРТС.

«Поиск и реализация технологичной идеи, которая позволила бы опередить время, – это задачи, которые я всегда ставил и ставлю перед собой и коллективом", – говорит бенефициар группы «СМАРТС», председатель совета директоров АО "СМАРТС" Геннадий Кирюшин. Сделав ставку на квантовые технологии и вложив в эту идею сотни миллионов рублей после продажи сотового бизнеса, самарский новатор, как и в начале 1990-х, когда предпочел GSM-связь более популярному в те времена DAMPS, снова оказался на шаг впереди.

«Развивая сотовый бизнес в России, мне приходилось вести переговоры с крупнейшими технологическими компаниями мира, и еще задолго до появления новых поколений связи (3G, 4G, 5G и т. д.) мы изучали способы передачи большого объема данных по защищенным каналам», – вспоминает Кирюшин. Одним из актуальных вопросов того времени была возможность доступа к коммуникациям в любое время года, что без специальных технологий укладки оптоволокна было недостижимо.

Так, в 2014 году у СМАРТСа появился проект по «Созданию защищенных автодорожных телекоммуникационных систем». Он был призван решить вопрос по созданию развитой инфраструктуры для построения волоконно-оптических сетей связи с круглогодичным доступом к коммуникациям. Идея проекта заключалась в закладке пакета микротрубок в минитраншею, разработанную в обочине автодороги, с последующей задувкой волоконно-оптического микрокабеля. На сегодняшний день СМАРТС построил более 1,5 тыс. км инфраструктуры для цифровизации дорожной отрасли и развития интеллектуально-транспортных систем. В перспективе проект предусматривает развитие во всех субъектах страны, а совокупный объем инвестиций достигнет 250 млрд рублей. Он уже реализован в Самарской области и охватывает 10 городских округов и 27 муниципальных районов.

В 2021 году СМАРТС построил первую региональную квантовую сеть в России, которая соединила центры обработки данных (ЦОДы) компании в Самаре, Тольятти и Сызрани. Проект поддержан Российским фондом развития информационных технологий, и на реализацию был предоставлен Правительственный грант (в качестве софинансирования проекта «СМАРТС») в рамках федерального проекта «Цифровые технологии» национальной программы «Цифровая экономика». Взломать такую сеть невозможно.

Ключевая информация для шифрования в этом случае передается по линиям связи с помощью потока одиночных фотонов – их невозможно разделить, скопировать или незаметно отвести в сторону. При этом смена квантовых ключей шифрования происходит постоянно с частотой свыше 10 раз в секунду.

Технологию построения программно-конфигурирумых квантовых сетей СМАРТС начинал развивать еще в 2017 году, совместно с университетом ИТМО и «Квантателеком». В 2018 году СМАРТС приобрел контрольный пакет (51%) в производственной компании «Квантателеком». В 2022 году ее переименовали. Сегодня «СМАРТС-Квантателеком» – один из лидеров в области квантовых коммуникаций и ядро группы «СМАРТС» в Северной столице России.

Предприятие служит партнером ОАО «Российские железные дороги», участвуя в реализации большой федеральной программы по развитию квантовых коммуникаций. Системы компании активно используются в действующей инфраструктуре РЖД: разворачиваются сети передачи данных с использованием узлов, где располагается квантовое оборудование. Компания сотрудничает с Главным управлением связи Вооруженных Сил РФ, в том числе с Военной академией связи в Санкт-Петербурге. В настоящее время прорабатываются различные аспекты применения этих технологий в интересах систем связи и программно-аппаратных комплексов Вооруженных Сил РФ.

Говоря о новых технологиях и трендах, Геннадий Кирюшин отметил, что будущее – за квантовыми технологиями и уже в ближайшей перспективе большинство каналов связи будут закрываться именно квантовыми ключами.

Источник: volga.news, 13.11.2023

Квантовые вычисления могут ускорить разработку лекарств

В 2022 году рынок разработки лекарств оценивался в 55,46 млрд долл., и к 2032 году прогнозируется его рост более чем вдвое, достигнув 133,11 млрд долл. В условиях таких динамичных изменений, акцент на времени становится ключевым в секторе разработки лекарств, особенно после вызовов, предъявленных COVID-19.

