Зачем нужны квантовые вычисления?
Часть 1. Что такое квантовый компьютер

Виктор Алексеев (victor.alexeev@gmail.com)

В первой части статьи описываются основные принципы работы квантовых компьютеров, рассматриваются в первом приближении различные их виды и проводится экскурс в технологии квантовых вычислений в целом. Также в этой части статьи приводится описание архитектуры квантового компьютера.

Сегодня не прекращаются дебаты относительно того, зачем нужны квантовые компьютеры; нужно ли инвестировать в эти проекты; насколько реальны перспективы появления полноценных квантовых компьютеров, способных заменить и даже вытеснить классические компьютеры в некоторых приложениях. Особый интерес представляет вопрос о том, когда будет создан квантовый компьютер, который сможет мгновенно взламывать любые шифры. Данная статья является попыткой ответа на такие вопросы на языке, доступном для неспециалистов в квантовой физике. В некотором смысле статья может заинтересовать и людей, знакомых с предметом, поскольку в ней цитируются интересные работы, опубликованные в последние годы в ведущих научных журналах.

С развитием науки и техники всё более актуальными становятся задачи моделирования в таких областях, как, например, квантовая химия и квантовая физика, современные криптографические системы высокого класса устойчивости, разработки новых материалов и лекарственных препаратов и в других аналогичных приложениях.

В ряде случаев стандартные компьютеры с двоичной логикой просто не в состоянии справиться с некоторыми из подобных задач. Надежды на решение этих проблем связаны с новым типом вычислительных устройств, которые используют квантово-механические явления микромира для работы со сложными вероятностными моделями. В отличие от стандартных компьютеров с двоичной логикой, эти квантовые вычислители используют в качестве единицы измерения квантовые биты (кубиты).

В настоящее время классифицируются два основных типа квантовых вычислителей – универсальные цифровые вентильные квантовые компьютеры UDGQC и адиабатические аналоговые квантовые вычислители, включающие в том числе модели с квантовым отжигом AQ, QA. В первой части статьи представлен краткий обзор ситуации с текущими разработками в области квантовых вычислений в ведущих лабораториях мира. Для неспециалистов сделан специальный раздел с простыми вводными пояснениями базовых терминов квантовых вычислений. Также в хронологическом порядке рассмотрены основные типы квантовых кубитов.

Вторая часть статьи посвящена компьютерам классов UDGQC и NISQ, куда входят VQE, адиабатические квантовые вычислители и вычислители с квантовым отжигом.

Введение

Много ли людей в мире слышали в конце 1990-х выражения «квантовый компьютер» и «квантовая физика»? Вероятно, не очень много. Ситуация резко изменилась в начале 2000-х после того, как специалисты концерна IBM с помощью своего лабораторного варианта квантового компьютера с семью вычислительными элементами (кубитами) экспериментально показали работоспособность алгоритма Шора, опубликованного еще в 1994 году. Этот алгоритм теоретически доказывает возможность реализации целочисленной факторизации больших чисел. Иными словами, с помощью этого алгоритма идеальный квантовый компьютер способен достаточно быстро взламывать большинство используемых сейчас асимметричных криптографических схем. Физики из IBM в 2001 году смогли продемонстрировать успешную работу алгоритма Шора на своём квантовом компьютере, разложив число 15 на произведение простых чисел [1].

Эта тривиальная задача вызывает ироническую улыбку. Однако идея была быстро подхвачена прессой и телевидением как реклама квантового компьютера в качестве инструмента, способного взламывать любые криптографические протоколы, в том числе банковские шифры и коды пуска ракет с ядерными боеголовками. Естественно, началась паника, стимулировавшая неограниченное финансирование во всех странах проектов, связанных с квантовыми компьютерами [2–4].

Практически CRQC представляют собой разновидность универсального цифрового квантового компьютера с вентильной обработкой сигнала, который способен атаковать реальные криптографические системы.

Возникли сотни новых лабораторий по всему миру, которые с огромным энтузиазмом взялись за развитие квантовых вычислений и поиск путей создания так называемого «криптографически релевантного квантового компьютера» (Cryptographically Relevant Quantum Computer – CRQC), способного взламывать шифры [5].

Но, несмотря на огромные финансовые вливания и интенсивные исследования, потребовалось около десяти лет для того, чтобы научный мир пришёл к неутешительному выводу о невозможности создания на современном технологическом уровне квантового компьютера типа CRQC. Например, для того чтобы взломать протокол RSA-1024, нужно разложить на простые множители число 2^{1024}. Поэтому для взлома протокола шифрования RSA-1024 в режиме реального времени понадобится универсальный квантовый программируемый вентильный квантовый компьютер с квантовой коррекцией ошибок вычислений, содержащий сотни тысяч кубитов. Хотя теоретическая возможность создания такого компьютера существует, но когда она будет воплощена в жизнь, сейчас сказать крайне сложно [6].

Поскольку ажиотаж, связанный с разработкой CRQC, постепенно утих, многочисленные лаборатории, образовавшиеся в результате «шифровального бума», переключились на новые

направления. Одни лаборатории продолжили развивать технологии квантовых вычислений и переключились на направления, связанные с моделированием задач квантовой химии и физики. Другие фирмы отказались от первоначально заявленной цели (универсальный цифровой квантовый компьютер с вентильным управлением) и начали искать другие применения кубитов.

Третьи фирмы предпочли заниматься специфическими направлениями, такими как, например, «постквантовая криптография». Несмотря на то что на практике создать универсальный цифровой квантовый компьютер, взламывающий коды, не удалось, в рамках этих работ возникло новое направление, целью которого стала разработка квантово-безопасной криптографической технологии, устойчивой к квантовым атакам. Эта технология, получившая название «post-quantum cryptography – PQC» (постквантовая криптография), разрабатывается под эгидой Европейского Института Стандартов и Телекоммуникаций (ETSI) [7].

Сегодня всё более актуальными становятся научные направления, связанные с использованием вероятностного моделирования многоуровневых систем, в которых при увеличении количества задействованных переменных экспоненциально увеличивается число возможных состояний. В ряде случаев, когда в моделях задействованы сотни тысяч параметров, даже сверхмощные современные компьютеры КДЛ просто не в состоянии справиться с некоторыми из подобных задач. Поэтому для решения проблем, связанных с динамикой сложных систем, необходимо либо существенно упрощать математическую модель, либо использовать какие-то совершенно новые типы вычислительных методик. Одним из вариантов ускорения подобных сложных вычислений являются «квантовые вычисления – quantum calculations».

