КВАНТОВЫЙ ДАЙДЖЕСТ

НКЛ Национальная Квантовая Лаборатория

Сентябрь 2023 г.

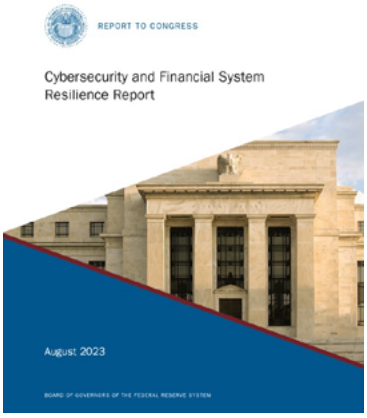
ISO определила международные стандарты для систем с квантовым распределением ключа

Международная организация по стандартизации (ISO) выпустила первый набор стандартов для квантовой криптографии. Документ содержит описание функциональных требований к устройствам квантового распределения ключа (КРК), их сетевым и оптическим компонентам. Также приведены правила реализации протоколов КРК и рекомендации по методологии тестирования криптографических модулей.

Как сообщается, документ основан на последних результатах в области атак на системы КРК и противодействия таким атакам. В соответствии с данным стандартом будут производиться исследования дизайна и качества безопасности продуктов, связанных с распространением квантовых ключей.

Источник: ISO

ФРС США предупреждает об угрозах квантовых вычислений и генеративного ИИ для финансовой системы



В отчете, представленном Федеральной резервной системой Конгрессу США, предупреждается, что квантовые вычисления могут сделать текущие методы шифрования, используемые банками и финансовыми фирмами, устаревшими. Аналитики ФРС также предупреждают о потенциальных угрозах искусственного интеллекта: хотя он и может улучшить средства контроля кибербезопасности, но злоумышленники могут использовать ИИ и для автоматизации атак. В частности, новые генеративные инструменты могут обеспечить более убедительные фишинговые и мошеннические действия против финансовых компаний.

В отчете делается вывод о том, что правительство и промышленность должны тесно сотрудничать, чтобы понять и смягчить эти новые угрозы.

Источник: ФРС США

Федеральные агентства США выпустили план миграции к постквантовой криптографии

Агентство национальной безопасности, Агентство по кибербезопасности и защите инфраструктуры и Национальный институт стандартов и технологий США (NIST) обратились к организациям, обслуживающим объекты критической информационной инфраструктуры, с рекомендацией начать подготовку к миграции на квантово-устойчивые алгоритмы шифрования. Соответствующий документ включает советы по формированию плана перехода, созданию необходимой инфраструктуры, а также требования к разработчикам алгоритмов.

Также стало известно, что NIST выпустил черновой вариант федеральных стандартов для 3 из 4 постквантовых алгоритмов, отобранных в 2022 г. Завершить стандартизацию планируется в 2025 г.

Источник: CISA NIST

США ограничат инвестиции в китайские высокотехнологичные компании

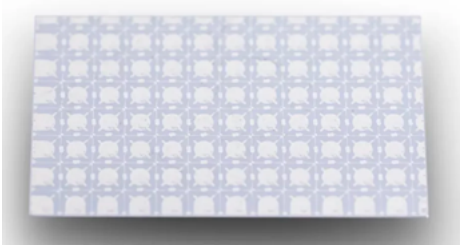
Президент США Джо Байден подписал указ, который ограничивает американские инвестиции в технологическую отрасль Китая. Под запрет попадают инвестиции в сектора разработки полупроводников и микроэлектроники, квантовых технологий и искусственного интеллекта. Конкретные меры для реализации указа выносятся на публичное обсуждение и будут дорабатываться.

Отметим, что ключевые игроки китайской квантовой программы — Национальная лаборатория в Хэфее, компании QuantumCTek и Shanghai QuantumCTek — находятся под американскими санкциями ещё с ноября 2021 г. Все они внесены в черный список с формулировкой «использование или попытка использования американских технологий для военных целей»

Источник: Белый дом

КВАНТОВАЯ ИНДУСТРИЯ

Rigetti выпустила процессор нового поколения с регулируемыми связями между кубитами



В соответствии с ранее озвученными планами компания представила 84-кубитный сверхпроводниковый чип Ankaa-1, который ляжет в основу будущей модульной архитектуры. Основным нововведением стало наличие настраиваемых связей, которые позволяют связывать кубит с ближайшими соседями на время выполнения операций или же изолировать его для предотвращения нежелательного взаимодействия. Скорость выполнения операций в новом чипе увеличена в 3 раза по сравнению с предыдущим поколением.

