КВАНТОВЫЕ ТЕХНОЛОГИИ: НОВЫЕ ВОЗМОЖНОСТИ, УСПЕХИ И ВЫЗОВЫ

Глеб Салахов,
младший научный сотрудник Российского квантового центра, магистр МФТИ

Антон Божедаров,
научный сотрудник Российского квантового центра, аспирант

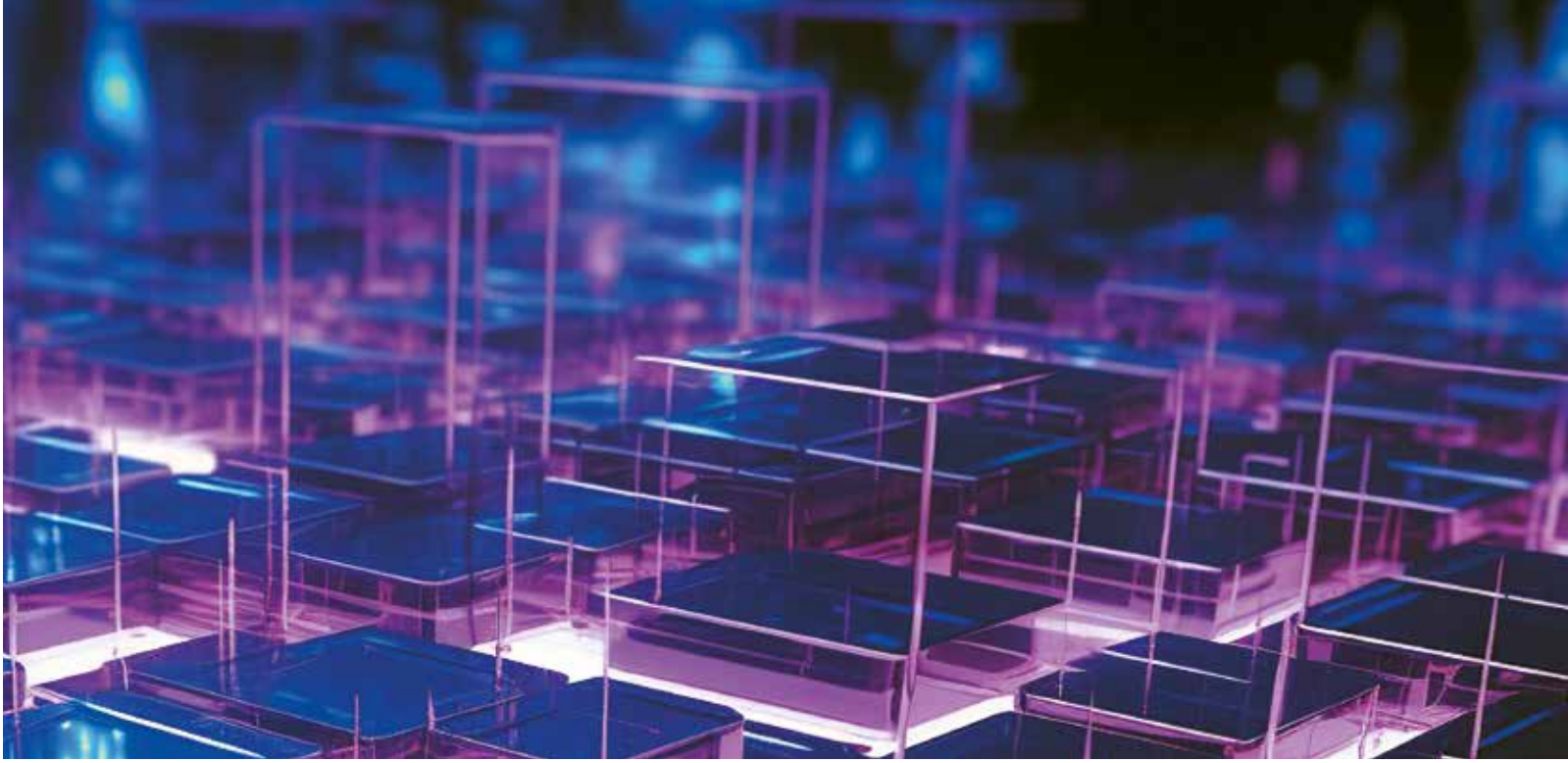
Алексей Федоров,
руководитель научной группы «Квантовые информационные технологии» Российского квантового центра, Национальный исследовательский технологический университет «МИСиС», PhD

Последние десятилетия квантовые технологии, то есть совокупность методов для создания приборов и устройств, основанных на управлении индивидуальными квантовыми системами, активно развиваются и привлекают все больший интерес как со стороны исследователей, так и потенциальных потребителей.