Под термином «квантовые вычисления» подразумеваются некие манипуляции со специальными вычислительными устройствами, в которых используются квантово-механические процессы. Целью квантовых вычислений является нахождение вероятностных решений математических задач специального класса, для которых не существует точных решений с использованием операций, число которых не превышает некоторого полинома в

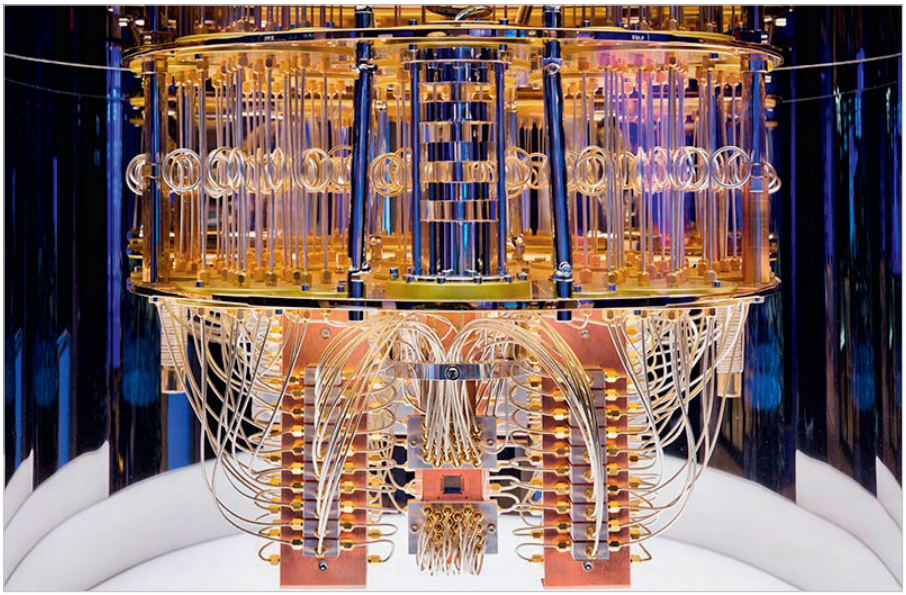

Рис. 1. Внешний вид нового универсального цифрового квантового вентильного компьютера IBM без камеры охлаждения

зависимости от размера исходных данных (NP hard).

Это совершенно иные математические действия, чем хорошо известные двоичные вычисления на стандартных компьютерах КДЛ с логикой «ноль и единица».

Предполагается, что со временем квантовые вычисления помогут коренным образом решить перечисленные выше проблемы с моделированием сложных нестационарных процессов.

В современной англоязычной научно-технической литературе стараются избегать общего термина «quantum computer» и пытаются конкретизировать тип устройства согласно его прямому назначению. В данной статье мы будем стараться придерживаться этого правила. В настоящее время существует пять основных типов устройств, предназначенных для квантовых вычислений:

- универсальный квантовый цифровой компьютер с вентильной обработкой (Universal Digital Quantum Gate Computer UDQGC);
- квантовые адиабатические вычислители (Adiabatic Quantum Processing Unit);
- вычислители с квантовым отжигом (Quantum Annealing Processing Unit – QAPU);
- вариационные квантовые решатели (Variational Quantum Eigensolvers);
- криптографически релевантный квантовый компьютер (Cryptographically Relevant Quantum Computer – CRQC).

В качестве единиц информации все эти устройства используют так называемые квантовые биты (quantum bit – кубит). Это то, что объединяет эти устройства в единый класс – квантовые вычислители.

Квантовые вычислители – это устройства, которые принципиально отличаются от наших стандартных компьютеров КДЛ. Квантовые вычислители в результате некоторых манипуляций с кубитами позволяют получить ответ на поставленную в форме специального алгоритма задачу в виде некоторого события, спрогнозированного с некоторой вероятностью.

Особенности кубитов заключаются в том, что они, являясь объектами квантового микромира, могут существовать в трёх состояниях – два крайних определённых состояния и одно неопределённое квантовое состояние, постулируемое теоретической квантовой механикой как «суперпозиция». К этому понятию вернёмся несколько позже.

Современные технологии позволяют создавать кубиты на базе самых разных квантовых объектов, таких, например, как ионы, нейтральные атомы, фотоны, дефекты в кристаллах, квантовые эффекты в сверхпроводниках и т.д. Использовать эти квантовые состояния можно только при сверхнизких температурах. Поэтому сами кубиты размещаются в специальной холодильной машине (dilution refrigerator), внутри которой поддерживается температура, близкая к абсолютному нулю. Современный квантовый компьютер – это сооружение достаточно внушительных размеров (рис. 1) [8].

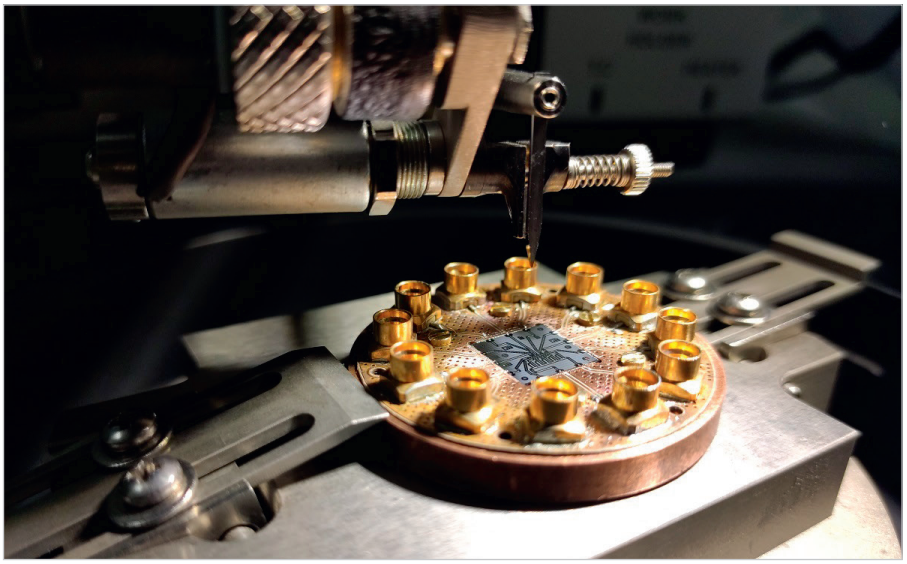

Рис. 2. Интегральная схема на основе пяти сверхпроводниковых кубитов в держателе, разработанная МФТИ

Следует отметить, что существует тип квантовых вычислителей, использующий дефекты в кристаллах, который может работать при комнатных температурах [9].

