DOI: 10.22184/1993-7296.FRos.2019.13.6.574.583

Квантовые технологии: от научных открытий к новым приложениям

А. К. Федоров
Российский квантовый центр (ООО «МКЦТ»), rqc.ru, Москва, Сколково, Россия

Квантовые технологии – одно из наиболее динамически развивающихся направлений. Квантовые технологии открывают новые возможности для целого ряда областей. За счет своих уникальных свойств квантовые системы могут стать основой нового поколения высокопроизводительных вычислительных устройств (квантовых компьютеров), методов защиты информации (с использованием квантовой криптографии), а также высокоточных измерительных устройств (квантовых сенсоров и квантовых метрологических устройств). Обзор посвящен прогрессу, наблюдаемому в основных сферах современных квантовых технологий: квантовой обработки информации, квантовой криптографии, а также квантовой метрологии и квантовой сенсорики.

Ключевые слова: квантовая обработка информации, квантовая криптография, квантовая метрология, квантовая сенсорика.

Статья получена: 08.08.2019. Принята к публикации: 30.09.2019.

Quantum Technologies: from Scientific Discoveries to New Applications

A. K. Fedorov
Russian Quantum Center (MQCT LLC), Moscow, Skolkovo, Russia

Quantum technology is an actively developing field. Quantum technologies open up new opportunities. Thanks to their unique properties, quantum systems can become a basis of a new generation of high-performance computing devices (quantum computers), information protection methods (using quantum cryptography), as well as high-precision measuring devices (quantum sensors and quantum metrological devices). The present review is devoted to the progress observed in the main areas of modern quantum technologies: quantum information processing, quantum cryptography, as well as quantum metrology and quantum sensors.

Keywords: quantum information processing, quantum cryptography, quantum metrology, quantum sensorics.

Received: 08.08.2019. Accepted: 30.09.2019.

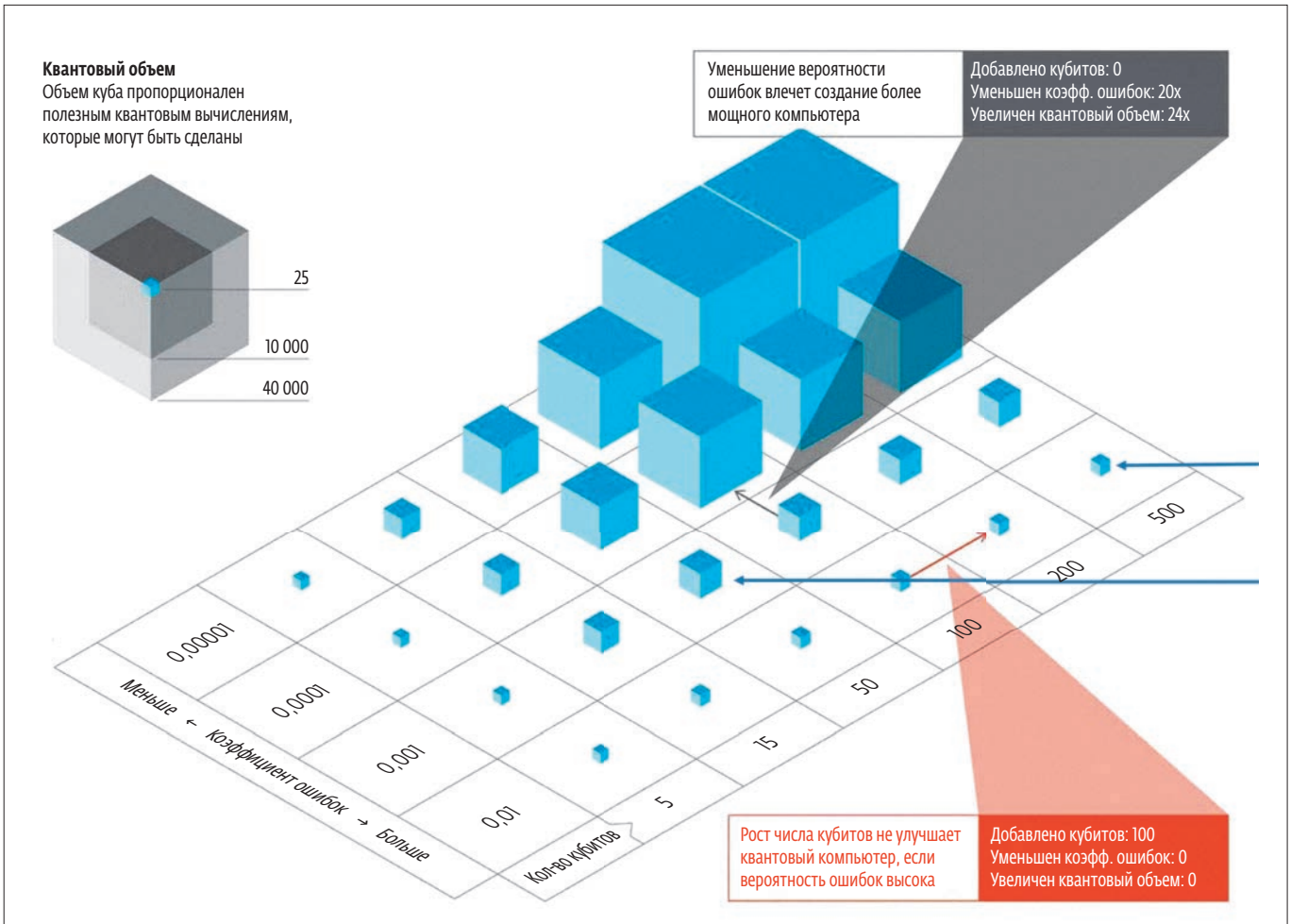
Посвящается памяти выдающегося ученого профессора Михаила Леонидовича Городецкого

ВВЕДЕНИЕ

Последние десятилетия наблюдается стремительный прогресс в области информационных технологий. С каждым годом вычислительные устройства становятся как более компактными, так и более производительными. Чтобы проиллюстрировать этот процесс, достаточно вспомнить цитату из журнала *Scientific American* [1]: «Если бы авиапромышленность в последние 25 лет развивалась столь же стремительно, как промышленность средств вычислительной техники, то сейчас самолет Boeing 767 стоил бы 500 долларов и совершал облет земного шара за 20 минут, затрачивая при этом 18,9 л топлива. Приведенные цифры весьма точно отражают снижение стоимости, рост быстродействия и повышение экономичности компьютеров».

