КВАНТОВЫЕ ВОЗМОЖНОСТИ И РЕАЛИИ

К числу наиболее значимых ресурсов информация добавилась еще в XX веке. Изобретение компьютеров позволило выполнять ее сложную обработку уже не только при помощи человеческой мысли. Сегодня IT-технологии настолько прочно вошли в нашу жизнь, что невозможно представить прогресс без их участия. Тем не менее компьютерная техника продолжает совершенствоваться, развиваясь поистине стремительно. В погоне за более мощной производительностью ее миниатюризация уже преодолела масштабы нанотехнологий и даже перешагнула квантовый порог. Исследователи не оставляют попыток заглянуть вглубь материи и на основе новых знаний о мире создать сверхмощный твердотельный квантовый компьютер. Его появление теоретически просчитано и обосновано, но, соединяя свои знания с реальностью, ученые попадают в очередные «ловушки для разума» – натыкаются на физические законы, затрудняющие реализацию новых возможностей. О квантовых технологиях и перспективах создания техники будущего мы поговорили с заместителем академика-секретаря Отделения физики, математики и информатики Национальной академии наук Беларуси, доктором физико-математических наук, профессором, членом-корреспондентом Сергеем КИЛИНЫМ.

– Определяя приоритеты – прорывные направления в науке – исследователи тем самым нацеливают себя на активную работу в определенной области, в которой, по их мнению, возможно получение наилучших результатов. Значит, прогресс вполне предсказуем?

– Спланировать, как будут развиваться направления научных исследований, – сложная, практически не решаемая задача, особенно, если речь идет о долгосрочном планировании. В качестве примера приведу известный факт. После Октябрьской революции в стране были развернуты масштабные мероприятия по осуществлению плана по электрификации – ГОЭЛРО. В энергетический сектор Госплана СССР стекались все данные, которые получали в результате экспериментальных исследований ученые, и прежде всего Петроградского физико-технического института. В середине 1930-х годов было принято решение создать перспективный план развития энергетики. Он получился гигантским, поскольку включал, казалось бы, всё – от ионных процессов для преобразования тока, котлов высокого давления, газовых турбин, ветроэнергетики до трансформаторного железа и качества изоляции проводов. Однако о ядерной энергетике там не было ни одного слова. Но прошло буквально 10 лет, и эта тема уже возникла. Так что любой написанный план в современном мире является очень краткосрочным. Разумеется, он может быть и глобальным, и перспективно оцененным, но не более того.

Что касается перехода к квантовым технологиям – он осуществлялся поступательно. В XIX веке ученые разобрались, условно говоря, со строением атомов, молекул. Все это привело, в конечном счете, к развитию химической промышленности. В XX веке человек досконально изучил электроны, стало известно, как обращаться и управлять ими в различных материалах, что стимулировало бурный рост электроники. Добытые знания и научные достижения воплотились в конкретных устройствах и системах, используемых в IT-технологиях. Их современный человек воспринимает как должное.

Шагнув на порог квантового мира, мы не теряемся в догадках, заниматься ли нам его изучением. Человечество уже пришло к пониманию, что и он будет освоен. Задача белорусских ученых решить, насколько существенно мы будем участвовать в данном процессе, дабы через некоторое время нам не пришлось вкладывать значительные средства в покупку новых технологий. Тем более что интеллектуальная база для проведения подобных исследований – это целый ряд институтов и научных коллективов – у нас в стране существует.

– Почему же, несмотря на прогнозы, новая техника до сих пор не создана, а разговоры о квантовом компьютере нередко сводятся к высказываниям типа «оптимистичный футуризм», «параллельные миры», «фантастика»…

– Желательно, конечно, об этом говорить не как о каких-то футуристических прогнозах или необъяснимых вещах. Хотя во многом квантовый мир пока труден для восприятия не только обычным человеком, но и самими исследователями. Конечно, постепенно наши знания о нем пополняются, тем не менее его восприятие остается очень абстрактным. Самый простой путь сделать квантовый мир более понятным – это выяснить, какую практическую пользу мы можем извлечь, используя его законы и особенности.