Кроме того, кубиты на нейтральных атомах работают с лазерным охлаждением и не требуют громоздких криогенных установок.

Современные квантовые вычислители способны моделировать сейчас только простые молекулы. Так, с помощью универсального цифрового квантового компьютера UDQGC сотрудники IBM смогли смоделировать основное состояние молекулы воды [10].

Исследовательская группа из Google Quantum AI при помощи разработанного ими алгоритма определила основные состояния молекулярного азота и других элементов. По мнению руководителя эксперимента Дэвида Райхмана, полученные результаты представляют собой одно из самых значимых событий в квантовой химии за 2022 год [11].

Несмотря на радужные перспективы, реальная оценка существующего уровня развития квантовых вычислений показывает, что, согласно современному уровню теоретической квантовой физики и существующих технологий, для моделирования сложных квантовых систем нужны квантовые компьютеры, содержащие сотни тысяч и миллионы вычислительных ячеек. Это сегодня в принципе невозможно. Самый лучший из квантовых компьютеров класса UDQGC, созданный концерном IBM, содержит 127 кубитов (по данным на 16 ноября 2021 года) [12].

В настоящее время технология квантовых вычислителей в начале 2000-х перешла из начального уровня развития в переходный период поиска новых прорывных технологий. Сейчас мы находимся скорее на уровне демонстрации потенциальных возможностей квантовых вычислений, а также поиска новых алгоритмов и технологий.

В настоящее время во всём мире эксплуатируются и модернизируются образцы универсальных цифровых квантовых вентильных компьютеров UDQGC, представляющие собой сложнейшие лабораторные установки.

Экспериментальные образцы этих компьютеров, расположенные в ведущих мировых исследовательских центрах, в чистом виде в основном используются для изучения и моделирования самого процесса квантовых вычислений и квантовых алгоритмов. В последнее время компьютеры этого типа в сочетании со стандартными компьютерами КДЛ используются в гибридных проектах VQE [13, 14].

Параллельно с развитием направления универсальных цифровых, вентильных квантовых компьютеров развивается направление адиабатических аналоговых квантовых вычислителей. В отличие от цифровых UDQGC, адиабатические квантовые вычислители не имеют цифровых вентилей. Кубиты в них управляются с помощью токов смещения в джозефсоновских переходах. Подробнее об этом в других разделах статьи.

Из чисто научных проектов квантовые вычисления постепенно начинают внедряться в реальную жизнь.

Канадская фирма D-Wave выпускает в продажу квантовые вычислители с отжигом (annealing quantum computer), которые используются многими крупными фирмами и университетами для изучения адиабатических квантовых процессов [15].

Швейцарская фирма ID Quantique предлагает квантовые ключи, квантово-безопасное сетевое шифрование, счётчики одиночных фотонов и аппаратные генераторы случайных чисел на базе кубитов [16]. Американская MagiQ Technologies разрабатывает и поставляет квантовые ключи и квантовые системы безопасности [17, 18].

В настоящее время исследованиями в области квантовых вычислений занимаются около пятисот различных лабораторий практически во всех развитых странах.

По данным [19] на сегодняшний день Великобритания является одним из главных центров по разработкам в области квантовых вычислений. В стране расположены такие ведущие лаборатории по разработке QC, как, например: Quantinuum; Oxford Quantum Circuits; Oxford Instruments; NQCC (UK Research and Innovation); Universal Quantum; Cambridge Quantum; Honeywell Quantum Solutions; Riverlane; QURECA и другие.

Интенсивные разработки квантовых компьютеров ведутся в лабораториях таких университетов, как Leopold-Franzens-Universitat Innsbruck, Kyoto University, Oxford University, University of Calgary, Wuhan University, University of Groningen, Jülich Supercomputing Centre, National Laboratory for Quantum Information Sciences in Hefei и других научных центрах мира.

Согласно данным консалтинговой компании Patinformatics, занимающейся патентной аналитикой, наибольшее число патентных заявок за последние несколько лет на тему квантовых вычислений в мире было подано Китаем, который всячески поддерживает и стимулирует разработки в этой области [20, 21].

Следует обратить внимание на то, что два из крупнейших в мире квантовых компьютеров находятся в КНР: «Jiuzhang 2.0» – мощный фотонный квантовый компьютер и «Zuchongzi» с 56 сверхпроводящими кубитами [22].

Проблемам квантовых вычислений уделяется особое внимание также и в России. Так, например, в научно-исследовательском центре RQC [23], а также

и в лаборатории искусственных квантовых систем МФТИ, разрабатываются квантовые интегральные схемы на основе кубитов из сверхпроводников (рис. 2) [24].

Учёные из Российского квантового центра и Физического института имени П.Н. Лебедева РАН создали прототип квантового компьютера на ионах, используя систему из четырёх кубитов и оригинальную технологию масштабирования квантовых процессоров с использованием многоуровневых носителей информации [25].

В этой связи следует отметить работы, выполненные под руководством одного из основателей «Российского квантового центра» (RQC), выпускника МФТИ, профессора Гарвардского Университета Михаила Лукина [26].

Фактически группа Михаила Лукина разработала первый ионный квантовый компьютер, который стал прототипом для многих вариантов QC, работающих в разных лабораториях мира. Использование модели компьютера с квантовым симулятором атома Ридберга позволило группе Михаила Лукина решить ряд вопросов, связанных с проблемой квантовых фазовых переходов (Quantum phase transitions – QPTs) в динамических изолированных, неравновесных квантовых системах в реальном масштабе времени. В частности, был экспериментально подтверждён квантовый механизм Киббла–Зурека (Kibble–Zurek mechanism – QKZM) для квантовых фазовых переходов изинговского типа (Ising-type QPT). Эти работы являются характерным примером того, как квантовые компьютеры могут быть с успехом использованы в фундаментальных прикладных исследованиях [27].

Простыми словами о квантовом компьютере

Историю развития квантовых компьютеров можно начать отсчитывать от различных событий. На этот счёт существует несколько разных мнений [28]. По одной из версий, начало новому направлению было положено в 1982 году, когда идея квантового компьютера была высказана выдающимся физиком Ричардом Фейнманом (Richard Feynman) в своей знаменитой лекции «Моделирование физики на компьютерах». В ней он обосновал идею некоего устройства на базе естественных квантово-механических процессов, работающего под управлением классического компьютера КДЛ. Следует особо подчеркнуть, что цель работы Фейнмана заключалась не в том, чтобы разработать новый тип вычислительного компьютера, а в том, чтобы лучше понять разнообразные варианты существования электронов в пространстве при различных условиях квантовых явлений. Поэтому и возникла идея изучения объектов квантовой физики с привлечением самих же этих объектов в исследовательском оборудовании. Такое устройство предлагалось использовать для создания вероятностных моделей квантовых систем и их элементов [29].