Что же движет столь стремительным прогрессом вычислительных технологий? Основным стимулирующим фактором развития компьютеров считается совершенствование технологий, связанных с миниатюризацией элементной базы. Иными словами, мощность компьютеров растет, так как в каждом новом поколении компьютеров на чипе той же площади можно разместить примерно вдвое больше транзисторов. Это эмпирическое правило, известное сегодня как закон Мура [2, 3], с достаточной степенью точности описывало развитие информационных технологий, начиная с 1960-х годов: количество транзисторов, размещаемых на кристалле интегральной схемы, удваивается каждые 18 месяцев.

На сегодняшний день наиболее компактные транзисторы имеют топологические элементы



Концепция «квантового объема» [9]

размером порядка 1 нм [4]. Чтобы поддерживать дальнейший рост производительности компьютеров, к 2020 году необходимо будет создавать транзисторы атомных размеров. Стоит отметить, что рост других параметров, которые сопутствуют развитию вычислительных технологий, таких как тактовая частота процессоров, уже завершился [5]. Таким образом, на этот раз развитие компьютеров сталкивается с новой физической парадигмой: не с привычной классической физикой, а с квантовой механикой.

Строго говоря, появление таких технологий, как транзисторы и лазеры также явилось результатом исследований в области квантовой физики. Однако в случае рассмотрения принципов функционирования лазера или транзистора речь идет о коллективных квантовых явлениях, проявляющихся на уровне коллектива большого числа квантовых объектов (атомов, фотонов или электронов). Задача же управления индивидуальными квантовыми объектами, такими как одиночные фотоны, атомы, ионы оказывается гораздо сложнее: она находится на переднем крае развития науки. Для ее решения в случае рассмотрения сложных квантовых систем на уровне индивидуальных частиц нужно разработать эффективные методы создания, контроля и измерения. Отметим, что в 2012 году Нобелевская премия по физике была вручена С. Арошу и Д. Вайленду с формулировкой: «За создание прорывных технологий манипулирования квантовыми системами, которые сделали возможными измерение отдельных квантовых систем и управление ими».

Квантовые технологии, т.е. технологии, основанные на управлении индивидуальными квантовыми свойствам частиц, активно развиваются по всему миру. Они разрабатываются в ведущих университетах, исследовательских центрах и компаниях. В Российской Федерации квантовые технологии входят в перечень основных сквозных цифровых технологий. В настоящей статье мы рассматриваем прогресс основных сфер развития современных квантовых технологий: квантовой обработки информации, квантовой криптографии, а также квантовой метрологии и квантовой сенсорики.

ПРОГРАММЫ РАЗВИТИЯ КВАНТОВЫХ ТЕХНОЛОГИЙ В МИРЕ

В технологически развитых странах (в США, Китае, Канаде, ЕС, Великобритании, Японии, Австралиии т.д.) исследования и разработки в области квантовой физики находятся под бдительным вниманием со стороны государства: для их развития создаются специализированные центры компетенций, а финансирование обеспечивается специальными целевыми программами. На сегодняшний день главным потребителем квантовых технологий является государство. Во многом это объясняется стратегической важностью квантовых технологий для обеспечения защищенности интересов государства, например, для обеспечения безопасности в информационной сфере. В 2016 году в Евросоюзе создана специальная программа «Quantum Flagship» (после завершения предыдущей программы 2013–2016 гг.) по развитию квантовых технологий с бюджетом около 3 млрд евро [6]. В Китае запущена программа в размере около 12 млрд долларов [7]. В 2018 году Конгрессом США утверждена долгосрочная программа развития квантовых технологий «National Quantum Initiative» [8]. Аналогичные программы рассматриваются в Великобритании, Японии, Канаде, Австралии и ряде других стран.

Последнее время, наряду с государственными программами поддержки, интерес к квантовым технологиям начал проявлять также и высокотехнологичный бизнес. Исследовательские центры в области квантовых технологий создаются при поддержке таких компании, как Google (США), IBM (США), Microsoft (США), Intel (США), и Alibaba (Китай). Общие вложения в сферу квантовых технологий со стороны частных компаний и фондов оцениваются в 1,5 млрд долларов, при этом порядка 150 млн долларов из венчурных фондов, поддерживающих малые исследовательские группы и стартап-компании, выросшие из академической среды, такие как, например, IonQ или Rigetti Computing.

Существенная особенность квантовых технологий – необходимость сочетания результатов фундаментальных и прикладных исследований. Российская фундаментальная наука традиционно сильна. Кроме того, в области квантовой физики российская диаспора является одной из сильнейших в мире. Тем не менее, трансфер результатов из науки в технологии в России пока не является полностью налаженным процессом – это один из барьеров, который требуется преодолеть для развития квантовых технологий в России. В Российской Федерации квантовые технологии входят в перечень основных сквозных цифровых технологий.

Сейчас проходит утверждение дорожной карты развития квантовых технологий до 2024 года в рамках национальной программы «Цифровая

экономика Российской Федерации» с привлечением более чем 120 экспертов из ведущих исследовательских центров в области квантовых технологий. Госкорпорации Росатом, РДЖ, Ростех и Правительство РФ подписали соглашения о намерениях по направлениям «Квантовые вычисления», «Квантовые коммуникации» и «Квантовые сенсоры» соотвественно.

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ: КВАНТОВЫЕ КОМПЬЮТЕРЫ И КВАНТОВЫЕ СИМУЛЯТОРЫ

Законы квантовой физики сильно отличаются от законов классической физики. Например, в квантовой физике согласно *принципу суперпозиции* система может находиться одновременно в двух возможных состояниях, даже если они являются альтернативными. Переводя явление квантовой суперпозиции на язык двоичной логики – основу работы современных информационных технологий – квантовые биты (кубиты) могут быть одновременно и в состоянии «0», и в состоянии «1». Кроме того, квантовые системы могут демонстрировать сильную взаимосвязь (корреляцию) параметров, даже находясь на большом расстоянии, в силу феномена *квантовой запутанности*. Это явление означает, что для квантовых систем, приготовленных специальным образом, есть взаимосвязь между параметрами, которая проявляется, даже если эти объекты разнесены в пространстве.

Исследования показывают, что компьютеры, построенные на принципах квантовых технологий – *квантовые компьютеры*, могут быть многократно эффективнее классических компьютеров в целом ряде задач, связанных с информационной безопасностью, задачами оптимизации, моделированием материалов и химических веществ, а также обработкой больших данных и машинным обучением.