Что касается непосредственно квантового компьютера, то необходимость его появления сегодня – результат прогресса. Возьмите любой ПК, вы вынуждены каждые два года как-то его совершенствовать или вообще приобретать новую машину. Согласно инновационному закону развития мира IT-технологий, во многом объясняющему такое обновление и открытому еще в 1965 году Гордоном Муром, основателем компании Интел, каждые 18 месяцев количество транзисторов в чипе удваивается. Они должны постоянно уменьшаться в размерах и, по прогнозам, к 2015 году транзистор сравняется по размерам с атомом водорода. Поэтому при разработке новых компьютеров уже сейчас необходимо учитывать законы квантового мира, которые открывают уникальные возможности выполнения задач, недоступных не только для привычных ПК, но и для суперкомпьютеров (например, СКИФов), даже объединенных в единую вычислительную сеть. Простой пример задачи, недоступной для классических устройств обработки информации: записать в память все числа, длина которых не превышает 200 значащих цифр. Причем не в десятичной системе, а в двоичной. Всего таких чисел 2^{200}, это столько, сколько атомов во Вселенной. Поэтому, если вы используете в качестве носителей информации, битов, принимающих только два значения 0 и 1, атомы, то для создания такой памяти вам понадобится вся Вселенная. А ведь современные компьютеры используют далеко не атомы. Кроме того, для записи всех этих чисел потребуется такое же огромное число операций – по одной операции на каждый из носителей. Если вы перейдете на квантовый уровень и используете в качестве носителей информации квантовые объекты с двумя возможными состояниями – кюбитами, то вам потребуется всего лишь 200 кюбитов и всего 200 операций, чтобы записать все 2^{200} чисел! Такое колоссальное увеличение возможностей, называемое квантовым параллелизмом, обусловлено тем обстоятельством, что кюбиты, в отличие от своих классических собратьев битов, обладают свойством суперпозиции – они могут совмещать в одном объекте два взаимоисключающих состояния сразу (одновременно представлять и состояние 0 и состояние 1). Для квантового мира суперпозиционные состояния частиц – это такая же обыденность, как суперпозиция волн для макроскопического мира. Однако, создавая квантовые суперпозиции, необходимые для квантовых вычислений, нельзя надеяться на принципы контроля состояний типа «посмотрел – исправил». Здесь требуются более изощренные методы.

Сегодня трудно даже представить, насколько сложные вычисления с громадным объемом чисел мы можем производить,

КИЛИН
Сергей Яковлевич
Родился в 1952 году в г. Гомель. В 1974 году после окончания физического факультета Белорусского государственного университета начал работать в Институте физики имени Б.И. Степанова НАН Беларуси.
С 1994 года – заведующий лабораторией квантовой оптики Института физики имени Б.И. Степанова НАН Беларуси.
В октябре 2008 назначен заместителем академика-секретаря Отделения физики, математики и информатики НАН Беларуси.
Кандидат физико-математических наук (1982), доктор физико-математических наук (1992). Профессор, член-корреспондент НАН Беларуси.
Автор более 440 научных работ, в том числе 4 монографий.
С.Я. Килиным создана признанная в мире белорусская научная школа квантовой оптики и квантовой информатики. В 2005 году избран председателем Белорусского физического общества.
Лауреат Государственной премии Республики Беларусь, лауреат премии Ленинского комсомола Беларуси.

используя возможности квантового мира. Одно из направлений практического их использования связано с моделированием сложных физических, химических и биологических систем. Известно, что природа решает задачу создания простой молекулы из ее фрагментов за фемтосекунды. Для современных компьютеров, решающих эту же задачу путем решения уравнения Шрёдингера, описывающего этот процесс, данная проблема неразрешима. Квантовый симулятор, по мнению исследователей, сможет решить ее за разумный отрезок времени.

– Получается, что ученым известны основные составляющие квантового мира, ясно и то, в решении каких практических задач его возможности применимы. Но ведь работать с этим пока не научились?

– Действительно, в полной мере не научились. В этом процессе есть и достижения, и сложности. К примеру, точно так же, как операции с совокупностью битов (регистрами) представляют упрощенную схему классического компьютера, квантовый компьютер можно представить себе как устройство, осуществляющее логические операции с системами кюбитов. Но с созданием системы кюбитов определенно есть сложности. Так, для того чтобы все 200 электронов квантового процессора работали синхронно, нужно их, условно говоря, заставить плясать под свою дудку. Но квантовый мир сопротивляется вмешательству: чем большее число кюбитов мы хотим объединить когерентным образом, тем более чувствительными они становятся к разрушению со стороны. В настоящее время предложены способы решения этой сложной задачи, но практическая реализация еще не осуществлена.

