Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Калмыков М.В. Квантовый компьютер-возникновение идеи, теоретические результаты, практические разработки и возможные угрозы криптографии. Создание квантовой сети в России // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2017. – № 06 (июнь). – АРТ 180-эл. – 0,3 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004

Калмыков Максим Владимирович
Курсант 3 курса, факультет информационной безопасности
в автоматизированных системах
Научный руководитель: Хисамов Ф.Г., д.т.н., профессор
Краснодарское высшее военное училище имени генерала
армии С.М.Штеменко
г. Краснодар, Российская Федерация
e-mail: Maksim-19971997@mail.ru

КВАНТОВЫЙ КОМПЬЮТЕР-ВОЗНИКНОВЕНИЕ ИДЕИ, ТЕОРЕТИЧЕСКИЕ РЕЗУЛЬТАТЫ, ПРАКТИЧЕСКИЕ РАЗРАБОТКИ И ВОЗМОЖНЫЕ УГРОЗЫ КРИПТОГРАФИИ. СОЗДАНИЕ КВАНТОВОЙ СЕТИ В РОССИИ

Аннотация: В статье рассмотрены теоретические разработки ученых(принципиальная схема квантового компьютера, его принцип работы, требования, предъявляемые к незамедлительной, беспрерывной работе квантовых машин), которые при применении в практический этап, смогут открыть новые возможности в криптографии.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Ключевые слова: квантовый компьютер, квантовые вычисления, кубиты.

Kalmykov Maxim Vladimirovich
3-course cadet, information security faculty
in automated systems
Supervisor: Khisamov FG, Doctor of
Technical Sciences, Professor
Krasnodar Higher Military School named after General of the
Army S. Shtemenko Krasnodar, Russian Federation

QUANTUM COMPUTER-INITIATION OF IDEAS, THEORETICAL RESULTS, PRACTICAL DEVELOPMENTS AND POSSIBLE THREATS OF CRYPTOGRAPHY. CREATION OF A QUANTUM NETWORK IN RUSSIA

Abstract: Theoretical developments of scientists (the quantum computer schematic diagram, its operating principle, the requirements for the immediate, continuous operation of quantum machines) are considered in the article, which, when applied in practice, can open new opportunities in cryptography.

Key words: quantum computer, quantum computing, qubit.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Человечество искало пути решения из сложившихся проблем, создавая новое, неизвестное ранее. Так и в среде вычислительных машин: от простейших счетов Абака пришли к суперкомпьютерам сегодня. Казалось бы, что это апогей, но возникла новая проблема- малая вычислительная мощность современных персональных компьютеров и ноутбуков. Дело в том, что они построены на основе фон-Неймановской архитектуры, таким образом, они работают с последовательным режимом выполнения команд. К примеру, если рассматривается число, у которого 100 000 знаков(в двоичной записи), то потребуется перебрать 3х вариантов. Если предположить, что для одного перебора требуется один процессорный такт, то при скорости в 3 ГГц для перебора всех чисел будет нужно время, превышающее возраст нашей планеты. В связи с этим многие ученые стали заниматься решением данной проблемы и предложили квантовые вычисления, которые стали бы основой квантовых компьютером, имеющие параллельный режим выполнения команд, тем самым увеличили число переработанной информации в единицу времени.

Первые теоретические результаты.

Первыми, кто выдвинул такую мысль были Фейман и Манин в 1980 году, после них-Дэвид Дойч, который предлагал конкретную математическую модель квантовой машины в 1985 году. Однако в 1994 году интерес к квантовым компьютерам усилился, после того как американский математик Питер Шор предложил разложения n-значного числа на простые множители за время полиномиально зависящее от n. Задача разложения числа на

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

простые множители имеет прямое отношение к криптографии, из ходя из этого делаем вывод ,что квантовые компьютеры могли бы подобрать ключи к надежной на сегодняшний день системе шифрования RSA. Но пока до практической реализации далеко, можно не опасаться, что шифры будут взломаны с помощью квантового компьютера. Теперь разберемся, как на теории должны работать квантовые компьютеры.