Сферу квантовых вычислений принято разделять на два больших направления: квантовые компьютеры и квантовые симуляторы. Квантовые компьютеры являются аналогами классических процессоров общего назначения в том смысле, что могут решать любую алгоритмическую задачу, при этом их функционирование существенно базируется на использовании квантовых эффектов.

Разработка квантового компьютера – чрезвычайно сложная научно-техническая задача. Сложной ее делает необходимость, с одной стороны, увеличивать количество кубит и, с другой стороны, сохранять возможность индивидуального контроля над ними. Именно одновременный рост и количества кубит, и «качества» работы с ними может дать выигрыш в «квантовом объеме» – мере вычислительной мощности, разработанной компанией IBM для оценки потенциала квантовых компьютеров [9]. Под «качеством» в данном случае подразумевается количество ошибок в результате операции над кубитами. Ошибки в квантовых вычислениях происходят из-за деструктивного воздействия на квантовую систему со стороны окружения. Возможным решением по нивелированию этого воздействия могут быть квантовые коды коррекции ошибок – аналог кодов исправления ошибок для классических компьютеров, которые адаптированы под работу с кубитами. Однако задача разработки практически применимых квантовых кодов коррекции ошибок оказывается чрезвычайно сложной.

Для решения задачи квантовые компьютеры могут использовать несколько подходов. Во-первых, это цифровая (гейтовая) модель вычислений. Она наиболее близка, с точки зрения возможных аналогий, к классической модели: существует набор регистров с кубитами, и над ними производятся квантовые аналоги логических операций. Набор квантовых логических операций формирует алгоритм. Для цифровой модели практические любые шумы играют деструктивную роль.

Во-вторых, существует адиабатическая модель квантовых вычислений. В ней исходная задача «кодируется» в параметры гамильтониана некоторой физической системы. Далее параметры системы (гамильтониан) достаточно медленно меняются, принимая значения, соответствующие решаемой вычислительной задаче. Изменившееся (эволюционировавшее) состояние системы считывается в качестве ответа. Адиабатическая модель обладает устойчивостью к шумам, однако свойства такой архитектуры пока недостаточно хорошо поняты. Существенной проблемой является необходимость отобразить исходную задачу на задачу нахождения минимума гамильтониана некоторой физической системы. К решению такой задачи на данный момент нет общего подхода.

Текущий статус развития квантовых компьютеров называют этапом «шумных» квантовых компьютеров промежуточного масштаба (Noisy intermediate-scale quantum, NISQ). В них реализовано 50–100 кубит, они уже не могут быть напрямую промоделированы с помощью классических суперкомпьютеров, но в них не применяются квантовые коды коррекции ошибок.

Канадская компания D-Wave Systems в настоящий момент предлагает купить 2048-кубитное

квантовое вычислительное устройство. Система позволяет решать задачи оптимизации, сводящиеся к поиску основного состояния некоторого гамильтониана по методу квантового отжига – нахождения глобального минимума некоей целевой функции посредством квантовых флуктуаций (туннелирования через потенциальные барьеры). В части оценки результатов D-Wave Systems в научном сообществе существует активная дискуссия о роли квантовых флуктуаций в указанной системе [10, 11].

Другое направление развития технологии квантовых вычислений – разработка квантовых симуляторов. Аналоговые квантовые симуляторы – это хорошо контролируемые системы, которые могут качественно воспроизводить свойства других систем. Например, атомный ансамбль при достаточно низкой температуре, помещенный в оптическую решетку (стоячую волну света), может воспроизводить поведение электронов в кристаллической решетке твердого тела. Таким образом, при помощи ультрахолодных атомов становится возможным моделирование различных явлений физики твердого тела, например, сверхпроводимости и магнетизма.

Квантовые симуляторы предназначены для решения узкоспециализированных квантовых задач, связанных, например, с моделированием сложных систем с большим числом частиц. Считается, что квантовые компьютеры могут быть полезны для задачи разработки новых материалов, например, материалов с высокотемпературной сверхпроводимостью. В последние годы развивается направление создания программируемых квантовых симуляторов. Программируемым квантовым симулятором называется система, в которой некоторые параметры могут быть изменены в процессе функционирования. Это расширяет класс задач, которые возможно решить с помощью таких систем.

Большая проблема для классических суперкомпьютеров – моделирование физических процессов в материалах, а также в ходе химических реакций. Для классических компьютеров сложность задачи моделирования квантовой системы растет экспоненциально быстро с увеличением размерности системы. Для квантовых компьютеров этот рост проявляется гораздо медленнее, так что квантовые системы можно моделировать значительно эффективнее.

Мощности существующих на данный момент квантовых компьютеров достаточно, чтобы промоделировать лишь достаточно простые молекулы (см. табл.). Например, в 2010 году была промоделирована молекула водорода, а наиболее сложной промоделированной молекулой является молекула гидрида бериллия – для этого группой ученых из IBM был использован 7-кубитный квантовый процессор. Рост мощности квантовых компьютеров растет, поэтому можно с оптимизмом рассчитывать на более интересные результаты.

Одной из востребованных задач, в которой квантовый компьютер может быть потенциально полезен, является поиск катализаторов для производства востребованных химических веществ. Одним из них является аммиак, который широко используется в качестве удобрений, противомикробных или чистящих агентов. Сейчас в основе производства аммиака лежит процесс Габера-Боша, очень энергозатратный, на него уходит порядка 1–2% всей вырабатываемой в мире энергии.

Одной из интересных особенностей развития квантовых вычислительных систем является тот факт, что на сегодняшний день не определена лидирующая физическая платформа для разработки квантовых компьютеров и квантовых симуляторов. Дело в том, что каждая из систем для квантовых вычислений (сверхпроводящие цепи, нейтральные атомы, ионы в ловушках, фотоны, центры окраски) обладают рядом преимуществ и недостатков. Наиболее мощные квантовые вычислительные устройства, из представленных на сегодняшний день, разработаны на основе разных технологий: 72-кубитный квантовый процессор на основе сверхпроводящих цепей (компания Google, США),

Развитие моделирования химических веществ с помощью квантовых компьютеров

Год	Система	Научная группа
2010	Молекула водорода H_2	A. Aspuru-Guzik, A. G. White
2014	Гидрид гелия HeH^+	A. Aspuru-Guzik
2015	Гидрид гелия HeH^+	A. Aspuru-Guzik, J. Wrachtrup
2016	Молекула водорода H_2	J.M. Martinis (Google)
2017	Гидрид лития	J.M. Gambetta (IBM)
2017	Гидрид бериллия BeH_2	J.M. Gambetta (IBM)

программируемый симулятор из 53 ионов (Университет Мэриленда, США) [12] и программируемый симулятор из 51 атома (Гарвардский университет, США) [13]. Системы из 50 твердотельных кубитов также созданы компаниями Intel (США) и IBM (США).

