УДК 004.27:004.056.55

КВАНТОВЫЕ ТЕХНОЛОГИИ КАК ОСНОВА КВАНТОВОГО КОМПЬЮТЕРА

В.И. КЛЮЧКО, Н.В. КУШНИР, Д.С. ШЕЛЕХАНЬ

Кубанский государственный технологический университет,
350072, Российская Федерация, г. Краснодар, ул. Московская, 2;
электронная почта: kushnir.06@mail.ru

В современном мире компьютерные технологии занимают очень важное место. Сейчас есть очень перспективное направление. Квантовые компьютер и квантовые технологии. В данной статье речь пойдёт о развитии и перспективах применения квантовых технологий. Также речь пойдет о преимуществах квантового компьютера. Классическая машина Тьюринга способна одновременно исполнять лишь одно вычисление, квантовая занимается несколькими вычислениями параллельно. Сегодняшние компьютеры работают по тому же принципу, что и нормальные машины Тьюринга – с битами, которые находятся в одном из двух состояний: 0 или 1. У квантовых компьютеров таких ограничений нет: информация в них зашифрована в квантовых битах (кубитах), которые могут содержать суперпозиции обоих состояний
Ключевые слова: квантовые технологии, квантовая криптография, квантовый компьютер.

Квантовые технологии – это попытка использовать квантовую физику на благо человечества. Квантовая физика – богатая наука, и мы здесь выделяем тот класс явлений, который считаем полезней. Квантовая оптика – это наука, в которой мы учимся создавать состояние света. Мы знаем, что самые быстрые линии, позволяющие нам работать в интернете, – это оптические линии. Связано это с тем, что у света высокая несущая частота порядка 1015, и его можно модулировать на очень высокой частоте. Если для электрического тока частоты 1 ГГц дают вам гигабит, и это уже достаточно высокие частоты, то для света эти частоты являются несерьезными.

Квантовые технологии можно использовать для квантовых вычислений и для квантовых линий связи. Зачем нам нужны квантовые линии? Вопрос в секретности. В современном интернете секретность обеспечивается криптографическими ключами, большая часть базируется на технологиях открытого ключа. Технология основана на том, что расшифровать ключ определенной длины сложно, имея современные вычислительные технологии, но если эти технологии улучшатся, то мы сможем этот ключ расшифровать, и

тогда банковские переводы станут небезопасными. Квантовые линии связи предлагают другой принцип: они предлагают посылать информацию, закодированную в одиночных частицах, фотонах. В квантовой механике запрещена сама возможность копировать квантово-механические частицы. Вы их можете измерить только один раз. Если кто-то попытается ее измерить и послать такую же, то это можно будет сделать только с ошибкой, что сразу будет заметно.

Сейчас квантовые технологии используются мало, в основном банками.

Обычный компьютер в качестве логической единицы информации имеет бит. Биты могут принимать только 2 значения – 0 или 1. А квантовый компьютер оперируетквантовыми битами– кубитами (сокращённо). Кубиты имеют не материальную (физическую), а квантовую природу. Поэтому могут одновременно принимать значения и 0, и 1, и все значения комбинаций этих 2-х основных.

Именно благодаря квантовой природе кубита и его способности принимать одновременно несколько значений, квантовые компьютеры имеют способность решать большое количество задач параллельно, т.е. одновременно. В то время, как бит обычного компьютера перебирает все возможные значения последовательно. Таким образом, задачу, на решение которой обычному компьютеру понадобится несколько десятков лет, квантовый компьютер решит за несколько минут.

