Электронный научный журнал «Век качества» ISSN 2500-1841 http://www.agequal.ru
2019, №4 http://www.agequal.ru/pdf/2019/AGE_QUALITY_4_2019.pdf
Ссылка для цитирования этой статьи:
Поначугин А.В., Тимофеева К.О., Ковалев Е.А. Квантовые сети // Электронный научный журнал «Век качества». 2019. №4. С. 194-209. Режим доступа: http://www.agequal.ru/pdf/2019/419013.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004.77

Квантовые сети

Поначугин Александр Викторович,
кандидат экономических наук, доцент кафедры
Прикладной информатики и информационных технологий в образовании
Нижегородского государственного педагогического университета
имени К. Минина,
Россия, 603005, г. Нижний Новгород, ул. Ульянова, 1
sasha3@bk.ru
Тимофеева Ксения Олеговна,
студентка, Нижегородский государственный педагогический университет
имени К. Минина,
Россия, 603005, г. Нижний Новгород, ул. Ульянова, 1
kceni_21_01_99@mail.ru
Ковалев Евгений Алексеевич,
студент, Нижегородский государственный педагогический университет
имени К. Минина,
Россия, 603005, г. Нижний Новгород, ул. Ульянова, 1
kovalevea@st.mininuniver.ru

Аннотация. Теоретически доказанная безопасность квантового распределения ключей может революционизировать способ защиты обмена информацией в будущем. Несколько испытаний доказали, что это надежная технология для обмена криптографическими ключами, а также были продемонстрированы узловые сети двухточечных соединений. Однако до сих пор не было дано убедительного ответа на вопрос о том, как расширить сферу применения квантового распределения ключей за пределы нишевых приложений в специализированных сетях с высоким уровнем безопасности. Явления, не имеющие аналогов в классических сетях, такие как невозможность клонирования, квантовое измерение, запутывание и телепортация, накладывают очень сложные ограничения на проектирование сети. В частности, классические сетевые функции, начиная с механизмов управления ошибками и заканчивая стратегиями управления накладными расходами, основаны на предположении, что классическая информация может быть безопасно прочитана и скопирована. Но это предположение не выполняется в квантовом Интернете. Как следствие, разработка такой сети требует серьезного изменения сетевой парадигмы, чтобы использовать особенности квантовой механики.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Ключевые слова: квантовая сеть; запутывание; телепортация; квантовая механика; вычисление; квантовый компьютер; IBM; интеллектуальный барьер; квантовая информация; кубит; виртуальная квантовая машина; криптография.

В настоящее время развитие квантовых компьютеров переживает значительный подъем. В ноябре 2017 г. IBM построила и протестировала 50-кубитовый процессор, в марте 2018 г. Google анонсировала 72-кубитовый процессор. Другие крупные компании, такие как Intel и Alibaba, активно работают над доказательством концепции двузначных кубитов. Такая борьба в создании квантовых компьютеров неудивительна, учитывая их потенциал полностью изменить рынки и отрасли, такие как торговля, разведка, военное дело и т.д. Фактически, квантовый компьютер может решать классы проблем, которые обычные машины выполнить не в состоянии, например, моделирование молекулярных и химических реакций, оптимизация производственных и снабженческих цепочек, финансовое моделирование, машинное обучение и повышенная безопасность. Строительный блок квантового компьютера - это квантовый бит (кубит). Если упростить, то, вычислительная мощность квантового компьютера масштабируется экспоненциально с количеством кубитов, которые могут быть встроены и соединены между собой. Чем больше число кубитов, тем сложнее задача, которую может решить квантовый компьютер. В настоящее время современные квантовые технологии ограничивают мощность квантовых систем двузначными цифрами (IBM - 50 кубитов и Google - 72-кубита).