Одним из перспективных путей оптимизации процессов стало внедрение квантовых вычислений. С их помощью открытие противовирусных препаратов может занять несколько месяцев вместо лет, снижая затраты времени и ресурсов.

Квантовые компьютеры существенно сокращают время исследований, обеспечивая более точные прогнозы о поведении молекул. Это имеет

критическое значение, ускоряя разработку терапевтических средств и повышая качество конечных соединений.

В среднем, вывод нового лекарства на рынок обходится в 1,3 млрд долл. Квантовые вычисления могут существенно снизить эту стоимость, сокращая период исследований и ускоряя процесс разработки.

Однако, несмотря на потенциальные выгоды, интеграция квантовых вычислений с существующей ИТ-инфраструктурой остается сложной задачей. Недостаток талантов в области квантовых вычислений и нестабильность квантового оборудования также представляют вызовы для компаний.

Квантовые вычисления обещают революционизировать фармацевтическую индустрию, но требуют внимательного решения технических и организационных проблем. С их успешным внедрением можно ожидать ускоренного развития новых лекарств и снижения общих затрат в этом важном секторе.

Источник: involta.media, 13.11.2023

Квантовые сети на железной дороге: основные принципы и применение

Квантовые сети – одно из самых инновационных достижений в области современных технологий. Они основаны на принципах квантовой физики и представляют собой сети из квантовых узлов, которые могут обрабатывать информацию в форме квантовых битов (кьюбитов). В последние годы такие сети широко используются в различных сферах, таких как вычисления, криптография и передача данных.

В последнее время исследователи начали обращать внимание на потенциальное применение квантовых сетей в транспортной индустрии. Особый интерес вызывает использование квантовых сетей в железнодорожном транспорте. Это связано с тем, что железные дороги играют важную роль в мировом транспортном секторе и высокие требования к безопасности и эффективности работы этой отрасли.

Концепция квантовых сетей на железной дороге основана на использовании квантовой телепортации для создания безопасной и надежной системы передачи информации. В квантовых сетях на железной дороге, информация может передаваться между квантовыми узлами, используя принципы квантовой физики, такие как суперпозиция и запутанность кюбитов. Такая система обладает высокой степенью защиты от взлома и подмены данных, что крайне важно для обеспечения безопасности на железнодорожных перегонах и станциях.

Помимо обеспечения безопасности, применение квантовых сетей на железной дороге может также повысить эффективность работы системы. Квантовые сети позволяют осуществлять быструю передачу информации с минимальной задержкой, что позволяет быстро реагировать на изменения в транспортном потоке и оптимизировать работу железнодорожного транспорта. Кроме того, квантовые сети могут быть использованы для создания системы управления железнодорожным транспортом, которая позволит автоматизировать процессы и уменьшить ошибки, связанные с человеческим фактором.

Квантовые сети на железной дороге:

Применение квантовых сетей на железной дороге может привести к революционным изменениям в области транспорта. Они позволят значительно увеличить пропускную способность железнодорожных линий, обеспечивая высокую скорость и надежность передачи данных. Кроме того, квантовые сети позволяют решить проблему информационной безопасности и защитить систему от взломов и кибератак.

Основным преимуществом квантовых сетей на железной дороге является заметное снижение задержек по сравнению с традиционными сетями. Использование квантовых технологий позволяет обеспечить быструю передачу данных и точную синхронизацию работы системы, что особенно важно для железнодорожного транспорта.

Однако, несмотря на многообещающие перспективы квантовых сетей на железной дороге, их внедрение требует значительных инвестиций и разработки соответствующей инфраструктуры. Кроме того, существует необходимость в подготовке специалистов, способных работать с такой новой технологией.

Тем не менее, квантовые сети на железной дороге представляют огромный потенциал для улучшения транспортной инфраструктуры. Они позволят создать интеллектуальные сети, способные оперативно реагировать на изменения в состоянии железнодорожных линий и обеспечивать более безопасное и эффективное движение поездов.

Концепция квантовых сетей

Квантовые сети представляют собой новое поколение информационных систем, основанных на принципах квантовой механики. Эта концепция открывает возможности для создания высокоскоростных и надежных сетей связи, способных решать сложные задачи в области передачи данных.