На основе чипа Ankaa в дальнейшем будут созданы модульные процессоры с 336 (в 2024–2025 гг.), 1000 (в 2025 г.) и 4000 (в 2027 г.) кубитами. Компания также опубликовала препринт статьи, в которой обсуждаются способы соединения кубитов, расположенных на разных процессорных модулях.

Источник: The Quantum Insider Arxiv

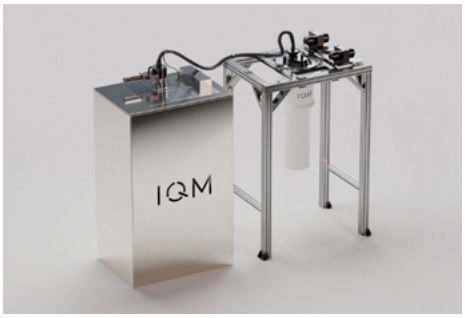
В Национальной лаборатории Sandia создана ионная ловушка на 200 кубитов

В лаборатории Sandia ion trap foundry, которая вот уже 20 лет занимается разработкой и производством ионных ловушек, создана новая 5-зонная ловушка «Enchilada Trap». Число одновременно захваченных ионов в ней увеличено до 200, кроме того, учёным удалось решить проблему отвода тепла, что позволило снизить шумы и увеличить время удержания ионов.

В конструкции использована сложная сеть электродов, позволяющая легко изменять конфигурацию массива ионов для проведения вычислений. Разработчики планируют использовать такой подход и в более крупных версиях ловушки в будущем.

Источник: Sandia National Lab

IQM открыл продажи 5-кубитного учебного квантового компьютера



Финский стартап предлагает полностью готовый к использованию 5-кубитный квантовый компьютер на сверхпроводниках «IQM Spark». Стоимость устройства составляет около 1 млн евро. Он предназначен для учебно-тренировочных целей, а основными покупателями должны стать университеты и исследовательские лаборатории.

IQM также разработала бесплатную учебную онлайн платформу «IQM Academy», предназначенную для углублённого знакомства с квантовыми технологиями.

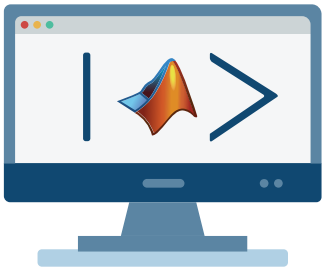
Источник: IQM

QuantrolOx и Qblox разработали интегрированный стек управления для сверхпроводниковых процессоров

Финский и нидерландский стартапы представили аппаратно-программный продукт Quantum Edge, который позволяет в полностью автоматическом режиме калибровать, настраивать и оптимизировать индивидуальные параметры каждого из кубитов в крупномасштабных вычислительных системах. Интегрированное решение подходит для всех типов сверхпроводниковых процессоров, а модульный дизайн позволяет пользователю настроить конфигурацию контроллера под конкретную задачу.

Источник: QuantrolOx

В математическом пакете MATLAB появилась поддержка квантовых вычислений



Библиотека квантовых вычислений для популярного математического пакета MATLAB, выпускаемого компанией MathWorks, позволяет разрабатывать с использованием встроенного набора квантовых схем различные программы оптимизации, сценарного моделирования и машинного обучения. Имеется возможность смоделировать выполнение готового алгоритма на классических компьютерах, а потом запустить его на различных квантовых компьютерах, используя облачные сервисы. Для этого в программе предусмотрена поддержка IBM Qiskit и Amazon Braket.

Источник: MathWorks

IonQ и BearingPoint открывают консалтинговую службу для европейских клиентов

BearingPoint — технологическая консалтинговая компания с офисами в 24 странах и более чем 1000 клиентами, совместно с компанией-разработчиком квантовых компьютеров IonQ будут консультировать европейских индустриальных клиентов по вопросам, связанным с квантовыми технологиями. Партнёры помогут определить перспективные направления внедрения квантовых технологий, оценить их влияние на бизнес и сформировать квантовую стратегию компании.