Таким образом, совсем недавно квантовый Интернет был предложен в качестве ключевой стратегии для значительного увеличения числа кубитов. В частности, соединяя несколько квантовых устройств через квантовую сеть, то есть через сеть, способную обмениваться квантовой информацией между удаленными узлами, и принимая распределенную парадигму, квантовый Интернет создает виртуальную квантовую машину, состоящую из нескольких кубитов, которые масштабируются с количеством соединенных удаленных устройств. Это, в свою очередь, подразумевает экспоненциальное ускорение

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

мощности квантовых вычислений. С точки зрения инженерных коммуникаций, разработка квантового Интернета представляет собой прорыв.

Фактически, квантовая сеть управляется законами квантовой механики. Следовательно, явления, не имеющие аналогов в классических сетях, такие как отсутствие клонирования, квантовое измерение, запутывание и телепортация, накладывают огромные ограничения на проектирование сети. Например, классические сетевые функции - механизмы контроля ошибок (например, ARQ) или стратегии overheadcontrol (например, кэширование), основаны на предположении, что классическая информация может быть безопасно прочитана и скопирована. Но это предположение не выполняется в квантовой сети. Как следствие, проектирование квантовой сети требует серьезного сдвига парадигмы для использования ключевых особенностей квантовой передачи информации, то есть запутывания и телепортации. Актуальность данной темы обусловлена следующими факторами:

1. Миниатюризация вычислительных устройств продолжается, человечество быстро приближаемся к микроскопическому уровню, где доминируют законы квантового мира. Таким образом, не только научное любопытство и проблемы, но и технический прогресс требуют полного изучения ресурсов и возможностей квантовых вычислений;

2. Квантовые вычисления - это потенциал. Уже есть результаты, убедительно демонстрирующие, что для некоторых важных практических задач квантовые компьютеры теоретически экспоненциально мощнее классических компьютеров;

3. Развитие квантовых вычислений является движущей силой и дает новый импульс для более детального и с новых точек зрения изучения концепций, потенциалов, законов и ограничений квантового мира и для совершенствования наших знаний о мире природы. Изучение законов обработки информации, ограничений и потенциалов в настоящее время в целом является мощной методологией для расширения наших знаний, и это, по-видимому, особенно верно для квантовой механики.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

С 1945 г. мы наблюдаем быстрый рост производительности компьютеров в отношении их скорости и объема памяти. Важным шагом в этом развитии стало изобретение транзисторов, которые уже используют некоторые квантовые эффекты в своей работе. Однако ясно, что если такое увеличение производительности компьютеров продолжится, то через несколько лет наши чипы должны будут содержать вентили и работать с тактовой частотой 1014 Гц (таким образом, обеспечивая 1030 логических операций в секунду). Кажется, что единственный способ достичь этого - научиться строить компьютеры непосредственно на основе законов квантовой физики.

Однако квантовый микромир нелогичен, многолик, имеет множество проекций [22].

Для того чтобы серьезно подойти к идее квантовой обработки информации и развить ее так далеко и так быстро, необходимо было преодолеть несколько интеллектуальных барьеров.

Самый основной из них касался важной особенности квантовой физики - обратимости. Ни одна из известных моделей универсальных компьютеров не была обратимой. Этот барьер был преодолен сначала Беннеттом (1973 г.), который показал существование универсальных обратимых машин Тьюринга, а затем Тоффоли и Фредкином (1982 г.), которые доказали существование универсальных классических обратимых ворот.

Второй интеллектуальный барьер был преодолен Бениоффом (1980-1982 гг.), продемонстрировавщим, что квантово-механические вычислительные процессы могут быть по меньшей мере столь же мощными, как и классические вычислительные процессы. Он сделал это, показав, как квантовая система может имитировать действия классических обратимых машин Тьюринга. Однако его «квантовый компьютер» еще не был полностью квантовым и не мог превзойти классические.