Выдающемуся физику Ричарду Фейнману принадлежат слова: «С уверенностью можно сказать, что никто не понимает квантовой физики» [https://ru.wikiquote.org/wiki/Ричард_Фейнман]. Ричард Фейнман был первым физиком, который предрёк возможность появления квантового компьютера

Ошибки в квантовых компьютерах можно разделить на два главных уровня. Ошибки первого уровня присущи всем компьютерам, в том числе и классическим. К таким ошибкам относится непроизвольная смена кубитов из-за внешнего шума (например: космических лучей или радиации). С этой проблемой недавно удалось справиться специалистам из компании Google. Для

решения этой проблемы команда ученых во главе с Джулианом Келли создала особую квантовую схему из девяти кубитов, которые ищут ошибки в системе. Остальные кубиты отвечают за сохранность информации, таким образом, сохраняя ее дольше, нежели с использованием единичного кубита. Однако основная проблема никуда не делась, остается второй уровень ошибок. Кубиты изначально по своей природе нестабильны, они мгновенно забывают информацию, которую вы хотите сохранить на квантовый компьютер. Под воздействием на кубит окружающей среды нарушается связь внутри квантовой системы (процесс декогеренции). Чтобы избавиться от этого, квантовый процессор нужно максимально изолировать от воздействия внешних факторов. По словам экспертов, 99% мощности такого компьютера уйдет на исправления ошибок, и лишь 1% хватит для решения любых задач. Конечно, от ошибок не удастся избавиться полностью, но если минимизировать их до определенного уровня, квантовый компьютер сможет работать.

Кубит – это квантовый разряд. Фактически количество состояний или значений кубита бесконечно. Это возможно благодаря его квантовой природе.

В нашем материальном мире это невозможно, поэтому это так трудно представить. Разберем понятие суперпозиции кубита на примере из нашего физического макромира.

Представим, что у нас есть один мяч, и он спрятан в одной из 2-х коробок. Мы точно знаем, что мяч может находиться только в одной из коробок, а в другой – пусто. Но в микромире всё не так. Представим, что в коробке атом вместо мяча. В этом случае неправильно было бы предположить, что наш атом находится в одной из 2-х коробок. Согласно закону квантовой механики, атом может находится в 2-х коробках одновременно – быть в суперпозиции.

Исходя из свойства суперпозиции, кубит может выполнять вычисления параллельно. А бит – только последовательно. Обычный компьютер последовательно перебирает все возможные комбинации (варианты), например, состояния системы. Для точного описания состояния системы из 100

составляющих на квантовом компьютере понадобиться 100 кубит. А на обычном – триллионы триллионов бит (огромные объемы оперативной памяти).

Квантовый компьютер нужен для решения задач, где для получения правильного ответа необходимо перебрать большое количество вариантов.

Это поиск по огромным базам данных, моментальное прокладывание оптимального маршрута, подбор лекарств, создание новых материалов и множество других важных для человечества задач.

В качестве наглядных примеров можно привести 2 задачи, которые в математике называются задачами рюкзака и коммивояжёра.

Представьте, что Вы завтра едете в путешествие и за сегодня необходимо сделать много дел. Вам надо так распланировать день, чтобы посетить все места за минимум времени. Эта задача по оптимизации перемещения по нескольким точкам в математике называется задачей коммивояжера. Поразительно, но за разумное время её невозможно решить. Если мест, немного, например, 5, то вычислить оптимальный маршрут не сложно. А если точек 15, то количество вариантов маршрутов составит 43 589 145 600. Если на оценку 1 варианта Вы потратите секунду, тогда для анализа всех вариантов Вы потратите 138 лет! Это всего для 15-ти точек маршрута!

Задачи, подобные задаче коммивояжера, которые нельзя решить за разумное время, даже пользуясь самыми мощными компьютерами, называются NP-полными. Они очень важны в обычной жизни человека. Это задачи по оптимизации, от размещения товаров на полках склада ограниченного объема до выбора оптимальной стратегии капиталовложения.

Теперь у человечества появилась надежда, что такие задачи будут быстро решаться с помощью квантовых компьютеров.

Почему боятся появления квантового компьютера?

Большая часть криптографических технологий, например, для защиты паролей, личной переписки, финансовых транзакций, создана на том принципе, что современный компьютер не может за короткое время решить определенную

задачу. Например, перемножить два числа компьютер быстро может, а вот разложить результат на простые множители ему не просто (точнее, долго).