Основной элемент квантовой сети – квантовый бит или кубит, который использует принципы квантовой механики для хранения и обработки информации. Квантовый бит может находиться в состоянии, называемом

сверткой, которое позволяет одному кубиту принимать несколько значений одновременно. Таким образом, квантовые сети могут обрабатывать и передавать информацию совершенно иначе, чем классические компьютеры и сети.

Одной из основных задач квантовых сетей является квантовая телепортация – передача квантового состояния одного кубита на другой удаленный кубит без физического перемещения частицы. Это явление основано на принципе квантовой связи, называемой квантовым запутыванием, и может быть использовано для создания защищенных и надежных сетей связи.

Кроме того, квантовые сети имеют квантовый параллелизм, позволяющий проводить одновременные вычисления на нескольких кубитах. Это свойство делает квантовые сети более эффективными в решении сложных вычислительных задач, таких как факторизация больших чисел или оптимизация сложных алгоритмов.

Однако, разработка и применение квантовых сетей в настоящее время является активной областью исследований, и требует дальнейшего развития технологий и алгоритмов. Несмотря на это, концепция квантовых сетей представляет огромный потенциал для будущего развития информационных технологий и связи.

Применение квантовых сетей в сфере железнодорожного транспорта

Квантовые сети представляют собой сетевые структуры, основанные на принципах квантовой физики и способные обеспечить передачу и обработку информации на квантовом уровне. В сфере железнодорожного транспорта такие сети могут использоваться для улучшения безопасности, эффективности и надежности работы систем.

Безопасность:

Квантовые сети могут быть применены для повышения безопасности железнодорожных систем. Передача информации в них осуществляется на квантовом уровне, что делает ее устойчивой к взломам и подделкам. Кроме того, такие сети позволяют создавать криптографические ключи с использованием квантовых состояний, что значительно повышает степень защиты данных.

Эффективность:

Квантовые сети позволяют улучшить эффективность работы железнодорожных систем. Благодаря использованию квантовой телепортации информации, можно осуществлять удаленное диагностирование и контроль состояния устройств и сетей, что сокращает время и затраты на обслуживание. Кроме того, квантовые сети способны передавать информацию с большей

скоростью и пропускной способностью, что улучшает скорость и надежность передачи данных.

Надежность:

Квантовые сети обладают высокой степенью надежности, что является особенно важным в сфере железнодорожного транспорта. Благодаря применению принципов квантовой измеримости, информация может быть передана без искажений и помех, что обеспечивает стабильную работу систем и снижает риск возникновения чрезвычайных ситуаций.

Применение квантовых сетей в сфере железнодорожного транспорта имеет большой потенциал для совершенствования работы систем и повышения качества услуг. Однако, внедрение таких сетей требует дальнейших исследований, разработок и инвестиций.

Преимущества квантовых сетей на железной дороге

Квантовые сети представляют собой новую концепцию в сфере телекоммуникаций на железнодорожном транспорте. Они отличаются от традиционных сетей высокой скоростью передачи данных и устойчивостью к помехам. В этом разделе мы рассмотрим ключевые преимущества квантовых сетей на железной дороге.

1. Высокая скорость передачи данных: Квантовые сети позволяют передавать данные со скоростью, сравнимой с максимально достижимой скоростью света. Это позволяет железнодорожным операторам обмениваться большим объемом информации в режиме реального времени, что способствует улучшению работы и эффективности системы.

2. Устойчивость к помехам: В отличие от традиционных сетей, квантовые сети обладают большей устойчивостью к помехам и внешним воздействиям. Это особенно важно на железной дороге, где могут возникать различные помехи, такие как электромагнитные излучения, вибрации и т.д. Квантовые сети позволяют поддерживать стабильную связь даже в условиях повышенной помехоустойчивости.

3. Безопасность передачи данных: Квантовые сети обладают высоким уровнем безопасности передачи данных. Они используют особые протоколы шифрования, основанные на принципах квантовой физики, которые невозможно взломать современными криптографическими методами. Это делает квантовые сети идеальным выбором для передачи конфиденциальной информации на железной дороге.

4. Гибкость и масштабируемость: Квантовые сети позволяют легко масштабировать систему в соответствии с растущими потребностями. Они демонстрируют высокую гибкость в поддержке различных протоколов и

форматов данных, что облегчает интеграцию с другими системами и оборудованием на железной дороге.