Преодоление этих основных интеллектуальных барьеров имело значительные последствия. Отношения между физикой и вычислениями стали исследоваться на более общем и глубоком уровне. Это также было связано с

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

тем, что результаты обратимости подразумевали теоретическую возможность вычислений нулевой энергии. Был организован семинар по физике и вычислениям, и в своем программном выступлении на первом из этих семинаров в 1981 году Р. Фейнман задал важный вопрос: «Может ли квантовая физика быть (эффективно) смоделирована (классическими) компьютерами?». В то же время он привел веские основания для того, что ответ отрицательный. По его мнению, невозможно моделировать общую квантовую физическую систему на вероятностной машине Тьюринга без экспоненциального замедления. Более того, он предположил, что можно решить эту проблему, позволив компьютерам работать в соответствии с законами квантовой механики. Другими словами, квантовые компьютеры могут быть экспоненциально более мощными, чем классические, и могут стать первой разумной моделью вычислений, которая не подчиняется современному тезису Тьюринга.

Третьим интеллектуальным барьером, который необходимо было преодолеть, было отсутствие надлежащей модели универсального квантового вычислительного устройства, способного эффективно имитировать любой другой квантовый компьютер. Первый шаг к преодолению этого барьера был сделан Д. Дойчем (1985 г.), который развил идеи Фейнмана и разработал (теоретически) физически реализуемую модель квантовых компьютеров - квантово-физический аналог вероятностной машины Тьюринга, которая в полной мере использует принцип квантовой суперпозиции и на любом заданном входе производит случайную выборку из распределения вероятностей. Д. Дойч предположил, что для некоторых вычислений это может быть более эффективным средством, чем классическая машина Тьюринга. Он также показал существование универсальной квантовой машины Тьюринга (которая, следовательно, может имитировать любой физический процесс и эксперимент), а также модель квантовых сетей - квантовый аналог классических последовательных логических схем.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Однако данная модель универсальной машины Тьюринга имела тот недостаток, что моделирование других квантовых машин Тьюринга могло быть экспоненциальным. Эта проблема была затем преодолена И. Бернштейном, У. Вазирани и А. Яо. Они показали существование универсальных квантовых машин Тьюринга, способных имитировать другие квантовые машины Тьюринга в полиномиальном времени. В работе Бернштейна и Вазирани (1993 г.) заложены основы квантовой теории сложности. Кроме того, Яо (1993 г.) показал, что квантовая машина Тьюринга и квантовые схемы вычисляют в полиномиальном времени один и тот же класс функций. Этот результат подразумевает, что концепция квантовых вычислений в полиномиальном времени достаточно надежна и не зависит от моделей машин.

Параллельно с разработкой базовых моделей квантовых вычислений предпринимались усилия по преодолению четвертого интеллектуального барьера. Могут ли квантовые вычисления быть действительно более мощными, чем классические вычисления? Есть ли веские основания предполагать, что квантовые вычисления могут привести к существенному (экспоненциальному) ускорению вычислений по крайней мере для некоторых важных задач обработки информации? Это был важный вопрос, потому что было ясно, что любая конструкция квантового компьютера потребует преодоления ряда крупных научных и инженерных барьеров, и поэтому необходимо было знать, предлагает ли данная модель квантового компьютера, по крайней мере теоретически, какие-либо существенные преимущества по сравнению с классическими компьютерами.

Крайне важными и необходимыми шагами в этом направлении были результаты работы П. Шора (1994-1997 гг.), который, опираясь на метод Саймона, показал, как разложить на множители целые числа и как вычислить дискретные логарифмы за полиномиальное время на потенциальных квантовых компьютерах - две проблемы, имеющие решающее значение для криптографии с открытым ключом.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Благодаря этим результатам квантовые вычисления, которые до сих пор считались диковинкой для немногих, стали представлять более широкий научный, и не только научный, интерес. Интенсивный поиск начал открывать физические принципы и процессы, которые могли бы в конечном итоге сделать квантовые вычисления практичными. Кроме того, несколько групп физиков-экспериментаторов по всему миру начали проекты по экспериментальному изучению основных принципов квантовых вычислений.

Следующий вопрос, который нужно было решить, состоял в том, можно ли построить практически успешный квантовый компьютер. Можно ли перевести квантовые вычисления с визионерской стадии на экспериментальную (а затем и на инженерную)?

Интенсивные усилия по решению проблем проектирования квантовых компьютеров принесли некоторые замечательные успехи, но также выявили новые проблемы.