Позднее этот прибор получил название «квантовый компьютер» (quantum computer, QC).

Израильтянин Дэвид Дойч (David Deutsch), переехавший в Великобританию и работавший в Оксфордском университете, был одним из самых влиятельных квантовых физиков XX века. В 1985 году он опубликовал статью, в которой были изложены основные принципы квантовых вычислений, а также было показано, что квантовые компьютеры могут иметь вычислительную мощность, превышающую вычислительную мощность классических компьютеров, и эффективно решать вычислительные задачи, которые не имеют эффективного решения даже на вероятностной машине Тьюринга [30].

Квантовая механика базируется на трудно воспринимаемых парадоксальных абстракциях, которые описываются крайне сложным математическим аппаратом. Очевидно, что существует какая-то идеальная теория микромира. Но пока она нам неизвестна, мы вынуждены пользоваться квантовой механикой в её текущем состоянии [31]. В прикладных исследованиях, в принципе, можно обойтись и без теоретических основ, принять на веру, что все постулаты так или иначе справедливо утверждаемы одной из интерпретаций, и просто молча использовать существующий математический аппарат. Примерно так охарактеризовал своё отношение к классической интерпретации квантовой механики американский физик David Mermin – «Shat up and calculate» («Перестаньте разглагольствовать и просто займитесь вычислениями») [32].

Иными словами – только формулы и никакой философии. Большинство статей, посвящённых вопросам квантовых компьютеров, следуют именно этому совету. Поэтому люди, не воспринимающие понятия квантовой механики и незнакомые с её экзотическим математическим аппаратом, сходу отвергают эту науку и её выводы вообще. В этой статье нам придётся в минимальном объёме привести некоторые ключевые термины из области квантовых вычислений. Поэтому автор заранее приносит извинение тем людям, которые ненавидят всякие формулы и абстрактные понятия, для которых нет аналогов в реальном мире. В этой статье намеренно не приводятся формулы квантовых вычислений. Для желающих ознакомиться с азами этой непростой науки можно рекомендовать вводный курс [33].

Наименьшая теоретическая единица информации в квантовых вычислениях получила название «quantum bit – qubit» (русский перевод – квантовый бит или кубит).

Коренным отличием единиц информации в КДЛ и квантовом компьютере является то, что, в отличие от двоичного бита с состояниями ноль и единица, кубит имеет третье промежуточное состояние. Это промежуточное неопределённое состояние в квантовой механике получило название «quantum superposition – квантовая суперпозиция».

Одним из удачных примеров, используемых в литературе для визуализации квантовой суперпозиции кубита, является брошенная с самолета на большой высоте монетка. Пока монета, вращаясь, падает вниз, нельзя сказать, в каком состоянии она находится в данный момент – орёл или решка. В этом смысле монета для наблюдателя, ожидающего её на земле, находится по отношению к нему в промежуточном состоянии, то есть в суперпозиции между орлом и решкой. Результат будет точно известен только тогда, когда монетка упадёт на землю. Можно попытаться составить уравнение, описывающее полёт монетки, с учётом законов классической физики, изменения скорости вращения монетки с высотой, сопротивления воздуха на разных высотах плюс наложения случайных факторов типа дождя, бокового ветра и т.д. Если ещё больше усложнить задачу и предположить, что с самолета был выброшен мешок с монетками и нужно определить, как распределятся монетки на земле в момент наименьшего значения их потенциальной энергии, то решение будет трудно найти даже с помощью самого современ-

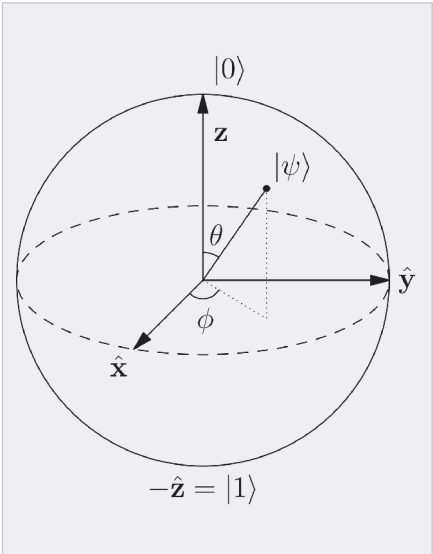

Рис. 3. Образ кубита на сфере Блоха

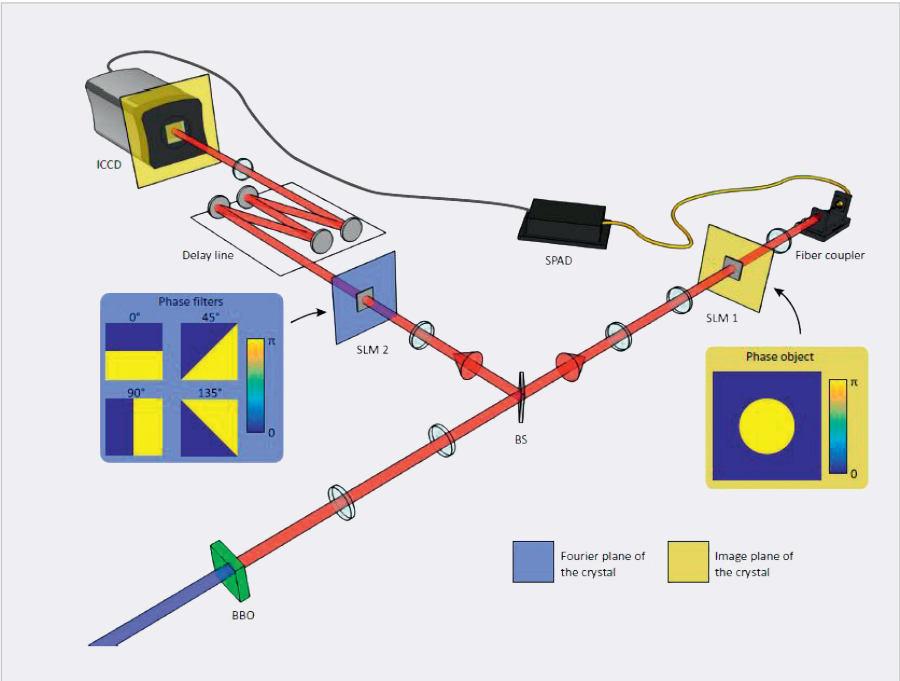

Рис. 4. Схема экспериментальной проверки запутанности фотонов

ного классического КБЛ. Существует третий вариант – попытаться смоделировать процесс падения монетки в лабораторных условиях, используя некий физический процесс. Примерно такой принцип используется в квантовом компьютере, в котором используются свойства квантовых объектов для моделирования сходных по алгоритму задач.