Пример. Чтобы разложить на два множителя число из 256 цифр, самому современному компьютеру понадобилось бы несколько десятков лет. А вот квантовый компьютер по алгоритму английского математика Питера Шора эту задачу сможет решить за несколько минут.

Благодаря сложности этой задачи для обычного компьютера, Вы безопасно снимаете деньги в банкомате и оплачиваете покупки платежной картой. К ней, помимо пин-кода, привязано большое число. Оно делится на Ваш пин-код без остатка. При вводе пина, банкомат делит Ваше большое число на введенный Вами пин и проверяет ответ. Для подбора правильного числа злоумышленнику понадобилось бы время, по истечении которого во Вселенной уже не осталось бы ни планеты Земля, ни платёжной карты.

Но на радость всем криптографам квантовый компьютер в серийном варианте всё ещё не создан. Однако по запросу «квантовый компьютер новости» уже сегодня звучит ответ: «Это дело не далекого будущего». Разработки активно ведутся крупнейшими корпорациями, такими, как IBM, Intel, Google и многими другими.

Когда ждать массового производства квантовых компьютеров?

Одно дело разработать теорию кубита, а совсем другое дело воплотить в реальность. Для этой цели надо найти физическую систему с 2-мя квантовыми уровнями для использования в качестве 2-х базовых состояний кубита – единицы и нуля. Для решения этой задачи научные группы разных стран используют фотоны, ионы, электроны, ядра атомов, дефекты в кристаллах.

Основных ограничений в работе кубитов два: 1. количество кубитов, которые могут работать сообща; 2. время их жизни.

В 2001 году в компании IBM было выполнено тестирование 7-кубитного квантового компьютера. Квантовый компьютер IBM выполнил разложение числа 15 на простые множители по алгоритму Шора.

В2005 году российские учёные совместно с японскими построили 2-кубитный процессор на сверхпроводящих элементах.

В 2009 году физики американского национального института стандартов и технологий создали программируемый квантовый компьютер, который состоял из 2-х кубит.

В 2012 году IBM достигла прогресса в реализации вычислений при помощи сверхпроводящих кубитов. В этом же году ученым нескольких американских университетов удалось построить 2-кубитный компьютер на кристалле алмаза.

Лидером в создании квантовых устройств является Канадская компания D-Wave System. С 2007 года D-Wave анонсирует создание таких квантовых компьютеров: 16 кубит, 28 кубит – в 2007 году, 128 кубит – в 2011 году, 512 кубит – в 2012 году, более 1000 кубит – в июне 2015 года.

Кстати, квантовый компьютер купить у компании D-Wave можно уже сегодня за 11 миллионов долларов

Такой компьютер уже купил Google, хотя и сам гигант интернета работает над созданием собственного квантового компьютера.

D-Wave квантовый компьютер не универсальный, а предназначен для решения одной определенной задачи – поиска минимума какой-либо очень сложной функции. Можно представить функцию в виде горной системы. Целью оптимизации является поиск наиболее глубокой долины в горной системе.

Задача на поиск минимальной функции очень важна для человечества и решает задачи от поиска минимальных затрат в экономике до анализа процессов фотосинтеза.

Google сообщил, что компьютер D-Wave смог решить эту задачу (найти минимум функции) приблизительно в 100 миллионов раз быстрее, чем классический компьютер

Относительно того, когда же появится компьютер, который можно будет назвать квантовым, исследователи сходятся на сроках в 10-15 лет. По

прогнозам футурологов компании Cisco Systems, квантовый компьютер должен появиться к середине 2020 года; футурологи TechCast прогнозируют, что повсеместное распространение квантовых компьютеров начнется приблизительно с 2022 года. В то же время, в компании IBM заявляют, что располагают всем необходимым, для того чтобы создать квантовый компьютер в течение ближайших 10-15 лет. Универсальные же квантовые компьютеры вряд ли появятся в самом ближайшем будущем.