Квантовая криптография, в которой пытаются использовать квантовые феномены для передачи квантовой информации таким образом, что невозможно обнаружить подслушивание, уже достигла экспериментальной стадии. Были также успешны попытки найти достаточно простые обратимые квантовые вентили, которые можно было бы использовать для создания потенциальных квантовых компьютеров. Классические универсальные реверсивные ворота имеют три входа и выхода. Sleator и Weinfurter, Barenco и DiVincenzo показали универсальные двухбитные квантовые ворота. Это стало важным результатом, поскольку задача управления взаимодействием трех частиц представляется гораздо более сложной, чем в случае двух частиц. Кроме того, Barenco и Lloyd доказали, что почти любой квантовый двухбитовый затвор универсален. Эти результаты значительно упростили поиск физических реализаций квантовых вычислительных сетей.

Оказалось также, что первые модели квантовых компьютеров были чрезмерно упрощены и что для того, чтобы квантовые вычисления вышли на экспериментальную или даже инженерную стадию, многие фундаментальные

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

проблемы все еще должны быть решены. Необходимость изучения влияния неточностей, выбросов и взаимодействия с окружающей средой любого реального устройства на способность квантовых вычислений выполнять свои обещания уже давно подчеркивалась Р. Ландауэром (1994 г.). Особенно проблемы декогерентности заставили многих поверить в то, что в принципе невозможно сконструировать достаточно надежно функционирующий квантовый компьютер.

Ситуация начала казаться почти безнадежной. Прорыв произошел после преодоления еще одного интеллектуального барьера: было осознано, что ситуация не так плоха, как кажется, и что физике не нужно полагаться только на себя в поисках путей преодоления проблем несовершенства операций, эмиссии и декогеренции. Оказалось, что начительную помощь могут оказать математика и информатика. Первый важный и обнадеживающий результат был достигнут благодаря И. Бернштейну и У. Вазирани (1993 г.). Они показали, что достаточно слабых требований к точности для квантовых вычислений, достаточно только логарифмической точности для входов и затворов. Открытие П. Шором (1995 г.), а вскоре и многими другими кодов, исправляющих ошибки, позволило справиться с декогеренцией и операционными несовершенствами при передаче и хранении квантовой информации. Открытие Шором (1996 г.) квантовых отказоустойчивых вычислений позволило справиться с декогеренцией и неточностями при обработке квантовой информации. Открытие «сцепленных кодов» (Knill and Laflamme, 1996 г.) и «квантовых ретрансляторов» (Briegel, 1998 г.), дало возможность с желаемой надежностью справляться с проблемой хранения и передачи квантовой информации в течение длительного времени и на большие расстояния.

Квантовая криптография также способствовала осознанию того, что квантовые вычисления полны подводных камней, которые еще не полностью поняты. В 1993 г. Брассар, Крепо, Жозса и Ланглуа удивили научное сообщество заявлением о том, что протокол квантовых бит-обязательств доказуемо нерушим обеими сторонами. Потребовалось три года, чтобы

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

выяснить (Ло и чау и Майерс, 1996 г.) что предлагаемые протоколы в принципе небезопасны.

Еще один интеллектуальный барьер был преодолен Кираком и Золлером (1995 г.), которые показали, по крайней мере на лабораторном уровне, что в поисках технологии для создания квантовых процессоров и компьютеров не нужно ждать, пока будет доступен «unobtainium», а что можно начать с существующих технологий, имеющих богатый экспериментальный опыт.

Для понимания проблем, с которыми сталкиваются ученые при разработке квантовой сети, рассмотрим некоторые постулаты и принципы квантовой механики.

Квантовый бит, или кубит, описывает дискретное двухуровневое квантовое состояние, которое может принимать два базисных состояния: ноль и один, обычно обозначаемое как «0 и «1».

Как известно, классический бит кодирует одно из двух взаимоисключающих состояний, находясь в одном состоянии в любой момент времени. И наоборот, кубит может находиться в суперпозиции двух базисных состояний, будучи таким образом одновременно и нулем, и единицей в определённое время.