В качестве физического воплощения кубитов в основном используются следующие типы:

- сверхпроводящие кубиты с переходом Джозефсона;
- кубиты с ионными ловушками;
- кубиты на основе нейтральных атомов;
- фотонные кубиты;
- кубиты с дефектами кристаллической решетки;
- кубиты для вычислителей с ЯМР.

Необходимо подчеркнуть, что, в отличие от классической физики, в квантовой механике используется понятие вектора состояния, подразумевающее множество математических величин, которое полностью описывает квантовую систему в гильбертовом пространстве. В ряде случаев вместо термина «вектор состояния» употребляется его синоним – «амплитуда состояния».

В общем случае кубит можно трактовать как вектор состояния двухуровневой системы в гильбертовом пространстве. Поскольку любой вектор состояния может быть представлен как совокупность элементарных векторов, то кубит вводится как понятие минимально возможного векторного состояния. В качестве наглядного представления кубита обычно используют сферу Блоха (рис. 3) [34, 35].

На рис. 3 угол в плоскости XZ соответствует амплитуде вектора, то есть вероятности события, а угол в плоскости XY определяет фазу вращения. Два крайних положения на вертикальной оси определяют два основных состояния кубита. В случае комплексной переменной с мнимыми значения ±i, образующими комплексную плоскость, возможные положения вектора кубита многократно увеличивают его возможные положения. Три проекции вектора полностью определяют матрицу плотности кубита. В случае чистого состояния, при замкнутой системе, вектор, вращаясь в горизонтальной и вертикальной плоскостях, описывает сферу единичного радиуса. Для чистого состояния (замкнутой системы) матрица плотности кубита может быть представлена точкой в нашем привычном трёхмерном пространстве, то есть точкой на поверхности сферы Блоха (рис. 3). Как можно понять, таких точек на поверхности сферы бесконечное множество. В случае смешанного состояния длина вектора становится меньше единицы, и он будет вращаться внутри единичной сферы.

Энергетическое состояние физической системы описывается оператором полной энергии – гамильтонианом *H*, в математическую формулу которого входят параметры, характеризующие потенциальную и кинетическую энергию системы, импульс, координаты, векторы скорости и ускорения и т.д. В квантовой механике гамильтониан генерирует эволюцию квантовых состояний системы во времени.

В то время как существующие классические КДЛ кодируют и обрабатывают информацию в виде двоичного кода, квантовый компьютер, оперирующий с тремя состояниями, определяет вектор состояния кубита, или, иными словами, вероятность нахождения кубита в том или ином состоянии.

Другой важнейший ключевой принцип квантовых вычислений, который называется «квантовая запутанность – quantum entanglement», определяет взаимозависимость состояния двух или большего числа квантовых объектов.

Благодаря «квантовой запутанности» частицы, взаимодействующие друг с другом, могут оставаться связанными, мгновенно меняя свои физические состояния независимо от того, насколько велико расстояние, которое их разделяет.

Эффект «квантовой запутанности» хорошо иллюстрируется на примере фотонов, которые могут иметь линейную, круговую или эллиптическую поляризацию. В свою очередь, круговая поляризация может быть правой или левой, в зависимости от направления вращения вектора индукции. Кроме того, в качестве дополнительного параметра могут быть задействованы орбитальные угловые моменты фотонов. Например, если в паре запутанных фотонов один из них имеет пра-

вую поляризацию, а другой левую, то при изменении поляризации одного из них одновременно изменяется поляризация другого. Причём подобная взаимозависимость сохраняется независимо от расстояния между ними. Это один из парадоксов квантовой механики, тем не менее неоднократно подтверждённый экспериментально.

Группа физиков из Университета Глазго разработала установку, в которой поток запутанных фотонов из квантового источника света пропускался через систему специальных фильтров, изменявших фазы вращения (рис. 4). Регистратор отдельных фотонов срабатывал только тогда, когда на него попадали запутанные кванты света. В результате им удалось получить визуальную картину, демонстрирующую эффект запутанности пары фотонов [36].

В квантовом компьютере для того, чтобы определить текущее состояние системы из N кубитов, нужно знать значения вероятностей нахождения каждого из кубитов в крайнем состоянии. Например, два кубита могут быть в двух состояниях и содержать четыре бита информации. Три кубита дают 8 возможных состояний. Продолжая этот процесс, получим, что 4 кубита – 16 возможных состояний, а N кубитов содержат 2^N бит информации.

Поскольку квантовый компьютер работает не с самими конечными состояниями ноль или единица, а вероятностями их появления, то в принципе возникает возможность обрабатывать все возможные состояния как бы параллельно, что является существенным преимуществом квантового компьютера над обычными компьютерами КДЛ. Однако нужно чётко понимать, что преимущество квантового компьютера перед обычным компьютером КДЛ заключается не в скорости выполнения операций, а в объёме обрабатываемых одновременно данных при решении только определённого круга задач. Поэтому квантовый компьютер никогда не заменит классический компьютер КДЛ, и наоборот. Просто у них изначально разные задачи.