Таким образом, квантовые сети на железной дороге предоставляют ряд значимых преимуществ, которые сделают транспортную систему более быстрой, надежной и безопасной.

Развитие квантовых сетей в железнодорожной отрасли

Квантовые сети представляют собой инновационное решение, которое играет важную роль в развитии железнодорожной отрасли. Они открывают новые возможности для повышения эффективности и безопасности железнодорожного транспорта.

Одной из ключевых особенностей квантовых сетей является возможность передачи и обработки большого объема данных с высокой скоростью и точностью. Это позволяет операторам системы железнодорожного транспорта эффективно управлять движением поездов, оптимизировать расписание и предотвращать возникновение аварийных ситуаций.

Кроме того, квантовые сети обладают высокой степенью надежности и устойчивости к внешним воздействиям, таким как электромагнитные помехи или перегрузки в сети. Это особенно важно для железнодорожной отрасли, где безопасность и надежность системы имеют решающее значение.

Применение квантовых сетей в железнодорожной отрасли также способствует снижению энергопотребления и обеспечению экологической устойчивости. Благодаря оптимизации работы системы, можно достичь экономии энергии и снижения выбросов вредных веществ в окружающую среду.

Важным аспектом развития квантовых сетей в железнодорожной отрасли является обучение специалистов и переподготовка персонала. Для эффективного использования новых технологий необходимо иметь специалистов, которые смогут разрабатывать и поддерживать инфраструктуру квантовых сетей, а также анализировать и использовать полученные данные.

Таким образом, развитие квантовых сетей в железнодорожной отрасли открывает новые перспективы для модернизации системы транспортировки и управления поездами. Это позволяет повысить эффективность работы и обеспечить безопасность пассажиров и грузов. Квантовые сети являются одним из ключевых элементов цифрового преобразования железнодорожной отрасли и являются обещающей технологией будущего.

Перспективы использования квантовых сетей в железнодорожной отрасли

Одной из главных проблем, с которыми сталкиваются железные дороги, является необходимость обеспечения безопасности и эффективности связи

между различными устройствами и системами, такими как поезда, пульмены, станции управления и системы информационной безопасности.

Квантовые сети основаны на принципах квантовой механики и предлагают новые возможности для передачи информации с высокой скоростью и безопасности. Квантовая связь позволяет достичь достоверности передачи данных, которую невозможно достичь с помощью классических методов.

Применение квантовых сетей в железнодорожной отрасли может привести к значительному улучшению эффективности и безопасности. Квантовая связь позволит передавать данные с большой скоростью, что позволит улучшить планирование и управление движением поездов, оптимизировать использование ресурсов и снизить затраты на энергию.

Одна из важных областей применения квантовых сетей в железнодорожной отрасли – это обеспечение безопасности и защиты информации. Квантовая связь обладает возможностью обнаружения попыток вторжения и подмены данных, что поможет предотвратить кибератаки и обеспечить надежную защиту систем железной дороги.

Квантовые сети также могут быть использованы для создания умных систем управления движением поездов, которые будут способны адаптироваться к изменяющимся условиям и обеспечивать наилучшую эффективность использования ресурсов.

Использование квантовых сетей в железнодорожной отрасли имеет большой потенциал для решения сложных задач и совершения качественного прорыва. Это технология, которая может изменить существующие подходы к управлению и связи в железнодорожной системе, обеспечивая высокую скорость, надежность и безопасность передачи данных.

Источник: zim-nk.ru, 11.11.2023

Физик РАН рассказал об интернете будущего

Физик Алексей Федоров уверен, что квантовый интернет сыграет решающую роль в широком внедрении квантовых технологий. В интервью РИА Новости он раскрыл перспективы, которые открывает этот новый инструмент коммуникаций, а также описал необходимые условия для его запуска.

Первая квантовая революция – это период быстрого технологического прогресса, который наступил после открытия квантовой физики. В результате этих исследований были изобретены транзисторы и лазерные технологии, а

затем стали доступны персональные компьютеры и другие цифровые устройства. Считается, что сегодня мы на пороге второй квантовой революции. Такая революция ставит перед собой одну из главных целей – разработку универсального квантового компьютера, способного справиться с вычислениями, недоступными для существующих технологий.