Особенностью модели работы компании является предоставление к квантовым процессорам открытого облачного доступа в рамках программы IBM Quantum Experience. Это позволяет уже сейчас исследовать возможную реализацию квантовых алгоритмов. Такие исследования проводятся большим количеством научных групп по всему миру, включая российские исследовательские центры [14].

В России следует отметить следующие выполняемые проекты в области технологии квантовых вычислений. Во-первых, разработка системы на основе сверхпроводниковых кубитов консорциумом исполнителей (ФГУП «ВНИИА им. Н.Л.Духова», НИТУ МИСиС, Российский квантовый центр (ООО «МКЦТ»), МФТИ, ИФТТ, МГТУ им. Н.Э.Баумана, НГТУ (Новосибирск)) с поддержкой Фонда перспективных исследований, ГК «Росатом» и Министерства науки и высшего образования РФ. На основе этой технологии реализованы прототипы квантовых компьютеров с 2–10 кубитами [15–18] и квантовые симуляторы с 10–20 кубитами [19]. Точность реализации одно- и двухкубитных операций в реализованных квантовых компьютерах составляет величину, близкую к 85–95%. Такие вычислительные устройства способны демонстрировать простейшие квантовые алгоритмы, например, для задач моделирование спиновых цепочек и простейших молекул.

Также группой исполнителей (ЦКТ МГУ им. М.В.Ломоносова, ИФП А.В.Ржанова СО РАН, ФГУП «ВНИИА им. Н.Л.Духова», МГТУ им. Н.Э.Баумана и ФТИ им. А.Ф.Иоффе РАН.) разрабатываются системы квантовых вычислений на основе двух систем: нейтральных атомов и фотонных чипов, а также развиваются вспомогательные технологии. В случае квантовых вычислений на основе нейтральных атомов используется существенный экспериментальный задел группы в ИФП А.В.Ржанова СО РАН [20–22] и группы в ЦКТ МГУ им. М.В.Ломоносова по загрузке атомов в оптические потенциалы [23].

Также работа ведется по направлению создания фотонных чипов для квантовых вычислений [24]. Стоит отметить, что в области элементной базы для фотоники в РФ существует ряд существенных научных достижений, который включает в себя разработку источников одиночных фотонов [25, 26], а также сверхпроводниковых детекторов одиночных фотонов [27–29].

В ФИАН им. П.Н.Лебедева (совместно с ИЛФ СО РАН) ведется работа в направлении квантовых вычислений и использованием ионов, в частности, экспериментально продемонстрирован захват, удержание и лазерное охлаждение одиночных ионов Yb (совместная работа ФИАН им. П.Н.Лебедева и ИЛФ СО РАН) в трехмерной ловушке Пауля и цепочек ионов Yb и Mg в линейной ловушке Пауля [30]. Кроме того, ведутся работы в области исследований физики ультрахолодных атомных газов, например, атомов тулия в Российском квантовом центре (ООО «МКЦТ») и ФИАН им. П.Н.Лебедева [31], а также лития [32, 33] в Институте прикладной физики РАН (Нижний Новгород) и Объединенном институте высоких температур РАН.

В России ведутся также теоретические исследования в различных направлениях, например, разработка моделей квантовых вычислений с использованием многоуровневых квантовых систем 34–37], исследование вариационных квантовых алгоритмов [38], а также исследование различных задач сферы квантового машинного обучения [39–41]. Одним из перспективных направлений является исследование систем для топологически-защищенной обработки квантовой информации, которые устойчивы к ошибкам. Исследованы некоторые модели таких систем на основе ультрахолодных атомов [42] и молекул [43].

КВАНТОВАЯ КРИПТОГРАФИЯ

Одной из практических задач, в решении которой использование квантового компьютера может дать существенный выигрыш, – это задача поиска скрытых подгрупп для конечных абелевых групп. Возможность решать данную задачу, в частности, позволяет эффективно решать задачи факторизации и дискретного логарифмирования. С помощью квантового алгоритма Шора [44] решение таких задач возможно за полиномиальное время, тогда как лучший классический алгоритм для решения этой задачи требует колоссального времени (решение возможно за субэкспоненциальное время).

На сложности решения таких задач, как факторизация больших чисел и дискретное логарифмирование основывается безопасность распространенных алгоритмов криптографии с открытым ключом (также называемых асимметричными криптографическими алгоритмами). Работа

такого класса алгоритмов строится на том, что легитимным сторонам коммуникаций для получения общего ключа – секретной информации, которая позволяет им шифровать данные и таким образом их защищать – требуется выполнить определенный, быстро выполнимый на любом классическом процессоре, алгоритм (например, перемножить два простых числа), тогда как злоумышленнику для взлома требуется решить обратную задачу (соответственно, решить задачу факторизации), для которой эффективный алгоритм отсутствует.

Конкретным примером может служить криптографический алгоритм RSA. Например, взлом RSA-ключа, состоящего из 1024 бит, займет миллионы лет непрерывных вычислений на классических компьютерах, тогда как на квантовом компьютере эта задача будет решена за 10 часов (если предположить, что каждая квантовая операция выполняется 10 нс и что в распоряжении имеется компьютер из достаточного количества логических кубит). Таким образом, квантовый компьютер представляет собой угрозу для большинства алгоритмов распределения ключей и цифровых подписей.

Квантовый компьютер оказывает также влияние на криптографическую стойкость симметричных криптографических алгоритмов, таких как AES и ГОСТ, однако в существенно меньшей степени. Квантовый алгоритм Гровера, предназначенный для поиска по неупорядоченной базе данных, позволяет существенно снизить сложность задачи полного перебора (brute-force attack). Защитой от этого может быть увеличение длины и частоты смены ключей в симметричных криптографических алгоритмах.