Ещё раз следует подчеркнуть, что квантовый компьютер – это не калькулятор, и он не может точно решить, например, такую задачу: найти Y, если $Y^2 = 4$. В отличие от классического компьютера КБЛ, который мгновенно ответит, что Y = 2, квантовый компьютер после долгих и мучительных поисков,

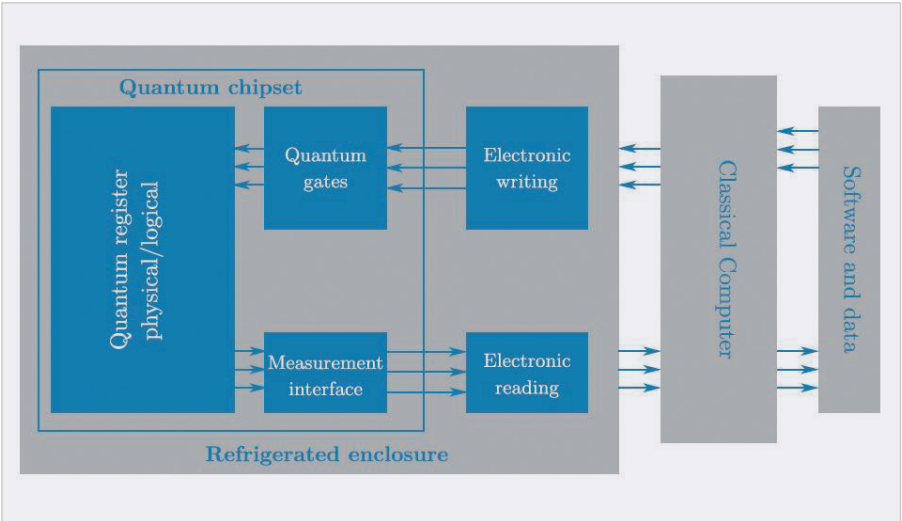

Рис. 5. Структурная схема универсального цифрового квантового компьютера с вентильной обработкой

перебирая различные варианты, скажет, что с вероятностью 99% Y = 2, но есть вариант, что с вероятностью 1% Y = 5. Квантовый компьютер используется только для моделирования некоторых процессов, для которых существуют конкретные квантовые алгоритмы, разработанные под конкретный квантовый компьютер, имеющий определённую структуру и определённый набор квантовых вентилей. При этом ответ будет получен не абсолютно точно, а с некоторой вероятностью.

Например, существует один из простейших квантовых алгоритмов Изинга, предназначенный для описания модели намагничивания материалов. Идея модели Изинга заключается в том, что все магнитные моменты разворачиваются под действием сильного магнитного поля в определённом направлении. После снятия магнитного поля система переходит в наименьшее энергетическое состояние, которое и является вероятностным результатом модели. Точного аналитического решения в общем случае эта задача не имеет. Однако она может быть решена с помощью стандартного компьютера КДЛ статистическими методами в двумерном варианте. В работе [37] было показано, что одномерную модель Изинга также можно успешно задействовать в квантовых вычислениях с помощью квантового алгоритма Изинга. Постепенно выяснилось, что к квантовому алгоритму Изинга можно формально свести и другие задачи в таких прикладных областях, как, например, моделирование молекул, различных физических явлений, процессов в твёрдом теле и т.д. Таким образом, можно применять квантовые вычисления для решения определённого класса задач, используя разработанные и проверенные алгоритмы [38].

На рис. 5 [39] показана структурная схема универсального цифрового квантового компьютера с вентильной обработкой (UDGQC).

Квантовый чипсет небольших размеров содержит: квантовый регистр, состоящий из вычислительных кубитов; квантовые вентили; интерфейс для снятия показаний состояния кубитов. Управляется квантовый чипсет внешней стандартной электроникой.

По аналогии с обычным компьютером КДЛ, управление универсальным квантовым компьютером реализуется с помощью логических вентилей, позволяющих выполнять простейшие операции над одним или двумя кубитами. В литературе встречается также название «квантовый гейт», являющееся калькой с английского термина «quantum gate», который дословно переводится как «квантовый вентиль».

Логические квантовые вентили, которые используются в квантовых вычислениях, имеют иные цели, чем те, которые используются в классических КДЛ. Квантовые логические вентили работают как квантовые операторы. Являясь, по существу, унитарными матрицами, они преобразуют одни текущие вероятностные состояния кубитов в другие состояния с другими вероятностями. Иными словами, квантовые вентили – это базовые управляющие элементы, манипулирующие кубитами в квантовом компьютере.

В квантовых компьютерах нет того привычного регистра, как в классиче-

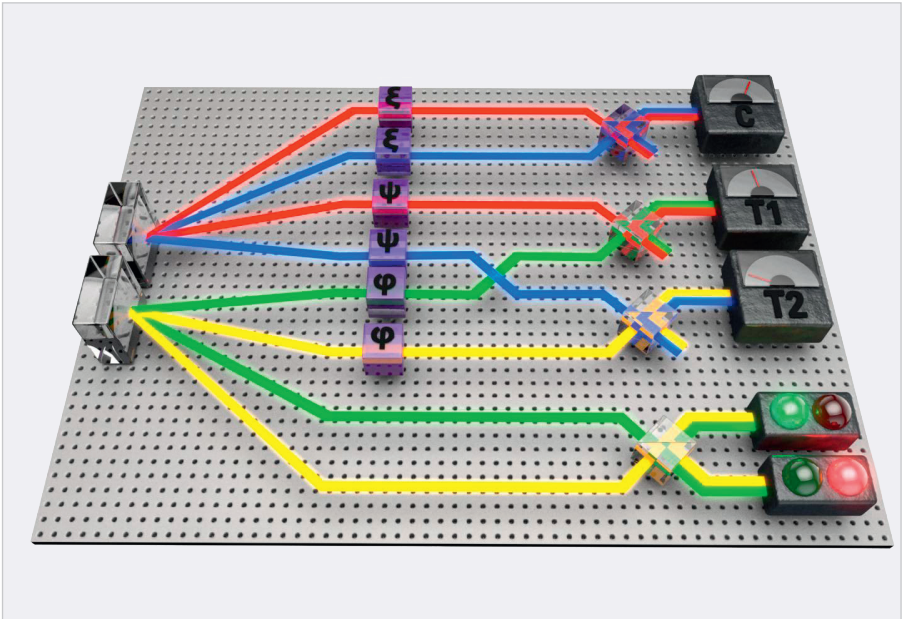

Рис. 6. Схема универсального квантового вентиля

Примечание: Три верхние пары определяют два вычислительных и один управляющий кубиты. Нижняя пара относится к триггеру срабатывания вентиля.

ских КДЛ с ячейками памяти и транзисторной логикой, размещающей нули и единицы в эти ячейки. Роль квантового регистра выполняют сами кубиты, в которых хранится информация в течение времени их жизни. Проще говоря, то, что подразумевается под термином «квантовый регистр», – это просто массив из n кубитов. Причём всё содержимое кубита носит вероятностный характер, заранее неизвестно и проявляется только в процессе вычислений. Квантовые регистры доступны при определённых условиях, в то время как классические регистры КБЛ доступны всегда. Ещё одно важное отличие от КБЛ заключается в том, что квантовые регистры нельзя ни скопировать независимо друг от друга, ни удалить индивидуально.