Основная сложность заключается в том, что для достижения этой цели необходимо создать систему, объединяющую, казалось бы, несовместимые свойства. С одной стороны, квантовый компьютер должен быть достаточно большим, чтобы обрабатывать огромные объемы данных. С другой стороны, его увеличение в размерах не должно приводить к потере квантовых свойств. Это означает, что необходим определенный уровень контроля над квантовой системой. Ученые считают, что одним из решений может стать создание устройств на базе концепции квантового интернета. Такой подход позволит увеличить вычислительную мощность квантовых компьютеров, объединив их в квантовые сети без ущерба контролю над каждым из них.

Источник: runews24.ru, 19.11.2023

Квантовые технологии начнут развивать на Дальнем Востоке

Дальневосточный государственный университет путей сообщения (ДВГУПС; Хабаровск) и российский разработчик квантовых решений для информационной безопасности QRate подписали соглашение о сотрудничестве в области развития квантовых технологий и подготовке кадров. Подписание состоялось 17 ноября в рамках проходящей в Москве «Транспортной недели».

Дальневосточный университет путей сообщения (ДВГУПС) продолжает развивать наукоемкие технологии, среди которых технология квантовых коммуникаций и квантовой криптографии. Сегодня на Транспортной неделе, проводимой Министерством транспорта России, ДВГУПС заключил соглашение о сотрудничестве с QRate – одной из крупнейших российских компаний в области квантовых технологий. После подписания соглашения ДВГУПС войдет в число немногих федеральных учреждений высшего образования, которые продвигают развитие квантовых технологий. Среди таких ВУЗов – МГУ, МТУСИ, МИСИС и другие.

Павел Воробьев, исполнительный директор QRate:

«Наш век демонстрирует особую роль университетов в развитии новых технологий. Университет – это, в первую очередь, площадка, позволяющая опережающим образом внедрить технологии в соответствии с требованиями заказчиков, научить пользователей не бояться инноваций, быть местом для

диалога между заказчиками и разработчиками. Уверен, что Дальневосточный государственный университет путей сообщений станет нашим надежным партнером в развитии стратегически важной для страны технологии».

Развитие квантовых коммуникаций отвечает важному требованию цифровой трансформации: развитию кадрового потенциала и выстраиванию системы образования на базе междисциплинарных учебных программ. Квантовые коммуникации – сквозная технология, позволяющая обеспечить максимально возможную степень защиты данных, гарантированную законами физики.

Владимир Буровцев, ректор ДВГУПС:

«Дальневосточный государственный университет путей сообщения является ведущим транспортным университетом Востока страны, который должен изучать и развивать современные технологии, в том числе и такие, как квантовые технологии связи, дающие значительные перспективы в развитие транспортной отрасли. Стоит отметить, что только во взаимодействии с индустриальными партнерами-лидерами, компанией QRate, создаются условия успешной реализации совместных образовательных и научных проектов, которые в будущем станут основой эффективной и безопасной коммуникации».

В соответствии с решением правительства России компания ОАО «РЖД» является ответственной за развитие высокотехнологичной области «Квантовые коммуникации». Подписанное соглашение позволяет ДВГУПС, являясь транспортным ВУЗом, не отставать от потребностей основного работодателя выпускников ДВГУПС.

Источник: itspeaker.ru, 17.11.2023

Квантовый нейрорасчет на холодном ионе

Ученые физического факультета МГУ совместно с коллегами из Физического института имени П. Н. Лебедева РАН впервые предложили использовать ультрахолодные ионы для создания квантовых мемристоров и проведения квантовых нейроморфных вычислений.

Нейроморфные вычисления – это подход к вычислительной технике, основанный на структуре и функциях человеческого мозга. Нейроморфный компьютер использует физические «искусственные нейроны» для решения своих вычислительных задач. Теоретически можно создать и квантовый нейроморфный компьютер – об этом задумались физики из МГУ и ФИАНа.

Ловушка Пауля и осцилляции Раби

Нейроморфные вычисления в основном проводятся с использованием классических мемристоров – устройств, электрическое сопротивление которых зависит от заряда, протекшего через них в предыдущие моменты времени, что позволяет им «запоминать» электрический сигнал, аналог гестерезиса в магнетизме для электричества. Такие вычисления доказали свою эффективность при решении ряда задач, таких, например, как распознавание образов и речи, прогнозирование, обобщение. Вместе с тем в настоящее время активно развиваются квантовые вычисления, которые имеют неоспоримые преимущества по сравнению с классическими, благодаря высокому уровню параллелизма, масштабируемости, принципу суперпозиции и запутанности. Возникла естественная идея найти такой класс устройств, который позволил бы проводить нейроморфные квантовые вычисления. К таким устройствам относятся квантовые мемристоры.