Подобного рода услуги становятся уже достаточно распространёнными на рынке консалтинга. Среди известных компаний, сформировавших «квантовые подразделения», в частности, EY и KPMG.

Источник: The Quantum Insider

Постквантовая криптография в браузере Chrome доступна уже сейчас

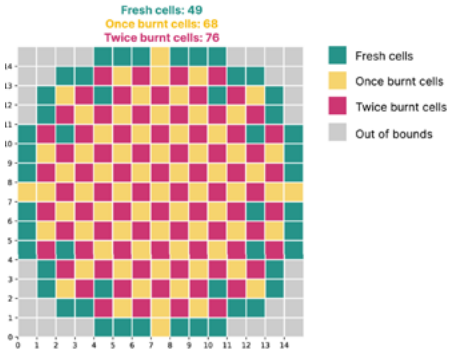
Компания Google объявила о том, что в следующем выпуске интернет-браузера Chrome версии 116 появится поддержка Kyber-768 — одного из алгоритмов постквантовой криптографии, ставшего победителем конкурса NIST.

При установлении соединения функция TLS (Transport Layer Security) в браузере будет проверять, поддерживается ли Kyber-768 компьютером на другой стороне. Если поддерживается, то браузер будет использовать гибридный механизм инкапсуляции ключей, который включает в себя как Kyber-768, так и X25519 — алгоритм эллиптической кривой. Таким образом, организована двухфакторная защита как против классических, так и против квантовых атак.

Источник: Chromium Blog

ИССЛЕДОВАНИЯ И РАЗРАБОТКИ

Российские учёные решили задачу перезагрузки топлива в ядерном реакторе

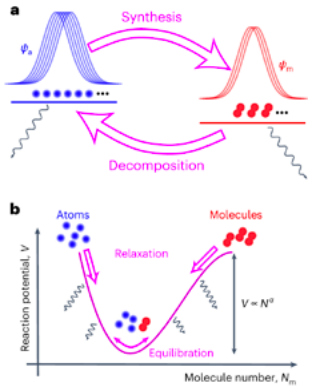


Учёные Российского квантового центра изучили пригодность и эффективность квантовых алгоритмов для расчёта циклов перезакладки активной зоны ядерного реактора. Подобные задачи дискретной оптимизации являются одними из самых сложных с точки зрения классических вычислителей и наиболее перспективными с точки зрения квантовых.

Вычисления выполнялись на классической системе, эмуляторе квантового компьютера и на 5000-кубитном адиабатическом вычислителе D-Wave. В результате учёным удалось определить 4 оптимальных цикла перезагрузки реактора. При этом тесты показали преимущество квантово-вдохновлённого метода, в то время как чисто квантовый расчёт пока возможен лишь для простейшего случая из-за несовершенства существующих квантовых компьютеров.

Источник: Arxiv

Впервые удалось наблюдать химические реакции с коллективной связью между бозе-конденсированными атомами

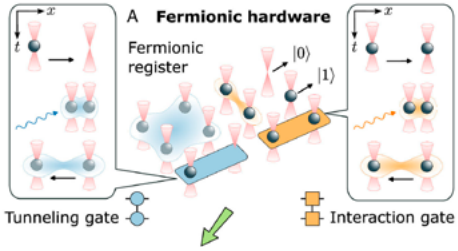


Квантовая механика предсказывает, что атомы в бозе-конденсате выполняют действия коллективно, в том числе они могут вступать в химические реакции как единое целое. Атомы в этом случае могут генерировать реакции и химические продукты, которые в обычных условиях были бы невозможны или крайне маловероятны.

Ученые из Университета Чикаго впервые наблюдали это явление «квантовой суперхимии» в эксперименте. Используя атомы цезия в состоянии квантового вырождения, они заметили, что химическая реакция с образованием молекулы Cs2 в этом случае протекает намного быстрее, а образовавшиеся молекулы имеют одно и то же молекулярное состояние.