Одним из возможных решений задачи обеспечения защищенной коммуникации в эпоху квантовых компьютеров является использование технологии квантовой криптографии или, более точно, квантового распределения ключей. Используя в качестве переносчиков информации квантовые объекты (на эту роль лучше всего подходят фотоны – кванты света), устройства квантового распределения ключей позволяют двум сторонам генерировать на расстоянии случайные двоичные последовательности, которые называются квантовыми ключами. Особенность этих двоичных последовательностей состоит в том (при соблюдении определенных условий), что, во-первых, они являются случайными на фундаментальном уровне и, во-вторых, в процессе приема/передачи информации можно сделать вывод о том, известна ли данная последовательность третьим лицам.

Основное преимущество технологии квантового распределения ключей – это возможность гарантировать информационно-теоретическую стойкость: какими бы вычислительными ресурсами ни обладал злоумышленник, квантовая криптография все равно надежна.

Однако системы квантового распределения ключа могут работать с практическими скоростями только на расстояния до 100 километров: квантовую информацию невозможно копировать, но по этой же причине ее нельзя передавать через традиционные повторители. Таким образом, возникает потребность в повторителях, построенных на основе доверенных узлов, или разработать полностью квантовые устройства, работающие, например, на спутниках.

Зарубежные компании, например, ID Quantique (Швейцария), уже продают устройства для квантового распределения ключей. В некоторых городах (например, в Женеве, Вене, Токио, Пекине) созданы городские сети безопасной передачи данных с помощью квантовых устройств безопасной передачи информации. Линия безопасной передачи информации с помощью квантовых устройств использовалась для обеспечения связи во время федеральных выборов в Швейцарии в 2007 году. Широкую известность получило использование квантовых устройств безопасной передачи информации во время чемпионата мира по футболу в 2010 году.

В мировом масштабе на сегодняшний день в направлении разработки квантовых устройств распределения ключей лидирует Китай. В данный момент построена «квантовая» сеть Пекин-Шанхай с протяженностью 2000 км, которая включает 4 локальные городские квантовые сети. К 2020 году планируется увеличить протяженность сети до 11000 км. Квантовая криптография реализуется как с использованием волоконных линий, так и в открытом пространстве. Например, в режиме «Земля – спутник» может быть реализовано глобальное распределение криптографических ключей. Китайскими учеными уже продемонстрирована квантово-защищенная видеоконференцсвязь через спутниковое распределение ключей между Пекином и Веной. Одно из основных применений – защита центров управления электросетями и электростанциями.

В Российской Федерации такими разработками в России занимается Российский квантовый центр [47–49], МГУ им. М.В. Ломоносова [50],

а также Университет ИТМО [51]. Вопросами внедрения технологий квантовой защиты данных занимаются Газпромбанк [45] и Сбербанк [46], а также Ростелеком.

Интересный вопрос – угроза квантового компьютера для блокчейн-технологий. С математической точки зрения за работу блокчейнов отвечают две технологии: электронно-цифровая подпись для подтверждения авторства предлагаемой транзакции и механизм достижения консенсуса между пользователями, в большинстве случаев основанный на использовании криптографических хеш-функций. Угроза цифровым подписям действительно актуальна для большинства блокчейнов, поскольку механизмы работы электронно-цифровых подписей базируются на протоколах, уязвимых к атакам с квантовым компьютером. Именно этот факт инициировал работу по созданию механизмов для квантово-защищенных блокчейнов [52, 53]. При этом механизмы достижения консенсуса находятся в относительной безопасности [54]: механизм консенсуса (proof-of-work) в криптовалюте Bitcoin будет в безопасности в ближайшие 10 лет, поскольку существующие квантовые компьютеры уступают в задаче майнинга интегральным схемам специального назначения (ASIC).

Стоит отметить, что помимо исследований непосредственно в области квантовых коммуникаций в РФ существует серьезный научный задел в области квантовой оптики, в частности, генерации неклассических состояний света, квантовой памяти, взаимодействию света с атомными ансамблями и др., однако обзор достижений в этой сфере выходит за рамки настоящей работы.

КВАНТОВАЯ МЕТРОЛОГИЯ И СЕНСОРИКА

Основная сложность создания квантовых компьютеров заключается в том, чтобы изолировать квантовые системы от окружающей среды. Это связано с тем, что даже малейшие изменения окружения могут деструктивно повлиять на квантовую систему, что может привести к декогеренции. С другой стороны, если квантовые системы столь чувствительны, то с их помощью могут быть созданы разнообразные сенсоры.

Квантовые сенсоры, например реализованные в виде кристалла размером порядка нескольких нанометров, могут быть внедрены в клетку живого организма без нарушения ее жизнедеятельности и затем использоваться для измерения микроскопических полей внутри этой клетки [36]. Это открывает совершенно новые горизонты для биологии и медицины. Становится доступным колоссальный объем знаний о жизнедеятельности частей клеток, развитии болезней, механизмов функционирования лекарств. Квантовые датчики помогут разобраться и в структуре связей головного мозга человека, сделав возможным лечение его болезней.

Одними из наиболее перспективных искусственных атомов можно назвать NV-центры окраски в алмазе, которые уже сегодня начинают активно использоваться в качестве чувствительных сенсоров. Такиой дефект возникает, если в кристалле алмаза, состоящего из атомов углерода, удалить два атома в соседних узлах решетки, а на место одного из них поместить азот (NV-центр – «nitrogen-vacancy center» или азото-замещенная вакансия). Алмаз обладает не только уникальной оптической чистотой, но также и уникальной чистотой с точки зрения имеющихся в нем спинов. Сам NV-центр позволяет оптическими методами считывать его внутреннее состояние, тем самым измеряя магнитные или электрические поля. Всего в нескольких кубических миллиметрах алмаза можно разместить достаточно NV-центров, чтобы реализовать чувствительность, сопоставимую с лучшими существующими магнитометрами. Кроме того, NV-центр можно локализовать в пределах нескольких нанометров: на базе этого центра может быть реализован магнитометр сверхвысокого разрешения, способный видеть спины отдельных частиц. Системы на основе NV-центров разрабатываются в России и используются для различных биомедицинских приложений [37, 38].