«К настоящему моменту направление развития квантовых мемристоров и их использования в нейроморфных вычислениях находится еще в зачаточной стадии. Предложена реализация квантовых мемристоров на нескольких платформах, на которых как раз и развиваются квантовые вычисления: квантовая фотоника и сверхпроводящие схемы. На некоторых из них уже реализуются методы машинного обучения. Однако за рамками рассмотрения оказалась ионная платформа, которая продемонстрировала свои уникальные преимущества в квантовых вычислениях», – отметил автор исследования, заместитель декана по научной работе физического факультета МГУ Павел Форш.

Это позволяет объединить преимущества квантовых вычислений и нелинейной мемристивной динамики изменения параметров, осуществлять хранение информации и проведение вычислений в рамках одного объекта. Ученые пришли к выводу, что ионная платформа – помещение ионов в электродинамическую ловушку – обладает рядом преимуществ по сравнению с предложенными ранее, поскольку в ее рамках открывается возможность создания целой последовательности связанных единичных мемристоров для проведения логических операций.

Для реализации концепции квантового мемристора необходимо поместить ультрахолодный ион в ловушку Пауля (использует динамические электрические поля для улавливания заряженных частиц), облучить его двумя лазерными полями, частота колебаний электромагнитного поля которых попадает в резонанс с последовательными переходами между уровнями иона. Такое воздействие позволяет инициировать осцилляции Раби населенности между специально подобранными тремя уровнями иона (осцилляции Раби –

плавный и периодический переход системы между энергетическими уровнями в ситуации воздействия на нее достаточно длинного и интенсивного импульса). Измеряя населенность одного из выбранных уровней и внося тем самым частичную декогерентность общему состоянию системы на определенном временном отрезке, можно модифицировать частоту осцилляций населенностей Раби, изменяя параметры лазерного поля (интенсивности излучения, длительности импульса) для последующего интервала времени. Тем самым осуществляется эффективное управление динамикой населенностей уровней трехуровневой системы. В результате чего, определяя входной сигнал в качестве населенности выбранного уровня после действия одночастотного поля, а выходной сигнал – в качестве населенности того же уровня после действия двух лазерных импульсов и осуществляя управление параметрами полей, можно получить гистерезисную зависимость выходного сигнала при изменении входного сигнала.

Многослойный квантовый персептрон

Предложенная идея была подтверждена серией численных расчетов. Кроме того, на примере 171Yb+ были предложены конкретные уровни, которые соответствуют необходимым условиям для осуществления мемристивной динамики, а также удобны для экспериментальной реализации квантового мемристора.

«Таким образом, мы впервые сформулировали идею создания квантовых мемристоров на ионной платформе, предложили конкретную схему для экспериментальной реализации предложенного объекта. Кроме того, продемонстрировали преимущество ионной платформы для реализации квантового мемристора, которое заключается в том, что квантовое состояние может быть передано другому связанному силами кулоновского взаимодействия иону по цепочке за счет низкочастотной колебательной моды центра масс. Это позволит задействовать два и более ионов для проведения логических операций, формируя нейронную сеть. Вместе с тем обилие уровней даже в одиночном ионе позволяет предложить схему связанных квантовых мемристоров в рамках одного иона, когда последовательное действие резонансных полей позволяет передавать состояние от мемристора к мемристору. Наличие двух и более групп уровней на одном ионе с предложенной схемой передачи информации по цепочке связанных ультрахолодных ионов позволит создавать многослойные квантовые персептроны, которые являются основной нейронных сетей», – подвел итог работы профессор физического факультета МГУ Сергей Стремоухов.

Источник: stimul.online, 21.11.2023

Постквантовый алгоритм электронной подписи «Шиповник» получил открытую реализацию

Российские компании с экспертизой в области криптографии и квантовых технологий объединяют усилия для предотвращения угрозы криптографическим системам со стороны квантовых компьютеров.