Нужно также отметить, что вероятность правильного ответа на выходе квантового алгоритма не бывает 100%. При 100% мы выставляем кубит в крайнее положение, выводим его из вычислительного состояния когерентности, тем самым «убивая» активную жизнь кубита и стирая всю предыдущую информацию, записанную ранее в «регистрах» суперпозиции. Именно поэтому в квантовых вычислениях в принципе невозможны необратимые операции. В квантовых компьютерах нет вентилей типа чистого сложения, но есть вентили для выполнения обратимых действий, таких, например, как вычитание, отрицание, тождество.

По сравнению с классическими компьютерами КДЛ у квантовых вентилей больше потенциальных возможностей. Кроме линейных преобразований однокубитные вентили могут также переводить кубиты в состояние суперпозиции, а многокубитные вентили способны запутывать кубиты между собой.

Важным свойством квантовых вентилей является принцип двойного отрицания. Как в английской грамматике два последовательных «не» нейтрализуют отрицание, так и в операторах квантовых вычислений двойное последовательное применение полностью ликвидирует последствия его действия.

Произвольные однокубитные унитарные вентили U также ассоциируются с вращением кубита. Например, вентиль U1 осуществляет вращение одного кубита вокруг оси Z, U2 осуществляет вращение одного кубита вокруг X+Y осей. Вентиль U3 – это универсальный однокубитный поворотный затвор с тремя углами Эйлера.

Следует обратить внимание на одно из фундаментальных свойств квантовых вычислений – квантовый параллелизм (quantum parallelism). Например, если применить оператор «инверсии» к некоторому кубиту, имеющему вероятности появления λ и β в крайних состояниях, соответственно ноль и единица, то кубит перейдет в состояние 0 с вероятностью β, а в состояние единица с вероятностью λ. В результате одной операции изменились сразу оба состояния кубита. В этом смысле вычисления проводятся параллельно. Подобным образом проводятся вычисления с трёхкубитными, четырёхкубитными и более сложными системами. В квантовой системе, состоящей из n кубитов, возможны 2^n значений состояний, определяемых амплитудами вероятности. Если кубиты в системе запутаны, то измерение одного кубита всегда выводит его из состояния запутанности с остальными кубитами и приводит в одно из двух чистых базисных состояний. При этом квантовое состояние всей системы кубитов изменяется скачкообразно по определённому закону. Свойство квантового параллелизма позволяет использовать сразу все состояния кубитов и вычислять функцию состояния квантовой системы в целом.

Существует универсальный набор вентилей, которого достаточно для выполнения любого квантового вычисления. Например, универсальным является набор, включающий вентиль Адамара, вентиль фазового сдвига, вентиль CNOT и вентиль $\pi/8$. С их помощью можно выполнить любое квантовое вычисление на произвольном наборе кубитов [40].

Всё чаще вместо отдельных квантовых вентилей используются универсальные квантовые вентили. В различных типах квантовых компьютеров состояние кубитов контролируется по-разному. Например, в квантовых компьютерах на основе нейтральных ядер состояние кубита определяется с помощью фотонов, которые атом испускает, переходя с одного энергетического уровня на другой. В работе [41] предложена конструкция универсального квантового вентиля, в котором каналы фотонных волноводов переключаются с помощью внешних управляющих сигналов (рис. 6) [42].

За основу в схеме, показанной на рис. 6, взят оператор SWAP, реализуемый в классе управляемых квантовых вентилей. На вход простейшего управляемого вентиля SWAP подаётся управляющий и один управляемый кубит. Вентиль срабатывает в зависимости от состояния управляющего кубита.

В рассматриваемой схеме используются три кубита – два вычислительных и один управляющий. Вентиль меняет состояния двух кубитов в зависимости от состояния третьего, управляющего кубита. Если управляющий вентиль находится в состоянии «единица»,

то вентиль меняет местами выходные каналы (рис. 6). Использование запутанных фотонов позволило контролировать операцию SWAP, поскольку путь по каналу, который выбирался для одного фотона, однозначно определял канал прохождения для другого фотона. Подробное описание этого эксперимента приведено в оригинальной статье.

Одна из самых существенных проблем в квантовых компьютерах связана с ошибками вычисления. Неправильное срабатывание вентилей, случайные сбои в системе считывания, потеря когерентности и другие причины могут приводить к значительным вычислительным ошибкам. Для коррекции ошибок используются специальные методы и дополнительные кубиты, о которых будет сказано ниже.

Важными характеристиками квантового компьютера являются время жизни кубита (qubits lifetime) и время когерентности кубита (qubits coherence time).

Время, в течение которого кубит находится в изолированном квантовом состоянии суперпозиции, при котором кубит сохраняет запутанность и свою информативность, называется временем когерентности.

Время, в течение которого кубит может сохранять свои состояния «0» или «1», в которые он перешёл при схлопывании волновой функции в процессе вычислений, называется временем жизни кубита.

В среднем современные кубиты на сверхпроводящих трансмонах могут иметь времена жизни около 50 микросекунд и времена когерентности примерно 20 микросекунд. Хотя есть работы, указывающие и на более длительные времена жизни кубита. Например, совсем недавно появилась статья, в которой описан процесс сухого травления танталовой пленки, в результате которого были получены трансмоновые кубиты с временами жизни около 500 мкс [43].

Такие времена жизни означают, что после начала работы квантового компьютера нужно провести сами вычисления и коррекцию ошибок в первые 20 мкс и завершить расчёты в течение 50 микросекунд. Это связано с достаточно серьёзными технологическими проблемами, сдерживающими развитие UDGQC в настоящее время.

Для манипуляций с кубитами и управлением квантовыми вентилями в зависимости от типа используемых кубитов используются различные методы. Например, в большинстве компьютеров с кубитами на сверхпроводниках применяются методы управления с помощью высокочастотных посылок с длительностью импульсов порядка 50 нс.

Алгоритмы для квантовых компьютеров являются неотъемлемой частью квантовых вычислений и во многом зависят от аппаратной реализации конкретной модели. Так же как и в случае компьютеров КДЛ, квантовые алгоритмы определяют последовательность унитарных операций для вентилей с указанием кубитов, над которыми их надо совершить (quantum gate array).

Стандартные квантовые алгоритмы описываются в терминах процедур высокого уровня, таких, например, как арифметические операции или специальные преобразования типа преобразования Фурье.

Критерий выбора того или иного алгоритма определяется типом постав-

ленной задачи. Подробно эти вопросы рассмотрены в [44].