Первая волна квантовых технологий, ознаменовавшая развитие физики в первой половине XX в., привела к созданию широко используемых устройств, наиболее важными из которых, пожалуй, являются лазеры и транзисторы. Эти изобретения вызвали скачкообразный прогресс полупроводниковой электроники, коммуникаций, Интернета, мобильной связи и многих других направлений, сформировав тем самым облик современного информационного общества.

С конца XX в. мир находится на пороге становления второй квантовой волны, которая может оказать еще большее влияние. Ее ключевое отличие от первой, в которой технологии и приборы строились на управлении коллективными квантовыми явлениями, заключается в способности управлять сложными квантовыми системами на уровне индивидуальных квантовых объектов – например, (искусственных) атомов, ионов и фотонов – и их свойств. Методы, основанные именно на таком уровне контроля, сегодня принято объединять термином «квантовые технологии», которым уделяется все большее внимание в силу возрастания их роли в вопросах национальной безопасности, а также в таких стратегически важных отраслях, как ИТ, медицина. Кроме того, квантовые технологии востребованы во всех направлениях цифровой экономики и экономики данных, в том числе, например, искусственного интеллекта (ИИ).

Квантовые технологии принято делить на 3 основных направления.



Квантовые вычисления – новый класс вычислительных устройств, использующий для решения задач принципы квантовой механики, такие как квантовая суперпозиция и квантовая перепутанность [1–2]. Прогнозируется, что в целом ряде случаев квантовые компьютеры обеспечат многократное ускорение в сравнении с существующими суперкомпьютерными технологиями, базирующимися на полупроводниковой электронике,– в сфере кибербезопасности, оптимизации (финансовой, производственной, логистической и т.д.), ИИ, обработки данных, при создании новых материалов и лекарств. При этом стоит отметить, что квантовые компьютеры рассматриваются не как замена традиционных вычислительных технологий, а как их усиление для решения определенных классов задач.

Квантовые коммуникации – технология передачи информации с помощью квантовых объектов; наиболее зрелой частью этой области является квантовое распределение ключей (КРК) [3]. Главное преимущество квантовых коммуникаций – защищенность информации, гарантированная законами физики.

Квантовые сенсоры и метрология – совокупность высокоточных измерительных приборов, основанных на квантовых эффектах. Высокая степень контроля состояния отдельных микроскопических систем позволяет создавать сверхточные квантовые сенсоры с пространственной разрешающей способностью, сравнимой с размером одиночных атомов, а также высокоточные атомные часы [4].

Уже сейчас некоторые направления квантовых технологий близки к коммерческому внедрению, и многие компании вкладывают свои средства в их развитие. Значительные инвестиции были направлены такими мировыми корпорациями, как, например, Google, Microsoft, Intel и IBM. Другие – Airbus, Volkswagen и MasterCard – с помощью этих методов уже решают прикладные задачи. Сети квантовых коммуникаций активно используются коммерческими фирмами Китая [5].

Ожидается, что нарастание применения квантовых технологий будет напоминать развитие лазерных приложений во второй половине XX в. Сначала исследовался лазер сам по себе, позже он стал инструментом для смежных научных отраслей – атомной, молекулярной и оптической физики, и далее для широкого спектра наук, в том числе химии и биологии. Текущий статус квантовых технологий схож: например, квантовые вычисления и разработанные устройства применяются для научных исследований в области квантовой физики многих тел и физики конденсированного состояния, а квантовые сенсоры – для биомедицинских исследований. В случае лазера дальнейший прогресс привел к появлению сначала специализированных

приложений, таких как голография и спектроскопия, а впоследствии и к тому, что лазер стал незаменимой технологией, которая присутствует во многих устройствах. По всей видимости, такой же путь пройдут и квантовые технологии. Например, первые специализированные приложения квантовых вычислений могут быть связаны с обучением нейронных сетей, а что касается квантовых технологий защиты информации, то распределенные ключи используются в высоконагруженных каналах связи. С учетом значительного потенциала последних спектр их применения будет расширяться.