Так, открытая реализация отечественного постквантового алгоритма «Шиповник» компании «Криптонит» подготовлена компанией «QApp» в ходе её деятельности в составе рабочей группы «Постквантовые криптографические механизмы» Технического комитета 26 Росстандарта (ТК 26). Проект написан на языке Си с оптимизацией под наборы команд SSE4.1, SSE2 и MMX. Исходный код доступен на GitHub. Он компилируется в библиотеку, которую можно встраивать в промышленные криптографические устройства и программные продукты.

«Использование оптимизации кода приводит к высокой скорости реализации «Шиповника». В тестах на Intel Core i7-8700 выработка ключевой пары заняла 3 мс, подпись одного сообщения – 848 миллисекунд, а проверка подписи – всего 11 мс», – пояснил Сергей Гребнев, криптоаналитик и руководитель группы прикладных исследований компании «QApp».

«Шиповник» – алгоритм электронной подписи, устойчивый к атакам с использованием квантового компьютера. Он разработан экспертами-криптографами российской компании «Криптонит», участвующими в деятельности рабочей группы ТК 26.

Алгоритм «Шиповник» построен на основе теоретико-кодового протокола идентификации Штерна. Стойкость этой схемы подписи к подделке основана на сложности задачи декодирования случайного линейного кода. Профессором математики Элвином Берлекэмпом в 1978 году было доказано, что эта задача относится к классу NP-сложных задач. Для задач данного класса до сих пор неизвестны эффективные алгоритмы решения ни на классическом компьютере, ни на квантовом.

Согласно данным «Криптонита», в настоящий момент лучшая известная атака с использованием классического компьютера на схему «Шиповник» потребует 2^256 битовых операций. То есть её невозможно выполнить за разумное время на самых быстрых суперкомпьютерах. Теоретическая стойкость к «квантовой» атаке оценивается в 2^170 операций, что также делает её выполнение невозможным даже на квантовых компьютерах будущего с миллиардами рабочих кубитов.

«Считаю публикацию программной реализации схемы подписи «Шиповник» значимым событием в международном криптографическом сообществе и важной вехой в развитии отечественной постквантовой

криптографии. Она позволяет создавать надёжные реализации электронной подписи, устойчивые к атакам с использованием самых мощных суперкомпьютеров традиционной архитектуры и ещё только разрабатываемых квантовых компьютеров», – пояснил руководитель лаборатории криптографии компании «Криптонит» Василий Шишкин.

«Если идти по пути традиционного принципа противодействия: сначала проблема, а потом решение, то надёжных решений информационной безопасности не построить. В те далёкие годы учёные пошли по пути разработки защиты, не имея реальной угрозы. Когда математика и физика как науки стояли у истоков защиты информации, был заложен основной фундамент в постквантовой криптографии и защите от атак с применением квантовых компьютеров при реальном отсутствии мощных вычислителей. Сегодня, когда вычислительные мощности производят сложнейшие операции за доли секунд, мы видим, как рабочая группа «Постквантовые криптографические механизмы» в составе ведущих специалистов из компании «Криптонит» и компании-резидента Киберхаба Сколково QApp создали открытую реализацию нового постквантового алгоритма электронной подписи «Шиповник». Данный алгоритм обеспечит целостность и доступность информации при передаче на любые расстояния и будет актуален ещё многие годы», – добавил руководитель Киберхаба Сколково Игорь Бирюков.

Разработкой квантовых компьютеров сегодня занимаются крупнейшие игроки IT-индустрии. Уже сейчас есть действующие прототипы, выполняющие специфические алгоритмы быстрее суперкомпьютеров традиционной архитектуры. Аналитики Gartner ожидают появления универсальных и коммерчески доступных квантовых компьютеров к 2030 году. Это несёт риски для информационной безопасности, поскольку с достаточно мощным квантовым компьютером появится возможность взлома многих криптографических алгоритмов. Все онлайн-сервисы – от интернет-магазинов до крупных государственных порталов, а также системы удалённого управления – могут стать уязвимыми. Работая на упреждение, компании «Криптонит» и «QApp» последовательно занимаются разработкой и стандартизацией постквантовых криптографических механизмов, которые останутся актуальными даже после появления квантовых компьютеров.

Источник: github.com, 14.11.2023