16-кюбитный квантовый чип компании «Ди-Вейв» в сборе с криогенной системой охлаждения – прототип квантового процессора

– Какие же варианты квантового компьютера предлагаются, исходя из собранных и накопленных исследователями знаний в данной области?

– Прежде чем ученые смогут заявить о создании полноценных квантовых компьютеров, им предстоит решить ряд проблем: выбрать способ реализации кюбитов, то есть определить, какие физические объекты наилучшим образом сохраняют свои когерентные свойства; определить физический механизм взаимодействия между кюбитами, позволяющий осуществлять логические операции с двумя и более кюбитами; найти способ селективного управления кюбитами и измерения их квантовых состояний на выходе системы. Надо реализовать схему исправления ошибок, неизбежно возникающих в процессе декогеренции системы кюбитов. Все это необходимо для создания квантовых компьютеров, нечувствительных к ошибкам.

Наибольшее внимание ученых приковано, конечно, к созданию центрального элемента – квантового процессора. В качестве возможных вариантов рассматриваются несколько схем построения: система ионов в ловушках, фотоны в микрорезонаторах, сверхпроводящие устройства, квантовые точки, также представлены прототипы с использованием в качестве центрального элемента органической молекулы. Ясно, однако, что предпочтение следует отдавать твердотельным устройствам, работающим при комнатной температуре. Другие решения потребуют значительно больших усилий и будут явно проигрывать в эксплуатационном аспекте.

В настоящее время речь идет о создании масштабируемого квантового процессора на примесных центрах «азот-вакансия» (NV-центрах) в алмазах. Идея использования NV-центров для квантовых вычислений была предложена белорусскими учеными совместно с Йоргом Врахтрупом из Штуттгартского университета в 2001 году. Отечественными исследователями доказано, что с помощью оптического излучения при одновременном воздействии магнитных и радиочастотных полей можно когерентным образом управлять одиночными ядерными спинами, принадлежащими NV-центру.

Начатая нами работа продолжает привлекать повышенное внимание исследователей всего мира. Сегодня в области квантовой физики мы работаем совместно с немецкими, французскими, английскими, австралийскими коллегами в проекте EQUIND в рамках 6-й Европейской рамочной программы. Результатом этих исследований должен стать прототип квантового процессора на алмазах.

В предложенном нашими учеными варианте твердотельных квантовых компьютеров на основе NV-центров в алмазе большую роль играет качество сверхчистых синтетических алмазов с минимальной примесью изотопического углерода 13. Создание таких образцов оказалось важным и для других промышленных применений. В частности, россияне очень заинтересованы в создании таких алмазов для «окон» в термоядерном устройстве ТОКАМАК. Белорусским партнером уже является всемирно известный производитель алмазов – компания «Де Бирс».

В целом же квантовые компьютеры – только одно из перспективных направлений квантовой физики, и огромный интерес к этой науке связан не только с созданием уникального компьютера будущего, но и с широкими возможностями развития новых квантовых и нанотехнологий, в том числе нанофотоники, использованием квантовых свойств нанообъектов в биологических и медицинских приложениях. Заняться решением столь актуальных задач Беларуси позволяет прежде всего накопленная поколениями выдающихся отечественных ученых база знаний в области атомной и лазерной физики, оптики и спектроскопии, теоретической физики, физики твердого тела и полупроводников, квантовой оптики. Можно даже сказать, что развитие в нашей стране широкого спектра различных научных направлений, а также наличие высококлассных ученых в области математики и информатики делают Беларусь уникальным местом для развития квантовой информатики, которая по своей сути является многопрофильной междисциплинарной наукой.