Источник: Nature Physics

Программируемый квантовый симулятор для моделирования фермионных систем

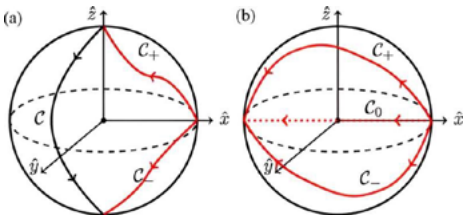


Команда под руководством Петера Цоллера из университета Инсбрука представила программируемый нейтрально-атомный симулятор, способный эффективно моделировать фермионные модели с помощью фермионных затворов. В отличие от традиционных квантовых компьютеров на основе кубитов, этот симулятор не требует дополнительных ресурсов для моделирования свойств систем, подчиняющихся принципу исключения Паули.

Новый симулятор идеально подходят для моделирования таких известных фермионных систем, как, например, сверхпроводники или кварк-глюонная плазма.

Источник: PNAS

В Лос-Аламосе предложили концепцию квантового компьютера без вентилей

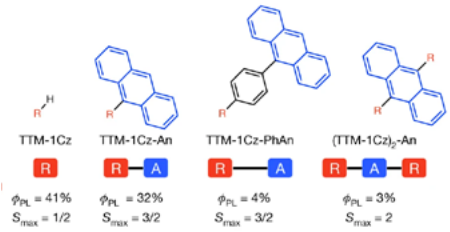


Команда теоретиков под руководством Николая Синицина в Лос Аламосе предложила идею «центрального квантового спина», который действует как стержень, взаимодействуя со всеми окружающими его кубитами. Подвергнув систему воздействию магнитного поля, можно манипулировать спинами этих электронов. Воздействуя на эволюцию спинов, исследователи могут направлять систему на решение задачи более простым и прямым способом, чем традиционные методы.

Одним из преимуществ подхода является также его совместимость с алгоритмом Гровера, разработанным для поиска в неструктурированных базах данных. Упростив и ускорив наиболее сложную часть алгоритма, данный метод может произвести революцию в обработке и поиске информации.

Источник: Physical Review A

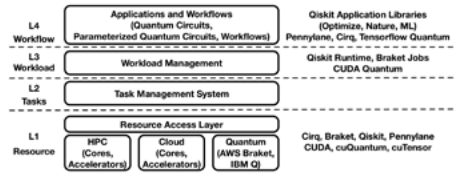
Обратимый спин-оптический интерфейс: молекулярный кубит при комнатной температуре?



Ученые из Кембриджа разработали новый класс органических полупроводников, в которых поглощение фотона действует подобно переключателю, контролируя поведение спинов электронов. “Блочный” метод сборки молекулы позволил прикрепить светоизлучающий радикал к молекуле антрацена. После того, как радикал поглощает фотон, возбуждение распространяется на соседний антрацен. Когда на другой стороне молекул антрацена прикрепляется еще одна радикальная группа, ее электрон также связывается, приводя к вращению четырех электронов в одном направлении. Достоинством сформированного таким образом молекулярного кубита является возможность работы при комнатных температурах.

Источник: Nature

Концепция архитектуры ПО для квантово-классических суперкомпьютеров

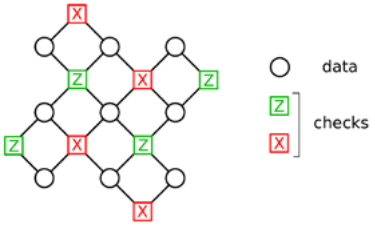


Одним из наиболее вероятных сценариев в ближайшие годы является совместное использование квантовых и классических вычислительных систем. В данной модели квантовые сопроцессоры (QPU) могут использоваться в связке с классическими суперкомпьютерами для ускорения ряда вычислительных операций, таких как оптимизация, решение дифференциальных уравнений, преобразование Фурье и др.

Учёные из США, Германии и Нидерландов разработали в этой связи концепцию оптимальной архитектуры связующего ПО (middleware) для наиболее эффективного взаимодействия классической и квантовой подсистем.