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Текущую степень применения квантовых технологий для решения прикладных задач можно связать с двумя аспектами: уровнем развитости аппаратной реализации квантовых компьютеров и алгоритмами, которые разрабатываются для решения задач квантовыми методами.

Квантовые компьютеры и симуляторы – это вычислительные системы, использующие для решения задач квантовые явления, такие как квантовая суперпозиция и квантовая перепутанность. Устройства, созданные на основе квантовых вычислений, могут многократно превосходить классические компьютеры при решении задач криптоанализа, моделирования сложных (квантовых) систем, машинного обучения. На данный момент существует множество различных видов квантовых компьютеров, которые отличаются как физической платформой, так и моделью квантовых вычислений.

Что касается последней, то ее можно разделить на 2 основные категории: универсальные и специализированные. В сравнении с классическими компьютерами, где универсальность означает возможность проводить произвольную последовательность операций над строкой бит, универсальный квантовый компьютер обеспечивает произвольное преобразование над состоянием кубитов. Примерами универсальных моделей квантовых вычислений являются цифровые (вентильные, или гейтовые) квантовые компьютеры, адиабатические квантовые компьютеры, однонаправленные, а также вариационные квантовые вычисления. Специализированные квантовые компьютеры создаются для решения конкретной задачи или определенного класса задач, например, для моделирования специальных классов квантовых систем или комбинаторной оптимизации [2].

Для реализации моделей квантовых вычислений можно использовать различные физические принципы управления квантовой информацией. Отличие заключается в том, какие системы применяются для кодирования этой информации. Например, это могут быть сверхпроводниковые кубиты, контролируемые с помощью микроволновых импульсов, или атомные кубиты, которые управляются с помощью лазеров.

Масштаб цифровых квантовых компьютеров достигает 433 кубитов, а уже концу 2023 г. прогнозируется появление систем до 1000 кубитов [6]. Нынешнее состояние квантовых технологий называют NISQ-эрой (от англ. Noisy Intermediate–Scale Quantum), когда размеры систем еще невелики – до 1000 кубитов, и при этом процессоры крайне чувствительны в части взаимодействия с окружением. Уровень ошибок в таких системах настолько высок, что не представляется возможным выполнять их квантовую коррекцию [7] – совокупность специальных процедур по исправлению эффектов декогеренции кубитов во время проведения квантовых операций.

Вместе с тем, даже NISQ-устройства претендуют на то, чтобы решать задачи, которые находятся за пределами возможностей классических технологий. В 2019 г. первый такой эксперимент представила компания Google, используя задачи запуска случайных квантовых цепочек [8]. Однако спустя некоторое время были найдены эффективные классические методы решения данной проблемы. Серия последующих опытов показала возможность достижения квантового превосходства с количеством кубитов более 70. Схожий эксперимент был зафиксирован с использованием задачи бозонного сэмплинга. Определенной особенностью является тот факт, что как моделирование случайных цепочек, так и бозонный сэмплинг пока что не имеют ясных практических приложений. Так что пока речь может идти в лучшем случае о демонстрационном квантовом превосходстве.

В 2023 г. научная группа IBM заявила о способе достижения «полезного» превосходства [9]. Используя усовершенствованную технику пода-

вления ошибок, им удалось воспроизвести на 127-кубитном компьютере физическую модель Изинга, которая, в частности, описывает магнетизм постоянных магнитов. Результаты сопоставили с вычислениями на суперкомпьютере для 68 кубитов; в свою очередь, более крупную систему – на 127 кубитах – классическими вычислениями, как утверждалось, посчитать невозможно. Однако спустя короткое время были показаны эффективные классические методы моделирования подобных систем. Поэтому текущий статус развития квантовых вычислений следующий: с помощью созданных NISQ-устройств можно решать демонстрационные задачи на уровне современных суперкомпьютеров, однако вычислительного превосходства, имеющего прикладное значение, пока не найдено. Тем не менее поиски продолжаются. Параллельно с разработкой новых квантовых компьютеров создаются и алгоритмы, но многие из них демонстрируют лишь возможность решения реальных задач уменьшенных масштабов в связи с ограничением размеров текущих квантовых компьютеров. Среди примеров можно назвать следующие:

- *квантовая химия (поиск основного состояния молекулы) [10];*
- *разработка новых лекарств [11] и сборка генома [12];*
- *финансы (оптимизация финансового портфеля, кредитный скоринг, прогнозирование обвалов рынка) [13];*
- *логистика (оптимизация трафика и поиск кратчайшего пути) [14];*
- *телекоммуникации (оптимизация оптических сетей связи) [15];*
- *нефтегазовая отрасль (определение подземных пород в местах нефтяных месторождений).*

Как уже отмечалось, на данный момент решаются задачи небольшой размерности и демонстрируется принцип работы алгоритма с возможностью масштабирования при увеличении мощности квантовых компьютеров.

Одним из возможных кандидатов на демонстрацию полезного квантового превосходства являются задачи машинного обучения. Отчасти это связно с тем, что, как предполагается, для ускорения задач машинного обучения может быть достаточно ресурса квантовых компьютеров, работающих с ошибками, тогда как в других, например в химическом моделировании, требования к ошибкам более строгие [2].

Таким образом, квантовые вычисления находятся на грани прикладной применимости – разрабатываются квантовые или гибридные алгоритмы, позволяющие на текущих размерах квантовых компьютеров решать небольшие прикладные задачи, в то время как количество кубитов в современных квантовых системах удваивается с каждым годом. Еще несколько лет назад предполагалось, что текущее состояние квантовых вычислений будет достигнуто через несколько десятков лет. Сейчас же видно, что множество исследований в этой области привело к бурному росту и достижениям, которые позволили приблизиться к полезному квантовому превосходству. Ожидается, что квантовые вычисления со временем перерастут из нишевого решения для узкого класса проблем в технологию, способную повлиять на развитие многих секторов экономики.

КВАНТОВЫЕ КОММУНИКАЦИИ

С развитием квантовых компьютеров возникает опасность взлома информации, передаваемой криптографическими алгоритмами на основе публичного ключа, например, одного из наиболее популярных протоколов – RSA. Криптографическая стойкость данного алгоритма сводится к предложению о сложности решения определенного класса математических задач, в данном случае – разложения числа на простые множители. Для классических компьютеров эта задача требует экспоненциально растущего времени в зависимости от размера числа. Однако квантовые компьютеры могут использовать для факторизации алгоритм Шора. На данный момент получены результаты, подтверждающие лишь принцип работы алгоритма, где на универсальных компьютерах были разложены числа 15, 21 и 35. Проведенные исследования предсказывают, что для разложения 2048-битного ключа будет необходимо 8 часов и 20 млн кубитов [16]. Таким образом, при появлении квантового компьютера возникает серьезная угроза современной архитектуре информационной безопасности.

Среди возможных решений этой проблемы – квантовые коммуникации, или, более точно, КРК, а также постквантовая криптография. Каждый из подходов обладает явными преимуществами, но и не лишен недостатков.

Квантовые коммуникации – область технологий, связанных с передачей квантовых состояний. Одним из направлений является создание защищенных каналов связи, основанных на квантовом распределении ключей (КРК) – методе защиты передаваемой информации с использованием технологий коммуникации, позволяющем гарантированно защитить данные от компрометации и несанкционированного доступа. Главное преимущество КРК – сохранность информации, обеспеченная законами физики. Сложность коммерциализации заключается в том, что большинство протоколов квантовой связи пока что обладают низкой скоростью распределения ключей, ограниченным расстоянием и требованием к инфраструктуре. Тем не менее уже сегодня в мире создаются протяженные сети КРК.