Первый в стране сканирующий ближнеполевой оптический микроскоп, созданный учеными НАН Беларуси

Кстати, вполне может оказаться, что самым важным результатом исследований в области квантовой информатики станет даже не сам квантовый компьютер, а те устройства, которые создаются и находят себе применение в процессе научного поиска. Так, использование спиновых и оптических свойств NV-центров позволит создать на основе наноалмазов необычайно чувствительные сенсоры-датчики, которые смогут делать томографию отдельной клетки. По интенсивности свечения уже сегодня можно определить локализацию на уровне клеток и изучать отклонения от нормы. В дальнейшем исследование магнитных полей от отдельных ионных каналов в клеточной мембране позволит биохимикам, медикам и фармацевтам узнать больше о жизни одиночной клетки, в том числе о влиянии лекарственных препаратов на ее функционирование. Понятно, что это направление – будущее медицины, которую квантовые технологии выводят на совершенно иной уровень. Хотя, как я уже отмечал, нельзя на самом деле разделить вещи, которыми занимаются физики, биологи, информатики. Если раньше их области интересов и влияния были разделены, то теперь, благодаря более обширным знаниям о мире, происходит их взаимопроникновение и, естественно, обогащение.

– Существует опасение, что квантовый компьютер сможет легко взломать любые, самые надежные компьютерные

коды классических ПК за довольно короткое время. Значит, с приходом квантовой техники современные криптографические системы защиты информации станут безнадежно устаревшими?

– Подобные опасения не лишены оснований. Все секреты государственных учреждений и частных фирм мгновенно станут беззащитными перед созданным квантовым компьютером, если их защита основана на классических криптографических системах. Квантовый компьютер действительно способен свести на нет существующие системы безопасности, фактически создав огромную проблему для пользователей и одновременно рай для суперхакеров. Однако сам квантовый мир предоставляет и защиту от информационных атак. Дело в том, что в квантовом варианте информация записана в состояниях отдельных летающих кюбитов (фотонов), которые очень лабильны и разрушаются при любых измерениях. Если я кодирую информацию в состояния кюбитов и пересылаю их принимающей стороне, то любая попытка нелегитимного участника «подсмотреть», определить эти состояния, не разрушая передаваемой информации, натыкается на физический закон, запрещающий клонировать неизвестные состояния кюбита. Физика запрещает нелегитимному участнику «словить» фотон, сделать его копию, оставить ее у себя, а оригинальный фотон отправить, как ни в чем не бывало, принимающей стороне. Квантовому компьютеру неподвластна квантовая система криптографии, поскольку информация там защищена на уровне физических законов. К слову, в Институте физики имени Б.И. Степанова НАН Беларуси уже создали работающую квантовую систему криптографии. Данный прототип передает по оптоволоконной линии ключи на расстояние до 5 км. Так что, в какой бы стране мира ни появилась реальная система квантового компьютера, защита от несанкционированного доступа к информации в Беларуси уже разработана.

Написание новых протоколов для квантовых компьютеров, создание новых программных продуктов в области квантовой криптографии в целом очень перспективное направление для нашей страны. Не лишним будет напомнить, что всё это важные патентные вещи. Точно так же, как и архитектура квантовых компьютеров. Никто сегодня точно не скажет, на какой основе будет реализован квантовый компьютер, но в тоже время многие результаты исследований уже запатентованы в надежде на то, что именно этот вариант окажется востребованным.

– С созданием квантового компьютера связано много новых понятий, в том числе и таких, что представляются не просто фантастическими, а иллюзорными. К примеру, квантовая телепортация…

– Почему же, это вполне реальные вещи. Есть такой протокол, согласно которому два находящихся в так называемых перепутанных состояниях кюбита можно использовать как новый ресурс. Допустим, один кюбит у нас в Беларуси, а другой – в Австралии. Условно, как первый шаг к пониманию, это можно представить в виде двух цветов (красный и зеленый) или состояний (0 и 1), которые находятся в сложной перепутанной суперпозиции. Согласно разработанному протоколу, воспользовавшись такими двумя перепутанными кюбитами в качестве ресурса, можно передать неизвестное состояние третьего кюбита, находящегося в Австралии, на кюбит, находящийся в Минске, то есть осуществить телепортацию состояния. Обращаю внимание, что сами кюбиты при этом никуда не перемещаются.