Согласно одному из постулатов квантовой механики, всякий раз, когда измерение может иметь более одного исхода, например, для двух возможных состояний кубита, после измерения исходное квантовое состояние коллапсирует в измеренном состоянии. Следовательно, измерение необратимо изменяет исходное состояние кубита. И результат такого измерения является вероятностным, так как получается либо нулевое состояние, либо состояние один, с вероятностью, зависящей от наличия нуля и единицы в исходном наложенном квантовом состоянии. Как следствие, хотя кубит может хранить более одного классического бита информации благодаря принципу суперпозиции, при измерении кубита можно получить только один бит информации. Постулат измерения имеет важное значение для проектирования квантовой сети. Фактически, мы не можем разделить квантовые состояния

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

между удаленными устройствами, просто измеряя кубиты и передавая результаты измерений. Вместо этого мы должны делиться кубитами между удаленными устройствами, не измеряя их, используя фундаментальное свойство квантовой механики - запутанность.

Теорема о невозможности клонирования утверждает, что неизвестный кубит не может быть клонирован. Она является прямым следствием свойств преобразований, допускаемых в квантовой механике. В частности, природа не допускает произвольных преобразований квантовой системы. Природа заставляет эти преобразования быть едиными. Линейность унитарных преобразований сама по себе подразумевает теорему об отсутствии клонирования. Теорема имеет критические последствия с точки зрения инженерной коммуникации, поскольку классические функции связи основаны на предположении, что они могут безопасно копировать информацию. Это, в свою очередь, глубоко влияет на проектирование квантовой сети.

Глубочайшее различие между классической и квантовой механикой заключается в понятии квантовой запутанности, своего рода корреляции, не имеющей классического аналога. Запутанность является частным случаем суперпозиции нескольких кубитов, где общее квантовое состояние не может быть описано в терминах (или как тензорное произведение) квантовых состояний отдельных кубитов.

Квантовая запутанность хорошо подходит для задач, которые требуют координации, синхронизации или конфиденциальность. Примером такого использования является распределение квантовых ключей, синхронизация часов, протоколы для задач распределенной систем, расширение базовой линии телескопов, а также определение местоположения, надежная идентификация и двусторонняя криптография в модели с шумным хранением.

Сегодня мир переживает как квантовую революцию, так и революцию в области машинного обучения. Ведущими компаниями в этих областях являются Intel, Google, IBM, Alibaba и др. Квантовые вычисления – это новая парадигма, которая сыграет большую роль в ускорении задач для

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

искусственного интеллекта (ИИ). Используя квантовые системы, объединенные в сеть, создается виртуальная квантовая машина, способная обеспечить экспоненциальное увеличение мощности вычислений, что значительно ускорит развитие машинного обучения.

Правительства во всем мире выдвигают инициативы в области квантовых вычислений:

– В начале 2016 г. Австралия объявила об инвестициях в размере 25 млн австралийских долларов в течение пяти лет в разработку Кремниевой квантовой интегральной схемы.

– В США в середине 2016 г. Национальный совет по науке и технике опубликовал доклад, который «рекомендует значительные и устойчивые инвестиции в квантовую информатику путем взаимодействия с академическими кругами, промышленностью и правительством в ближайшие месяцы».

– В сентябре 2016 г. канадское правительство выделило 76 млн долларов на программу трансформационных квантовых технологий Университета Ватерлоо для решения трех задач в области квантовых исследований: разработки универсального квантового процессора, квантовых датчиков и дальней квантовой связи.

– Европейская комиссия объявила о планах запуска проекта стоимостью 1,13 млрд долларов США для поддержки ряда квантовых технологий, который начат в 2018 г.

– Китайская академия наук работает с крупной компанией Alibaba, чтобы построить исследовательский центр, в котором будут проводиться квантовые исследования.

Существуют «компьютерные программы, диалог с которыми ориентирован на человека», их обозначают аббревиатурой HCI, что в переводе с английского означает «интерфейс человек-компьютер» (Human-Computer-Interface) [19].