Для передачи информации в квантовом канале связи необходимо, чтобы фотон находился в одном из двух базовых состояниях:|1>,либо |0>. Такие состояния называют состоянием поляризации. В каком состоянии окажется фотон, и будет зависеть дальнейшее состояние всей системы. Вектор состояния системы также называется волновой функцией квантовых состояний или кубитами. В отличие от классического бита, который может принимать два логических значения, кубит-это квантовый объект, и число его состояний, определяемых суперпозицией ,неограниченно. Однако ещё раз подчеркнем, что результат измерения кубита всегда приводит нас к одному из двух возможных состояний. В общем случае, если квантовая система состоит из L кубитов, то у нее имеется возможных состояний, каждое из которых может быть измерено с некоторой вероятностью. Функция состояния такой квантовой системы запишется в виде[1]:

$$|\psi\rangle = \sum_{n=0}^{2^L-1} c_n |n\rangle$$

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

где $|n>$- базисные квантовые состояния, а c_n- вероятность нахождения в базисном состоянии $|n>$.

Рассмотренное нами преобразование состояния суперпозиции квантовой системы, состоящей из L кубитов представляет собой модель квантового компьютера. Чтобы использовать квантовую схему для вычисления, нужно уметь вводить входные данные, проделывать вычисления и считывать результат Поэтому принципиальная схема любого квантового компьютера должна включать функциональные блоки, показанные на рис1[1]: квантовый регистр для ввода данных, квантовый процессор для преобразования данных и устройство для считывания данных.

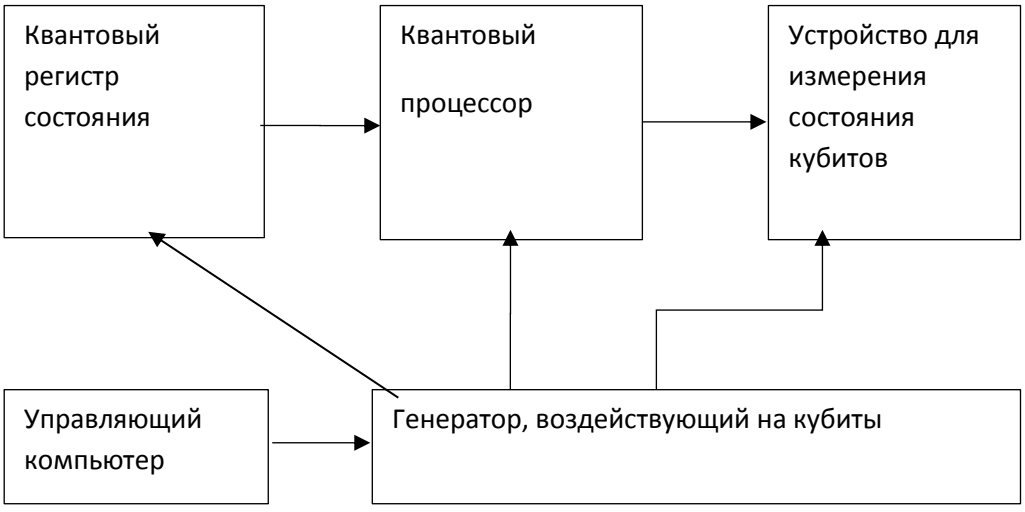

Рис.1 Принципиальная схема квантового компьютера

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Считается, что для реализации полномасштабного квантового компьютера, превосходящего по производительности любой классический компьютер, на каких бы физических принципах он ни работал, следует обеспечить выполнение следующих основных требований:[1]

физическая система, представляющая собой полномасштабный квантовый компьютер, должна содержать достаточно большое число L>103 хорошо различимых кубитов для выполнения соответствующих квантовых операций;

необходимо обеспечить максимальное подавление эффектов разрушения суперпозиции квантовых состояний, обусловленных взаимодействием системы кубитов с окружающей средой, в результате чего может стать невозможным выполнение квантовых алгоритмов. Время разрушения суперпозиции квантовых состояний должно в 104 раз превышать время выполнения основных квантовых операций;

необходимо обеспечить измерение с достаточно высокой надежностью состояния квантовой системы на выходе. Измерение конечного квантового состояния является одной из основных проблем квантовых вычислений.