Источник: Arxiv

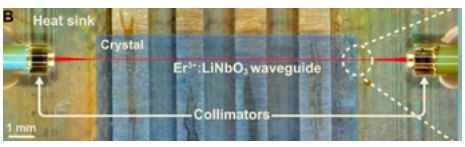
IBM разрабатывает новый протокол коррекции ошибок с использованием небольшого числа кубитов



Протокол основан на семействах кодов Low-Density Parity-Check (LDPC). Этот подход имеет два преимущества перед аналогами: он имеет низкий порог ошибок, то есть он может исправлять больше ошибок, и он требует меньше дополнительных кубитов и операций для работы. Исследователи показали, что их код может достичь практически важного порога ошибок 0.8% — этот результат сравним с поверхностным кодом, который уже почти 20 лет является ведущим методом коррекции ошибок в квантовых вычислениях. С использованием нового подхода для создания 12 логических кубитов потребуется 288 физических кубитов, в то время как при использовании поверхностных кодов их необходимо не менее 4000.

Источник: Arxiv

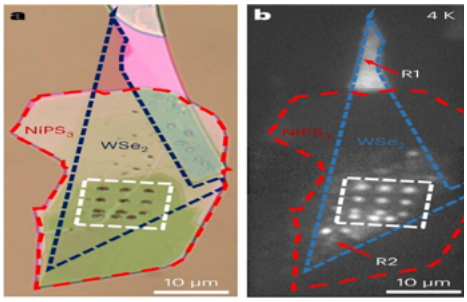
Мультимодовая фотонная квантовая память для телекоммуникационных линий



Новый тип квантовой памяти, разработанный в Университета Чэнду в Китае, работает в телекоммуникационном диапазоне длин волн и предназначен для использования в квантовых повторителях для протяженных сетей квантовой связи. Ключевой элемент системы — это волновод из кристалла Er^{3+}:$LiNbO_3$, соединенный с одномодовым волоконным пигтейлом для подключения к стандартным телекоммуникационным сетям. Устройство интегрировано с источником одиночных фотонов и позволяет хранить несколько квантовых состояний на одном чипе. Квантовая память имеет достаточно высокую эффективность и длительное время хранения квантового состояния.

Источник: Science Advances

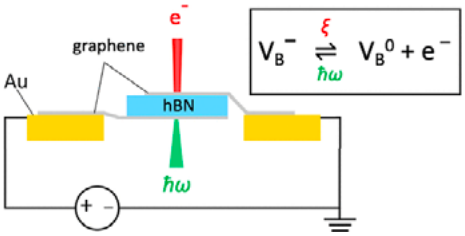
Компактный источник одиночных фотонов с круговой поляризацией



Исследователи из Национальной лаборатории в Лос Аламосе разработали компактный источник одиночных циркулярно поляризованных фотонов для систем квантовой информатики. Вдавливая зонд атомно-силового микроскопа в сложенные вместе листы двух атомарно тонких материалов $WSe_2/NiPS_3$, им удалось создать массив углублений диаметром 250 нм и глубиной ~ 1 нм, каждое из которых являлось локализованным квантовым эмиттером. За счёт ближнего взаимодействия с магнитным слоем каждый из излучённых фотонов получал круговую поляризацию — прежде такой эффект был возможен только в присутствии очень сильного внешнего поля. Полученное однофотонное излучение имело чистоту более 95% и степень поляризации 89%. Для работы устройства необходимо криогенное охлаждение.

Источник: Nature Materials

hBN предложен в качестве альтернативы алмазу для твердотельных квантовых сенсоров



Гексагональный нитрид бора (hBN) ранее не использовался в качестве квантового датчика. Однако недавно в этом материале был обнаружен ряд новых дефектов, которые могут позволить ему стать серьезным конкурентом для алмазов с NV-центрами. Наиболее перспективным для использования в качестве кубита оказался дефект вакансии бора. Исследователи из университета Сиднея под руководством Игоря Аароновича разработали метод стабилизации этого дефекта, что позволило сделать его более устойчивым в условиях, типичных для квантовых устройств.

Источник: Nano Letters

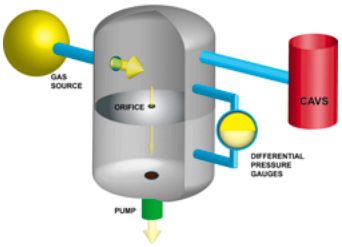
Получение 3D изображений с помощью квантовой визуализации

Немецкие исследователи разработали способ трёхмерной визуализации с использованием «призрачных изображений» (“ghost imaging”). Для получения 3D изображения используются пары запутанных фотонов, один из которых (сигнальный) отражается от исследуемого объекта и детектируется камерой, а второй используется для определения времени взаимодействия сигнального фотона с исследуемым объектом с помощью матрицы лавинных диодов. Это позволяет построить 3D-карту глубины объекта.