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Сейчас очень интересное и неоднозначное время, когда были продемонстрированы программируемые квантовые вычислительные устройства, но практическая полезность квантовых компьютеров еще не установлена. Переход к подобным ЭВМ сталкивается с рядом новых технических проблем, начиная от улучшения и расширения аппаратного обеспечения кубитов до разработки управляющих/операционных систем и инноваций в алгоритмах и приложениях. Поиск решений этих технических проблем определяет спрос на новое поколение аппаратных средств, программного обеспечения и инженеров для создания и поддержания предстоящей индустрии квантовых вычислений.

Список литературы

1. Аджер Т.Б., Зеленко Г.В., Рощин А.В. Квантовые компьютеры – задачи квантовых вычислений // Уральский научный вестник. 2017. Т. 5. № 3. С. 21-23.

2. Алтунин К.К. Излучение квантовых точек и реализация квантового компьютера на квантовых точках // Когерентная оптика и оптическая спектроскопия: Седьмая Всероссийская молодежная научная школа / Под ред. Салахова М.Х., Самарцева В.В. - Казань, 2003. С. 55-60.

3. Альбов А.С. Квантовая криптография. - М.: Страта, 2018. 248 с.

4. Андрианов С.Н., Моисеев С.А. Нанофотонный квантовый компьютер на основе атомного квантового транзистора // Квантовая электроника. 2015. Т. 45. № 10. С. 937-941.

5. Барановский В.И. Квантовая механика и квантовая химия: учеб. пособие для студ. высш. учеб. заведений. - М.: Издательский центр «Академия», 2008.

6. Блохинцев Д. И. Основы квантовой механики. - М.: Наука, 2014.

7. Богданов Ю.И., Бантыш Б.И., Лукичёв В.Ф., Орликовский А.А., Холево А.С. Динамика сцепленности в квантовых операциях на

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

сверхпроводниковых фазовых кубитах // Известия Российской академии наук. Серия физическая. 2014. Т. 78. № 1. С. 13.

8. Божич В.И., Гушанский С.М., Пипник И.В. Система критериев перепрограммируемого квантового компьютера // Информатизация и связь. 2017. № 4. С. 13-15.

9. Буза М.К. Архитектура компьютеров. Минск: Высшая школа, 2015. 416 с.

10. Валиев К. А. Квантовые компьютеры и квантовые вычисления // УФН. 2005. Т. 175, № 1. С. 3-39.

11. Выгоняйло Р.А. Исследование квантового компьютера и разработка математического и программного обеспечения симулятора квантовых вычислений // Нейрокомпьютеры и их применение: XVI Всероссийская научная конференция: тезисы докладов. 2018.

12. Гузик В.Ф., Гушанский С.М., Чурсин В.А. Использование квантовой суперпозиции и квантовой запутанности для обучения квантовой нейронной сети // Информатизация и связь. 2017. № 4. С. 9-12.

13. Кайе Ф.А., Лафламм Р.К. Введение в квантовые вычисления. - Ижевск: РХД, 2013.

14. Китаев А.Ю., Шень А., Вялый М. Классические и квантовые вычисления. - М.: МЦНМО, 2015.

15. Кокс Б., Форшоу Д. Квантовая вселенная. Как устроено то, что мы не можем увидеть: пер. с англ. А. Коробейникова, [науч. ред. В. Марача, М. Павлов]. - М.: Манн, Иванов и Фербер, 2016. 278 с.

16. Кузнецов В.М. Квантовая механика. - М.: БИНОМ. Лаборатория знаний, 2015. 291 с.

17. Куксин С. Б., Нейштадт А.И. О квантовом усреднении, квантовой теории Колмогорова–Арнольда–Мозера и квантовой диффузии //Успехи математических наук. 2013. Т. 68. № 2(410). С. 145-158.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

18. Молотков С.Н. Квантовая запутанность и составные ключи в квантовой криптографии. Письма в Журнал экспериментальной и теоретической физики. 2017. Т. 105. № 11-12. С. 763-767.