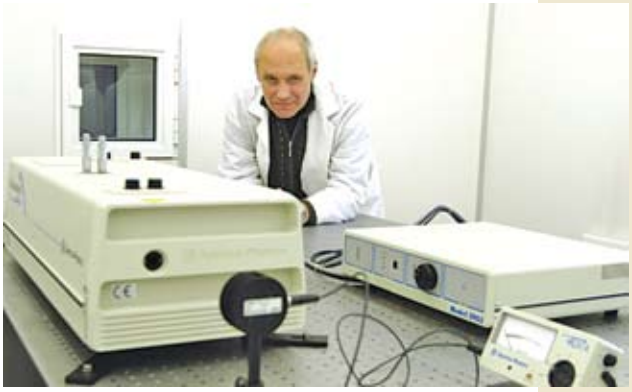
Одной из наиболее разработанных областей применения квантовой информатики является криптография – наука о математических методах обеспечения конфиденциальности и аутентичности информации. Основные направления применения криптографических методов – передача конфиденциальной информации по открытым каналам связи (например, через Интернет), а также установление достоверности передаваемых сообщений. Свойство квантовых объектов изменять состояние при измерении как нельзя лучше подходит для обеспечения секретности передаваемых по открытым сетям сообщений. Первый криптографический протокол обмена данными, основанный на квантовых свойствах фотонов, был придуман канадскими учеными Чарльзом Беннетом и Жилем Брассаром. Он был назван в их честь BB84 и вошел практически во все публикации, посвященные квантовой криптографии.

Данный протокол работает и в отношении макроскопических объектов. В настоящее время проводятся эксперименты с молекулами типа фуллерена. Квантовую телепортацию можно использовать для квантовой криптографии, создания квантового повторителя, который необходим для увеличения дальности действия квантовой криптографии. Квантовая коммуникация с использованием перепутанных состояний (сверхплотное квантовое кодирование) позволяет передать намного большее количество информации в сравнении с классической связью. Кроме того, квантовая связь – передача кюбитов на расстояние – ускорит возникновение своего рода квантового Интернета.

– Так кто же будет первым? Кто представит миру не гипотетический, а работающий квантовый компьютер?

– Сегодня исследователи всего мира борются за первенство, каждый ищет собственные новые подходы. За то, чтобы стать главными в квантовых компьютерах, конкурируют и сразу несколько материалов. Аналогичную гонку столетие назад выиграл кремний и стал основным материалом для микроэлектроники. Для следующего поколения рассматриваются, например, сверхпроводящие устройства. Компания «Ди-Вейв» объявила о создании 16-кюбитной системы на сверхпроводящих материалах. Другими разработчиками в качестве альтернативного варианта предлагается использовать квантовые точки, есть попытки имплантировать кремний с помощью фосфора, создавать компьютеры на основе фотонов и элементов линейной оптики. Но если исходить из реально поставленной задачи – создания твердотельного квантового компьютера, работающего при комнатной температуре, – здесь все преимущества именно у белорусского варианта: алмазного прототипа.

Заглянуть в будущее хотелось бы многим разработчикам. С этой целью в мире созданы и активно работают специальные прогнозные программы (QIPC в Европе и ARDA в США). Расчеты прогнозирования сводятся к тому, что в ближайшее время будут созданы квантовые процессоры



Исследование на фемтосекундном лазере в Международной научной лаборатории НАН Беларуси

на 50 кюбитах. Но это только прогнозы – насколько быстро и успешно новые технологии будут реализованы, покажет время. Ничуть не меньшие перспективы открывают нам и квантовые приложения. Авторитетный технологический журнал MIT Enterprise Technology Review, например, не так давно опубликовал список десяти наиболее быстро развивающихся технологий, способных изменить мир. Квантовая криптография – одна из них.

Высокий научный потенциал Беларуси позволяет оптимистично смотреть на отечественные достижения в области создания квантовых процессоров, развития квантовой криптографии, а также их многочисленных приложений в биологии, химии и нанотехнологиях. В ближайшее время будет реализовываться европейский проект по криптографии через открытое пространство, спутник. Белорусские специалисты сейчас проводят переговоры с российской стороной о том, чтобы осуществить собственный аналогичный проект.

Современные футурологи и ученые поразному представляют открывающиеся миру перспективы: одни считают, что наступивший век будет веком оптики и нанотехнологий, другие говорят о господстве квантовой физики. На перекрестке этих дисциплин находится квантовая информатика, и не исключено, что именно она станет первым практическим результатом технологий XXI века, основанных на хранении и обработке данных на квантовом уровне.

Беседовала
Снежана МИХАЙЛОВСКАЯ ■