Квантовые технологии позволяют создать сверхточные датчики позиционирования (с использованием атомных часов), а также новое поколение метрологических устройств. Квантовые или атомные часы представляют собой приборы для измерения времени, в которых в качестве периодического процесса используются собственные колебания, связанные с процессами, происходящими на уровне атомов или молекул. Определение положения космических кораблей, спутников, баллистических ракет, самолетов, подводных лодок, а также передвижение автомобилей в автоматическом режиме по спутниковой связи (GPS, ГЛОНАСС, Galileo) немыслимы без атомных часов. Атомные часы используются также в системах спутниковой и наземной телекоммуникации, в том числе в базовых станциях мобильной связи, международными и национальными бюро стандартов и службами точного времени, которые периодически транслируют временные сигналы по радио. Иссле-

дования и разработки в области создания оптических часов на ультрахолодных атомах и ионах привели к снижению относительной погрешности частоты вплоть до единиц в 18-м знаке после запятой. Использование новых высокоточных методов сличения частот открывает новые возможности при проведении фундаментальных исследований (чувствительные тесты общей теории относительности, поиск дрейфа фундаментальных констант, поиск «темной материи»), а также в современной навигации и гравиметрии. В работе обсуждаются основные методы, использующиеся при создании высокоточных часов (в том числе транспортируемых) на основе ультрахолодных атомов и ионов, и возможность их использования в современных задачах релятивистской гравиметрии.

В 2017 году Министерством образования и науки РФ поддержан проект 14.610.21.0010 «Разработка генератора ультрастабильных опорных сигналов частоты на холодных ионах иттербия для повышения на порядок точности геопозиционирования, космической навигации и формирования новых сегментов массового спроса на рынке приложений глобальной спутниковой навигации», задачей которого является создание компактного (1 м^3) стандарта частоты на одиночном ионе иттербия [39].

В целом в России на данный момент идут работы над некоторыми решениями в области квантовой сенсорики и метрологии, имеющими практические приложения и коммерческие перспективы. К ним можно отнести: оптические атомные/ионные часы [39]; гравиметры/акселерометры на атомах рубидия; гироскопы на ансамблях спинов в твердом теле; локальные сенсоры магнитного поля и температуры на основе азото-замещеной вакансии в алмазе и электрического поля; датчики электромагнитных полей на основе когерентных состояний спинов в магнитоупорядоченных средах; спинтронные сенсоры; магнитоплазмонные сенсоры; твердотельные фотоумножители; спектрограф (электронный нос) с использованием микрорезонаторов; источники и приемники фотонов (например, [40, 41]).

Традиционно сильно развита в РФ область квантовой оптомеханики. Достижения научной школы, созданной В.Б.Брагинским, в этой области были отмечены при вручении Государственной премии в области науки и техники 2019 года по фундаментальной физике за открытие гравитационных волн. Сегодня «Московская группа» продолжает исследования в этой области квантовых измерений для различных приложений, которые, помимо гравитационных волны, включают также атомно-силовые микроскопы и квантово-оптическую память. Сегодня «Московская группа» продолжает исследования в этой области квантовых измерений для различных приложений, которые помимо гравитационных волны включают в себя также атомно-силовые микроскопы и квантово-оптическую память.

ЗАКЛЮЧЕНИЕ

В работе приведен краткий обзор последних достижений в области квантовых технологий, полученных в России и за рубежом.

БЛАГОДАРНОСТИ

Автор выражают благодарность за финансовую поддержку работы. Исследование выполнено при поддержке гранта Президента РФ (проект МК-923.2019.2).

СПИСОК ЛИТЕРАТУРЫ

1. **H.D. Toong, A. Gupta.** Personal computers. *Scientific America*. 1982; 247(6): 86–107.
2. **G.E. Moore.** Cramming more components onto integrated circuits. *Electronics*. 1965; 38(8): 114–117.
3. **M.M. Waldrop.** The chips are down for Moores law. *Nature*. 2016; 2016530: 144.
4. **S.B. Desai, S. R. Madhvapathy, A. B. Sachid, J. P. Llinas, Q. Wang, G. H. Ahn, G. Pitner, M. J. Kim, J. Bokor, C. Hu, H.S.P. Wong, A. Javey.** MoS2 transistors with 1-nanometer gate lengths. *Science*. 2016; 354(6308): 99–102.
5. **P.J. Denning, T. G. Lewis.** Exponential laws of computing growth. *Communications of the ACM*. 2017; 60(1): 54–65.
6. **M. Riedel, M. Kovacs, P. Zoller, J. Mlynek, T. Calarco.** Europe's Quantum Flagship initiative. *Quantum Science and Technology*. 2019; 4(2): 020501.
7. **S. Decker, C. Yasiejko.** *Forget the trade war. China wants to win computing arms race.* **Bloomberg. 9 Apr., 2018.**
8. **M.G. Raymer, C. Monroe.** The US National Quantum Initiative. *Quantum Science and Technology*. 2019; 4(2): 020504.
9. **L.S. Bishop, S. Bravyi, A. Cross, J. M. Gambetta, J. Smolin.** *Quantum volume. Technical report*. IBM T. J. Watson. 2017.
10. **V.S. Denchev, S. Boixo, S. V. Isakov, N. Ding, R. Babbush, V. Smelyanskiy, J. Martinis, H. Neven.** What is the computational value of finite-range tunneling? *Phys. Rev.* 2016; X 6, 031015.
11. **T.F. Rønnow, Z. Wang, J. Job, S. Boixo, S. V. Isakov, D. Wecker, J. M. Martinis, D. A. Lidar, M. Troyer.** Defining and detecting quantum speedup. *Science*. 2014; 345: 420.
12. **J. Zhang, G. Pagano, P. W. Hess, A. Kyprianidis, P. Becker, H. Kaplan, A. V. Gorshkov, Z.-X. Gong, C. Monroe.** Observation of a many-body dynamical phase transition with a 53-qubit quantum simulator. *Nature (London)*. 2017; 551: 601.
13. **H. Bernien, S. Schwartz, A. Keesling, H. Levine, A. Om-ran, H. Pichler, S. Choi, A. S. Zibrov, M. Endres, M. Greiner, V. Vuletic, M. D. Lukin.** Probing many-body dynamics on a 51-atom quantum simulator. *Nature (London)*. 2017; 551: 579.
14. **A.A. Zhukov, E. O. Kiktenko, A. A. Elistratov, W. V. Pogosov, Y. E. Lozovik.** Quantum communication protocols as a benchmark for programmable quantum computers. *Quant. Inf. Proc*. 2019; 18: 31.
15. **I.S. Besedin, G. P. Fedorov, A. Yu. Dmitriev, V. V. Ryazanov.** Superconducting qubits in Russia. *Quantum Electron*. 2018; 48: 880.
16. **A.S. Averkin, A. Karpov, K. Shulga, E. Glushkov, N. Abramov, U. Huebner, E. Ilichev, A. V. Ustinov.** Broadband sample holder for microwave spectroscopy of superconducting qubits. *Rev. Sci. instrum*. 2014; 85: 104702.
17. **K.V. Shulga, P. Yang, G. P. Fedorov, M. V. Fistul, M. Weides, A. V. Ustinov.** Observation of a collective mode of an array of transmon qubits. *JETP Lett*. 2017;