Многие страны развивают и другой подход – постквантовые алгоритмы. Это новое поколение криптографических методов, которые устойчивы к атакам, как с применением классических, так и квантовых компьютеров. Ряд государств уже ведет работу по стандартизации постквантовых алгоритмов. Также стоит отметить, что КРК и постквантовая криптография – не конкурирующие технологии, а, скорее, дополняющие друг друга при решении разных задач. Например, КРК может быть использовано для защиты высоконагруженных каналов связи между центрами обработки данных, тогда как постквантовая криптография – для защиты мобильных устройств и цифровых подписей.

Еще одной сферой квантовых коммуникаций является передача определенных типов квантовых состояний, что необходимо для создания квантового Интернета – сети взаимосвязанных квантовых устройств [17]. Основное их применение в ближайшем будущем – создание распределенных квантовых вычислений. Объединение нескольких квантовых компьютеров в одну систему позволит увеличить мощность вычислительной системы. Квантовый интернет находится на раннем этапе своего развития – на уровне лабораторных исследований. В 2022 г. была продемонстрирована перепутанность между двумя атомами, разделенными 33-километровым оптическим волокном – следующий шаг к квантовому Интернету и распределенным квантовым вычислениям. Эти изыскания представляют собой развитие идеи передачи перепутанности для практически важных задач квантовых технологий.

Квантовые коммуникации – область квантовых технологий, которая больше всего готова к реальным квантовым приложениям. Сети квантовых коммуникаций уже сейчас используются компаниями (например, в Китае), а планы по внедрению и увеличению таких сетей есть у многих крупных стран мира. Более того, надвигающаяся угроза взлома наиболее популярных протоколов передачи информации квантовым компьютером повышает интерес к развитию квантовых коммуникаций.

КВАНТОВЫЕ СЕНСОРЫ И МЕТРОЛОГИЯ

Квантовые сенсоры – высокоточные измерительные приборы, основанные на квантовых эффектах. Ожидается, что они будут иметь высокое пространственное и временное разрешение, что позволит повысить точность измерений в сравнении с существующими классическими сенсорами, а использование свойств суперпозиции, перепутанности и сжатия квантовых состояний, в свою очередь, обеспечит в перспективе максимально возможную чувствительность измерения за счет преодоления стандартного квантового предела.

На данный момент квантовые сенсоры обладают ограниченным спектром использования, но количество возможных областей их приложения растет с каждым днем.

Яркий тому пример – атомные часы [18]. Технология существует уже несколько десятков лет, и одним из примеров ее удачного и востребованного применения считается система глобального позиционирования (GPS). Квантовые часы представляют собой хронометр, который умеет проводить самокалибровку благодаря собственным колебаниям, связанным с процессами на уровне атомов и молекул.

Также активно развиваются градиометры и гравиметры [19]. Существуют как коммерческие, так и лабораторные датчики. Основной плюс квантовых датчиков – их повышенная чувствительность. Подобные устройства нашли применение в георазведке, археологии, почвоведении, гидрологии и картировании. Некоторые исследования показывают, что квантовые датчики на холодных атомах в 1,5–2 раза эффективнее классических для решения задач по определению небольших закопанных объектов.

Магнитометры – датчики, способные измерять различные характеристики магнитного поля [20]. Существует несколько их физических реализаций: от датчиков на центрах окраски алмазов до приборов, называемых СКВИД, и специальных материалов (например, пленок феррит-граната). Благодаря повышенной точности они востребованы в широком спектре различных отраслей, среди которых можно выделить геологию, археологию, сейсмологию, навигацию, дефектоскопию, биологию и медицину.

Несмотря на вариативность возможного применения, квантовые сенсоры обладают своими минусами, проблемы с которыми сейчас пытаются решить ученые: например, ограничение количества шума для повышения точности технологий. Многие компании сталкиваются с потребностью в больших камерах охлаждения для использования сенсоров, что является одной из проблем при коммерциализации. На текущем этапе в силу повышенной точности квантовых сенсоров их используют как инструмент для исследований в различных отраслях, не связанных с квантовыми технологиями. Постепенно с уменьшением их размеров такие приборы получат более широкое коммерческое применение.