19. Поначугин А.В., Лапыгин Ю.Н. Цифровые образовательные ресурсы вуза: проектирование, анализ и экспертиза // Вестник Мининского университета. 2019. Т. 7. № 2. С. 5.

20. Попов Д.Е. История и методология физики. Квантовая механика: учебное пособие / Костромской государственный университет. - Кострома, 2015.

21. Потапов В.С., Гузик В.Ф., Гушанский С.М. О производительности и вычислительной сложности квантовых алгоритмов // Информатизация и связь. 2017. № 4. С. 16-19.

22. Ревунов С.Е., Кузнецов С.И., Бархатова О.М., Ревунова Е.А. Проблема связи сознания наблюдателя и квантово-механического описания физической реальности // Вестник Мининского университета. 2019. Т. 7. № 3. С. 14.

23. Садовничий В.А. Квантовый компьютер и квантовые вычисления. - Ижевск: Ижевская республиканская типография. 1999.

24. Ciliberto C., Herbster M., Davide Ialongo A., Pontil M., Rocchetto A., Severini S., Wossnig L. Quantum machine learning: a classical perspective // Proceedings Of The Royal Society A: Mathematical, Physical and Engineering Sciences. 2018. Vol. 474. No 2209. P. 20170551.

25. Cover T.M., Thomas J.A. Elements of Information Theory / John Wiley & Sons, Inc., 1991. 542 pp.

26. Gambetta J.M., Chow J.M, Steffen M. Building logical qubits in a superconducting quantum computing system / npj Quantum Information. 2017. No 3.

27. O'Malley P.J.J., Babbush R., Kivlichan D., Romero J., McClean J.R., Barends R., Kelly J., Roushan P., Tranter A., Ding N., Campbell B., Chen Y., Chen Z., Chiaro B., Dunsworth A., Fowler A.G., Jeffrey E., Lucero E., Megrant A., Mutus J.Y., Neeley M., Neill C., Quintana C., Sank D., Vainsencher A., Wenner J., White

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

T.C., Coveney P.V., Love P.J., Neven H., Aspuru-Guzik A., Martinis J.M. Scalable Quantum Simulation of Molecular Energies // Physical Review X. 2016. No 6. P. 031007.

28. Wendin G. Quantum Information Processing with Superconducting Circuits: a Review // Department of Microtechnology and Nanoscience - MC2 / Chalmers University of Technology, SE-41296. - Gothenburg, Sweden, 2017.

29. Willsch D., Willsch M., Jin F., De Raedt H., Michielsen K. Testing quantum fault tolerance on small systems // Physical Review A. 2018. Vol. 98. No 5. P. 052348.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Quantum networks

Ponachugin Alexander Viktorovich,
Candidate of Economics, associate Professor, Department of Applied Informatics and information technologies in education, Nizhny Novgorod state pedagogical University named after K. Minin

Timofeeva Ksenia Olegovna,
student, Nizhny Novgorod state pedagogical University named after K. Minin

Kovalev Evgeny Alekseevich,
student, Nizhny Novgorod state pedagogical University named after K. Minin

Abstract. The theoretically proven security of quantum key distribution could revolutionize the way information exchange is protected in the future. Several trials have proven it to be a reliable technology for exchanging cryptographic keys, and point-to-point nodal networks have also been demonstrated. However, no convincing answer has yet been given to the question of how to extend the scope of quantum key distribution beyond niche applications in specialized high-security networks. Phenomena that have no analogues in classical networks, such as the impossibility of cloning, quantum measurement, entanglement and teleportation impose very complex restrictions on the design of the network. In particular, classical network functions ranging from error management mechanisms to overhead management strategies are based on the assumption that classical information can be safely read and copied. But this assumption does not hold in the quantum Internet. Therefore, the development of such a network requires a major change in the network paradigm to take advantage of the features of quantum mechanics.

Keywords: quantum network; obfuscation; teleportation; quantum mechanics; computing; quantum computer; IBM; intellectual barrier; quantum information; qubit; virtual quantum machine; cryptography.