105: 47.
18. **D.S. Shapiro, P. Macha, A. N. Rubtsov, A. V. Ustinov.** Dispersive response of a disordered superconducting quantum metamaterial. *Photonics*. 2015; 2: 449.
19. **K.V. Shulga, E. Ilichev, M. V. Fistul, I. S. Besedin, S. Butz, O. V. Astafiev, U. Hubner, A. V. Ustinov.** Magnetically induced transparency of a quantum metamaterial composed of twin flux qubits. *Nature Commun*. 2018; 9: 150.
20. **I.I. Ryabtsev, I. I. Beterov, D. B. Tretyakov, V. M. Entin, E. A. Yakshina.** Spectroscopy of cold rubidium Rydberg atoms for applications in quantum information. *Phys. Usp*. 2016; 59: 196.
21. **D.B. Tretyakov, I. I. Beterov, E. A. Yakshina, V. M. Entin, I. I. Ryabtsev, P. Cheinet, P. Pillet.** Observation of the borromean three-body Forster resonances for three interacting Rb Rydberg atoms. *Phys. Rev. Lett*. 2017; 119: 173402.
22. **I.I. Beterov, I. N. Ashkarin, E. A. Yakshina, D. B. Tretyakov, V. M. Entin, I. I. Ryabtsev, P. Cheinet, P. Pillet, M. Saffman.** Fast three-qubit Toffoli quantum gate based on three-body Forster resonances in Rydberg atoms. *Phys. Rev. A*. 2018; 98: 042704.
23. **C.H. Nguyen, A. N. Utama, N. Lewty, K. Durak, G. Maslennikov, S. Straupe, M. Steiner, C. Kurtsiefer.** Single atoms coupled to a near-concentric cavity. *Phys. Rev. A*. 2017; 96: 031802.
24. **I.V. Dyakonov, I. A. Pogorelov, I. B. Bobrov, A. A. Kalinkin, S. S. Straupe, S. P. Kulik, P. V. Dyakonov, S. A. Evlashin.** Reconfigurable photonics on a glass chip. *Phys. Rev. Applied*. 2018; 10: 044048.
25. **M.V. Rakhlin, K. G. Belyaev, G. V. Klimko, I. S. Mukhin, D. A. Kirilenko, T. V. Shubina, S. V. Ivanov, A. A. Toropov.** InAs / AlGaAs quantum dots for single-photon emission in a red spectral range. *Sci. Rep*. 2018; 8: 5299.
26. **S.V. Sorokin, I. V. Sedova, M. V. Rakhlin, K. G. Belyaev, M. A. Yagovkina, A. A. Toropov, S. V. Ivanov.** Nanoheterostructures with CdTe / ZnMgSeTe quantum dots for single-photon emitters grown by molecular beam epitaxy. *Tech. Phys. Lett*. 2018; 44: 267.
27. **G.N. Goltsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, and A. Dzardanov.** Picosecond superconducting single-photon optical detector. *Appl. Phys. Lett*. 2001; 79: 705.
28. **W.H.P. Pernice, C. Schuck, O. Minaeva, M. Li, G. N. Goltsman, A. V. Sergienko, H. X. Tang.** High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits. *Nature Commun*. 2012; 3: 1325.
29. **S. Ferrari, O. Kahl, V. Kovalyuk, G. N. Goltsman, A. Korneev, W.H.P. Pernice.** Waveguide-integrated single- and multi-photon detection at telecom wavelengths using superconducting nanowires. *Appl. Phys. Lett*. 2015; 106: 151101.
30. **G.A. Vishnyakova, A. A. Golovizin, E. S. Kalganova, V. N. Sorokin, D. D. Sukachev, D. O. Tregubov, K. Yu. Khabarova, N. N. Kolachevsky.** Ultracold lanthanides: from optical clock to a quantum simulator. *Phys. Usp*. 2016; 59: 168.
31. **V.V. Tsyganok, V. A. Khlebnikov, E. S. Kalganova, E. T. Davletov, D. A. Pershin, I. S. Cojocaru, I. A. Luchnikov, V. S. Bushmakin, V. N. Sorokin, A. V. Akimov.** Polarized cold cloud of thulium atom. *J. Phys. B: At. Mol. Opt. Phys*. 2018; 51: 165001.
32. **T.V. Barmashova, K. A. Martiyanov, V. B. Makhalov, A. V. Turlapov.** Fermi liquid-to-Bose condensate crossover in a two-dimensional ultracold gas experiment. *Phys. Usp*. 2016; 59: 174.
33. **V.A. Sautenkov, S. A. Saakyan, A. A. Bobrov, D. A. Kudrinskiy, E. V. Vilshanskaya, B. B. Zelener.** Optical dipole trap for laser-cooled lithium-7 atoms. *Journal of Russian Laser Research*. 2013; 40: 230.
34. **A.R. Kessel, N. M. Yakovleva.** Implementation schemes in NMR of quantum processors and the Deutsch-Jozsa algorithm by using virtual spin representation. *Phys. Rev. A*. 2002; 66: 062322.
35. **E.O. Kiktenko, A. K. Fedorov, O. V. Manko, V. I. Manko.** Multilevel superconducting circuits as two-qubit systems: Operations, state preparation, and entropic inequalities. *Physical Review A*. 2015; 91: 042312.
36. **E.O. Kiktenko, A. K. Fedorov, A. A. Strakhov, V. I. Manko.** Single qudit realization of the Deutsch algorithm using superconducting many-level quantum circuits. *Physics Letters A*. 2015; 379: 14091413.
37. **A.A. Popov, E. O. Kiktenko, A. K. Fedorov, V. I. Manko.** Information processing using three-qubit and qubit-qutrit encodings of noncomposite quantum systems. *Journal of Russian Laser Research*. 2016; 37: 581.
38. **J. Biamonte.** *Universal variational quantum computation*. arXiv:1903.04500.
39. **J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, S. Lloyd.** Quantum machine learning. *Nature (London)*. 2017; 549: 195.
40. **E.S. Tiunov, A. E. Ulanov, A. I. Lvovsky.** Annealing by simulating the coherent Ising machine. *Opt. Express*. 2019; 27: 10288.