Развитие квантовых технологий достигло этапа, когда создаются государственные программы поддержки и дорожные карты квантовых технологий, все больше средств вкладывается со стороны частного бизнеса. Однако у каждого из направлений – вычислений, коммуникаций и сенсорики – имеются определенные ограничения, которые нужно преодолеть, чтобы перейти от лабораторных исследований к решению практических задач на индустриальном уровне.

Если ранее классические компьютеры и Интернет считались нишевыми технологиями, то сейчас они развились за пределы ожиданий, изменив весь технологический и экономический ландшафт. Это произошло за счет увеличения вычислительных мощностей и, фактически, качества технологии, а также повышения их доступности для массового пользователя. Сейчас сфера квантовых технологий развивается подобным образом, научные институты, государства и крупные компании стараются создавать более продвинутые версии квантовых компьютеров, устройств квантовых коммуникаций и сенсоров, пока параллельно ведется разработка масштабируемых квантовых алгоритмов и других подходов с реальной промышленной эксплуатацией. Поэтому можно ожидать демонстрации первых примеров полезного применения квантовых технологий, и в первую очередь квантовых вычислений, уже в ближайшие годы. НИ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Килин С.Я. Квантовая информация // Успехи физических наук. 1999. №5. Т. 169. С. 507–527.
2. Quantum computing at the quantum advantage threshold: a down-to-business review. Fedorov A.K. [and al.] 2022 г. // https://doi.org/10.48550/arXiv.2203.17181.
3. Килин С.Я. [и др.]. Квантовая криптография: идея и практика.– Минск, 2007.
4. Хабарова К.Ю., Заливако И.В., Колачевский Н.Н. Методы квантовой логики в ионных стандартах частоты, квантовых вычислителях и современной спектроскопии // Успехи физических наук. 2022. №12. Т. 192. С. 1305–1312.
5. Chen Yu-Ao [and al.]. An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. 2021. №7841. Т. 589. P. 214–219.
6. Choi Charles Q. IBM's Quantum Leap: The Company Will Take Quantum Tech Past the 1,000-Qubit Mark in 2023 // IEEE Spectrum. 2023. №1. Т. 60. P. 46–47.
7. Lau J., Wei Zhong [and al.]. NISQ computing: where are we and where do we go? // AAPPS Bulletin. 2022. №1. Т. 32. P. 27.
8. Arute F. [and al.]. Quantum supremacy using a programmable superconducting processor. // Nature. 2019. №574. Т. 574. P. 505–510.
9. Kim Y., Eddins A., Anand S. Evidence for the utility of quantum computing before fault tolerance // Nature. 2023. №618. P. 500–505.
10. Sapova M.D., Fedorov A.K. Variational quantum eigensolver techniques for simulating carbon monoxide oxidation // Communications Physics. 2022. №1. Т. 5. P. 199.
11. Gircha A.I. [and al.]. Hybrid quantum-classical machine learning for generative chemistry and drug design. // Scientific Reports. 2023. №1. Т. 13. P. 8250.
12. Boev A.S. Genome assembly using quantum and quantum-inspired annealing // Scientific Reports. 2021. №11. Article number: 13183.
13. Mugel S. [and al.]. Dynamic portfolio optimization with real datasets using quantum processors and quantum-inspired tensor networks // Physical Review Research 4.1. 2022. 013006.
14. Neukart F. [and al.]. Traffic flow optimization using a quantum annealer // Frontiers in ICT 4. 2017. №29.
15. Boev A.S. [and al.]. Quantum-inspired optimization for wavelength assignment // Frontiers in Physics. 2023. №10. P. 1092065.
16. Gidney C., Ekera M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits (2019) // Quantum. 2021. Т. 5. P. 433.
17. Gyongyosi L., Imre S. Advances in the quantum internet // Communications of the ACM. 2022. Т. 65(8). P. 52–63.
18. Ludlow A.D. [and al.]. Optical atomic clocks // Reviews of Modern Physics. 2015. Т. 87(2). P. 637.
19. Rademacher M., Millen J., Li Y.L. Quantum sensing with nanoparticles for gravimetry: when bigger is better // Advanced Optical Technologies. 2020. №5. Т. 9. P. 227–239.
20. Hrvoic I. [and al.]. Brief review of quantum magnetometers // GEM Systems Technical Papers. 2005.