Новый способ подходит в том числе для визуализации прозрачных объектов, а также материалов, чувствительных к свету, например, биологических объектов.

Источник: Optica

Испытан новый первичный стандарт измерения сверхнизкого давления газов



Исследователи из NIST испытали квантовый сенсор измерения абсолютного давления газов на основе холодных атомов. За счет лазерного облучения атомы в магнитооптической ловушке испускают свечение, которое фиксируется датчиками и которое снижается, если во введенные атомы врезаются «местные», которые выбивают введенные атомы из ловушки. За счет изменения свечения в ловушке определяется точное давление, близкое к нулю.

Точность предложенного способа измерения давления для инертных газов сравнима с существующим «золотым» стандартом. Новый датчик давления имеет меньшие габариты и более удобен в применении и может использоваться как первичный стандарт, так как не требует калибровки.

Источник: AVS Quantum Science

Эксперты продолжают обсуждать достоинства и проблемы квантово-защищённых сетей

QUANTUM COMMUNICATION

Способ шифрования передаваемой информации с помощью квантового распределения ключей (КРК) имеет своих сторонников и противников. В частности АНБ США и Британский центр по кибербезопасности не рекомендуют госучреждениям использовать КРК в качестве единственного способа защиты данных. Эксперты указывают на ряд уязвимостей технологии, её сложность, дороговизну и риски отказов оборудования.

В новом исследовании специалисты ETH и квантового центра Цюриха пришли к выводу, что эти недостатки обусловлены исключительно «детскими болезнями» из-за раннего этапа развития технологии. Учёные приводят варианты преодоления проблем и дают прогнозы наступления зрелости технологии КРК.

Источник: Arxiv

БЛИЖАЙШИЕ МЕРОПРИЯТИЯ

Quantum Business Europe

QUANTUMBUSINESS EUROPE

3-й европейский саммит, посвященный коммерциализации квантовых технологий. Среди более чем 1500 участников — госслужащие, представители крупного бизнеса, предприниматели и учёные.

В рамках саммита также пройдёт выставка.

Даты: **25–26 сентября**
Страна: **Франция (Париж)**
Формат: **очный**
Web: https://www.quantumbusinesseurope.com/

IEEE Quantum Week

IEEE QUANTUM WEEK

Крупная ежегодная конференция по квантовым вычислениям, организуемая некоммерческой инженерной ассоциацией США, объединит учёных инженеров и предпринимателей из различных стран мира.

Возможно дистанционное участие.

Даты: **17–22 сентября**
Страна: **США (Вашингтон)**
Формат: **очный/онлайн**
Web: https://qce.quantum.ieee.org/2023/

Quantum World Congress

Quantum World Congress - одна из больших международных конференций по квантовым технологиям. В рамках конгресса пройдут научные семинары, ежегодная встреча представителей индустрии и питч-сессия для квантовых стартапов.

Даты: **26–28 сентября**
Страна: **США (Тайсон)**
Формат: **очный**
Web: https://www.quantumworldcongress.com

Quantum Latino 2023

Первая в Латинской Америке конференция по квантовым технологиям объединит учёных, работающих в регионе, и приглашённых спикеров.

Возможно дистанционное участие.

Даты: **10–12 октября**
Страна: **Перу (Лима)**
Формат: **очный/онлайн**
Web: https://quantum-latino.com/

European Quantum Technologies Conference (EQTC)

European Quantum Technologies Conference 2023
Hosted by Quantum Valley Lower Saxony

Ежегодная конференция в рамках Европейской квантовой инициативы.

Даты: **16–20 октября**
Страна: **Германия (Ганновер)**
Формат: **очный**
Web: https://eqtc2023.qvls.de/

Quantum Techniques in Machine Learning

Ежегодная международная конференция, посвященная междисциплинарной области квантовых технологий и машинного обучения.

Даты: **19–24 ноября**
Страна: **Швейцария (CERN)**
Формат: **очный**
Web: https://qtml-2023.web.cern.ch