41. **Y.A. Kharkov, V. E. Sotskov, A. A. Karazeev, E. O. Kiktenko, A. K. Fedorov.** *Revealing quantum chaos with machine learning*. arXiv:1902.09216.
42. **A.K. Fedorov, V. I. Yudson, G. V. Shlyapnikov.** P-wave superfluidity of atomic lattice fermions. *Physical Review A*. 2017; 95: 043615.
43. **A.K. Fedorov, S. I. Matveenko, V. I. Yudson, G. V. Shlyapnikov.** Novel p-wave superfluids of fermionic polar molecules. *Scientific Reports*. 2016; 6: 27448.
44. **P.W. Shor.** Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput*. 1997; 26: 1484.
45. **E.O. Kiktenko, N. O. Pozhar, A. V. Duplinskiy, A. A. Kanapin, A. S. Sokolov, S. S. Vorobey, A. V. Miller, V. E. Ustimchik, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, V. L. Kurochkin, Y. V. Kurochkin, A. K. Fedorov.** Demonstration of a quantum key distribution network in urban fibre-optic communication lines. *Quantum Electronics*. 2017; 47: 798–802.
46. **A.V. Duplinskiy, E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, R. P. Ermakov, A. I. Kotov, A. V. Brodskiy, R. R. Yunusov, V. L. Kurochkin, A. K. Fedorov, Y. V. Kurochkin.** Quantum-secured data transmission in urban fibre-optic communication lines. *Journal of Russian Laser Research*. 2018; 39, 113.
47. **E.O. Kiktenko, A. S. Trushechkin, Y. V. Kurochkin, A. K. Fedorov.** Post-processing procedure for industrial quantum key distribution systems. *Journal of Physics: Conference Series*. 2016; 741: 012081.
48. **E.O. Kiktenko, A. S. Trushechkin, C.C.W. Lim, Y. V. Kurochkin, A. K. Fedorov.** Symmetric blind information reconciliation for quantum key distribution. *Physical Review Applied*. 2017; 8: 044017.
49. **A.S. Trushechkin, E. O. Kiktenko, A. K. Fedorov.** Practical issues in decoy-state quantum key distribution based on the central limit theorem. Physical Review A. 2017; 96: 022316.
50. **K.A. Balygin, V. I. Zaitsev. A. N. Klimov, A. I. Klimov, S. P. Kulik, S. N. Molotkov.** Practical quantum cryptography. *JETP Lett*. 2017; 105: 606.
51. **A.V. Gleĭm, V. V. Chistyakov, O. I. Bannik, V. I. Egorov, N. V. Buldakov, A. B. Vasilev, A. A. Gaĭdash, A. V. Kozubov, S. V. Smirnov, S. M. Kynev, S. Ê. Khoruzhnikov, S. A. Kozlov, V. N. Vasil'ev.** Sideband quantum communication at 1 Mbit / s on a metropolitan area network. *J. Opt. Technol*. 2017; 84: 362–367.
52. **E.O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, A. K. Fedorov.** Quantum-secured blockchain. *Quantum Sci. Technol*. 2018; 3, 035004.
53. **A.K. Fedorov, E. O. Kiktenko, A. I. Lvovsky.** Quantum computers put blockchain security at risk. *Nature (London)*. 2018; 563: 465.
54. **D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, M. Tomamichel.** Quantum attacks on Bitcoin, and how to protect against them. Ledger. 2018; 3: 68.
55. **G. Kucsko, P. C. Maurer, N. Y. Yao, M. Kubo, H. J. Noh, P. K. Lo, H. Park, M. D. Lukin.** Nanometer scale quantum thermometry in a living cell. *Nature*. 2017; 500: 54.
56. **I.V. Fedotov, L. V. Doronina-Amitonova, A. A. Voronin, A. O. Levchenko, S. A. Zibrov, D. A. Sidorov-Biryukov, A. B. Fedotov, V. L. Velichansky, A. M. Zheltikov.** Electron spin manipulation and readout through an optical fiber. *Sci. Rep*. 2014; 4: 5362.
57. **I.V. Fedotov, L. V. Doronina-Amitonova, D. A. Sidorov-Biryukov, N. A. Safronov, S. Blakley, A. O. Levchenko, S. A. Zibrov, A. B. Fedotov, S. Ya. Kilin, M. O. Scully, V. L. Velichansky, A. M. Zheltikov.** Fiber-optic magnetic-field imaging. *Opt. Lett*. 2017; 39: 6954.
58. **Н.Н. Колачевский, К. Ю. Хабарова, И. В. Заливако, И. А. Семериков, А. С. Борисенко, И. В. Шерстов, С. Н. Багаев, А. А. Луговой, О. Н. Прудников, А. В. Тайченачев, С. В. Чепуров.** Перспективные квантово-оптические технологии для задач спутниковой навигации. *Ракетно-космическое приборостроение и информационные системы*. 2018; 5: 13.
N. N. Kolachevskij, K.YU. Habarova, I. V. Zalivako, I. A. Semerikov, A. S. Borisenko, I.V. SHerstov, S. N. Bagaev, A. A. Lugovoj, O. N. Prudnikov, A. V. Tajchenachev, S.V. CHepurov. Perspektivnye kvantovo-opticheskie tekhnologii dlya zadach sputnikovoj navigacii. *Raketno-kosmicheskoe priborostroenie i informacionnye sistemy.* **2018; 5: 13.**
59. **D.A. Kalashnikov, A. V. Paterova, S. P. Kulik, L. A. Krivitsky.** Infrared spectroscopy with visible light. *Nat. Photonics*. 2016; 10: 98.
60. **D.A. Shushakov, S. V. Bogdanov, N. A. Kolobov, E. V. Levin, Y. I. Pozdnyakov, T. V. Shpakovskiy, V. E. Shubin, K. Yu. Sitarsky, R. A. Torgovnikov.** The new-type silicon photomultiplier for ToF LiDAR and other pulse detecting applications. *Proceedings of SPIE*. 2018; 10817: 108170J.
61. **S.L. Danilishin, F. Ya. Khalili, H. Miao.** Advanced quantum techniques for future gravitational-wave detectors, arXiv:1903.05223, to be published in *Living Reviews in Relativity*.