В настоящее время известны 63 квантовых алгоритма, которые были опубликованы в ведущих научных журналах мира. Их перечень, составленный программистом из корпорации Microsoft Скоттом Джорданом, приведён в онлайн-каталоге квантовых алгоритмов «Quantum Algorithm Zoo» [45].

Анализ некоторых из существующих квантовых алгоритмов на русском можно найти в работе [46]. Достаточно подробно и доходчиво основы квантовых вычислений рассмотрены в руководстве [47].

Огромную образовательную роль играют обучающие сайты ведущих разработчиков квантовых вычислений. Так, корпорация IBM реализовала открытую программу обучения работе с квантовым компьютером «IBM Q Experience». В рамках этой программы любой, зарегистрировавшийся на сайте концерна, получает доступ к платформе «IBM Quantum Composer» с открытым исходным кодом «Quiskit» [48]. Систему «IBM Q Experience» кроме сотен тысяч частных физических пользователей поддерживают около 100 таких известных мировых фирм, как, например, Delta Air Lines, Anthem Health, Daimler AG и другие. Цели и задачи у партнёров проекта самые различные. Так, Delta Air Lines надеется с помощью квантовых вычислений разработать новое машинное масло с молекулярными присадками. Автомобильный гигант Daimler AG экспериментирует с расчётами аккумуляторов для электромобилей следующего поколения.

В 2020 году начали полностью функционировать ещё две аналогичные открытые платформы по обучению квантовым вычислениям – Microsoft Azure Quantum [49], Amazon Braket [50]. Недавно Google анонсировал новую библиотеку под названием TensorFlow Quantum. TensorFlow – это библиотека с открытым исходным кодом, используемая для машинного обучения на различных языках программирования. Библиотека использовалась такими компаниями, как Airbnb для распознавания изображений, GE для интеллектуальной визуализации мозга и рядом других крупных компаний [51]. Об основных этапах развития квантовых компьютеров будет рассказано во 2-й части статьи.

Литература

1. URL: https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm.
2. URL: https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html.
3. URL: https://www.express.co.uk/news/science/841491/hacking-encryption-quantum-computer-physics.
4. URL: https://futurism.com/worlds-leading-physicist-says-quantum-computers-are-tools-of-destruction-not-creation.
5. URL: https://www.cyber.gov.au/acsc/view-all-content/publications/post-quantum-cryptography.
6. URL: https://arxiv.org/pdf/1312.2316.pdf.
7. URL: https://www.etsi.org/technologies/quantum-safe-cryptography.
8. URL: https://media.nature.com/original/magazine-assets/d41586-021-03476-5/d41586-021-03476-5.pdf.
9. URL: https://quantumbrilliance.com/.
10. URL: https://research.ibm.com/blog/quantum-entanglement-forging.
11. URL: https://news.columbia.edu/news/toward-quantum-computer-calculates-molecular-energy.
12. URL: https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor.
13. URL: https://towardsdatascience.com/the-variational-quantum-eigensolver-explained-adcbc9659c3a.
14. URL: https://www.nature.com/articles/s41534-020-0259-3.
15. URL: https://www.dwavesys.com/.
16. URL: https://www.idquantique.com/.
17. URL: https://www.magiqtech.com/company/.
18. URL: https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-021-00113-y#:~:text=Quantum%20warfare%20(QW)%20is%20warfare,as%20well%20as%20ethics%20issues.
19. URL: https://thequantuminsider.com/2022/05/07/the-whos-who-of-quantum-a-directory-of-40-quantum-companies-from-around-the-world.
20. URL: https://www.patinformatics.com/quantum-computing-report.
21. URL: https://www.tandfonline.com/doi/abs/10.1080/01402390.2021.1973658.
22. URL: https://spectrum.ieee.org/quantum-computing-china.
23. URL: https://habr.com/ru/post/496570/.
24. URL: https://mipt.ru/news/fiziki_mfti_priblizili_sozdanie_kvantovogo_kompyutera_v_rossii.
25. URL: https://www.cnews.ru/news/top/2021-12-28_v_rossii_sozdan_kvantovyj.
26. URL: https://mipt.ru/alumni/intervyu-s-vypusknikami/mikhail-lukin-vse-budet-khorosho.php.
27. URL: https://www.nature.com/articles/s41586-019-1070-1.
28. URL: https://apps.dtic.mil/sti/pdfs/AD1098553.pdf.
29. URL: https://physics.whu.edu.cn/dfiles/wenjian/1_00_QIC_Feynman.pdf.
30. URL: https://www.semanticscholar.org/paper/Quantum-theory%2C-the-Church%E2%80%93Turing-principle-and-the-Deutsch/6b0f06617d9f5256a80ed62d9398acb92a55a6bd.
31. URL: http://philsci-archive.pitt.edu/17688/1/de%20Ronde%20-%20QM%20Needs%20No%20Interpretation.pdf.
32. URL: https://physicstoday.scitation.org/doi/pdf/10.1063/1.1768652.
33. URL: https://habr.com/ru/company/microsoft/blog/351628/.
34. URL: https://habr.com/ru/company/microsoft/blog/351634/.
35. URL: https://quantum-computing.ibm.com/composer/docs/iqx/terms-glossary.
36. URL: https://www.researchgate.net/publication/334438648_Imaging_Bell-type_nonlocal_behavior.
37. URL: https://arxiv.org/pdf/1807.07112.pdf.
38. URL: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.103.032433.
39. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9274431.
40. URL: http://theor.jinr.ru/~diastp/april06/lectures/gerdt/gerdt.pdf.
41. URL: https://www.science.org/doi/10.1126/sciadv.1501531.
42. URL: https://www.science.org/doi/10.1126/sciadv.1501531.
43. URL: https://www.nature.com/articles/s41534-021-00510-2.pdf.
44. URL: https://www.researchgate.net/publication/326959129_An_Introduction_to_Quantum_Search_Algorithm_and_Its_Implementation_Proceedings_of_ICDMAI_2018_Volume_1.
45. URL: https://quantumalgorithmzoo.org/.
46. URL: https://www.rtj-mirea.ru/jour/article/view/138.
47. URL: https://portal.tpu.ru/SHARED/t/TORGAEV/academic/Tab1/Tab/%D0%9F%D0%BE%D1%81%D0%BE%D0%B1%D0%B8%D0%B5%20%D0%BF%D0%BE%20%D0%9A%D0%92.pdf.
48. URL: https://quantum-computing.ibm.com/.
49. URL: https://azure.microsoft.com/ru-ru/free/.
50. URL: https://aws.amazon.com/ru/braket/.
51. URL: https://www.tensorflow.org/.