Проанализировав работы в области создания квантовых алгоритмов и квантовых компьютеров можно сделать вывод, что достигнут новый качественный уровень, Который открывает перспективные возможности по реализации многокубитовых квантовых компьютеров. Эти компьютеры дают существенный прирост в эффективности в сравнении с обычными компьютерами и обеспечивают решение ряда сложных математических (в том числе криптографических) задач. Перспективы создания многокубитовых квантовых компьютеров связаны не только с технологическими возможностями, но и с решением вопросов построения эффективных квантовых алгоритмов решения актуальных математических задач, задач криптографии и задач управления (оптимизации). Появление шифрования такого рода поставит окончательную точку в борьбе криптографов за наиболее надежные способы шифрования сообщений Гигантская вычислительная мощь квантового компьютера позволит переложить на плечи машины самую разнообразную интеллектуальную деятельность. Машина может не только накапливать, хранить и обрабатывать информацию, но и производить с ней операции, совершенно недоступные даже самым мощным современным компьютерам. Нельзя сказать, что нейронные и квантовые компьютеры целиком вытеснят классические, однако в определенных сферах данные типы вычислителей смогут значительно улучшить выполнение специфичных задач.

ЛИТЕРАТУРА

1. Немного о квантовых компьютерах и о том, изменят ли они нашу жизнь [Электронный ресурс] – Режим доступа: URL: https://geektimes.ru/company/ua-hosting/blog/247424/Дата обращения: 10.12.2016.

2. Как квантовые компьютеры изменят мир [Электронный ресурс] – Режим доступа: URL: http://www.lookatme.ru/mag/how-to/inspiration-howitworks/212579-quantum-computers-explained Дата обращения: 10.12.2016.

3. Квантовый компьютер. [Электронный ресурс] – Режим доступа:URL: https://ru.wikipedia.org/wiki/Квантовый_компьютер Дата обращения: 10.12.2016.

4. Квантовые компьютеры [Электронный ресурс] – Режим доступа: URL: http://www.nkj.ru/archive/articles/5309/ Дата обращения: 26.11.2015.

5. Ричард Фейнман [Электронный ресурс] - Режим доступа: URL: https://ru.wikiquote.org/wiki/Ричард_Фейнман

REFERENCES

1. A little bit about quantum computers and whether they will change our lives [Electronic resource] – Access mode: URL: https://geektimes.ru/company/ua-hosting/blog/247424/ Date of the application: 10.12.2016.

2. How quantum computers will change the world [Electronic resource] - Access mode: URL: http://www.lookatme.ru/mag/how-to/inspiration-howitworks/212579-quantum-computers-explained Date of the application: 10.12.2016.

3. Quantum computer. [Electronic resource] – Access mode: URL: https://ru.wikipedia.org/wiki/Kvantovyy_kompyuter Date of the application: 10.12.2016.

4. Quantum computers [Electronic resource] – Access mode: URL: http://www.nkj.ru/archive/articles/5309/ Date of the application: 26.11.2015.

5. Richard Feynman [Electronic resource] - Access mode: URL: https://ru.wikiquote.org/wiki/Ричард_Фейнман/ Date of the application: 26.11.2015

QUANTUM TECHNOLOGY AS THE BASIS FOR A QUANTUM COMPUTER

V.I. KLYUCHKO, N.V. KUSHNIR, D.S. SHELEKHAN

Kuban State Technological University,
2, Moskovskaya St., Krasnodar, Russian Federation, 350072,
e-mail: kushnir.06@mail.ru

In today's world of computer technology occupy a very important place. Now there is a very promising direction. Quantum computers and quantum technologies. In this article we will focus on the development and prospects of the application of quantum technologies. Also, we will focus on the benefits of a quantum computer. Classical Turing machine can simultaneously execute only one computation, quantum computing is engaged in several parallel. Today's computers work on the same principle as that of a normal Turing machine - with the bits that are in one of two states: 0 or 1. Quantum computers do not have these restrictions: The information in them is encoded in quantum bits (qubits), which may contain superposition of both states.

Key words: quantum technology, quantum cryptography, quantum computer.