Практические разработки

Для практического применения пока не создано ни одного квантового компьютера, который удовлетворял всем вышеперечисленным требованиям. Но скажем что попытки есть. Так в столице Татарстана запущен пилотный участок первой в России многоузловой квантовой сети.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Проект, над которым работают ученые из Казанского квантового центра КНИТУ-КАИ и Санкт-Петербургского исследовательского университета информационных технологий, механики и оптики (ИТМО), должен стать основой для создания инфраструктуры квантовых коммуникаций в масштабе страны.

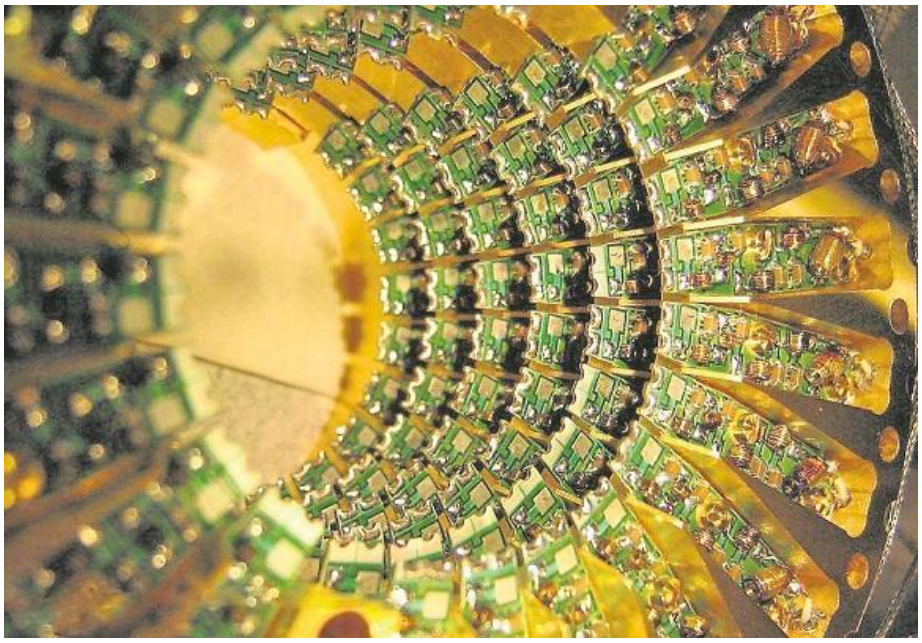

Рис.2 Увеличенная в 100 раз модель квантового узла в разрезе

Квантовая связь будет востребована всеми пользователями, кому необходима конфиденциальность передачи данных.

В рамках казанской сети квантовым каналом будут объединены четыре узла на расстоянии 30-40 километров друг от друга. На данный момент запущен первый участок, соединивший два корпуса КНИТУ-КАИ. При этом используется действующая оптоволоконная линия.

Запущенная в Казани сеть полностью основана на оригинальных отечественных разработках и по техническим

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

параметрам не уступает, а по ряду характеристик превосходит передовые зарубежные аналоги. Так, например, скорость генерации просеянных квантовых последовательностей на линии протяжённостью 2,5 километра достигла 117 кбит/с - на порядок быстрее, чем в европейских сетевых проектах в области квантовой связи. Передача квантовых бит была осуществлена в оптическом канале с потерями 20 дБ, что эквивалентно расстоянию 100 километров Реализуемый проект является важным шагом для внедрения технологии.

Главная задача создаваемой сети - "полевые испытания": тестирование технологии, отработка механизмов интеграции квантовых каналов в существующую телекоммуникационную инфраструктуру и масштабирования квантовой сети. Все это осуществляется на реальных местах пользования и на базе работающих городских линий связи. Для нашей страны это важнейший шаг в развитии квантовых систем сложной конфигурации и топологии, адаптированных под потребности операторов связи и конечных пользователей.

До нынешнего момента в России в городских условиях уже использовались линии квантовой связи, однако организованы они были только по принципу "точка-точка". Первую подобную сеть запустил в 2014 году Университет ИТМО в Санкт-Петербурге, объединив два корпуса вуза по подземному оптоволоконному кабелю. В этом году сообщалось о том, что Российский квантовый центр провел сеанс квантовой связи между двумя офисами банка в Москве.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Запуск пилотных участков, связывающих между собой университеты, приведёт к взрывному росту технологий и формированию новых рынков, на базе которых вырастет отечественная инфраструктура связи нового поколения. По прогнозам ученых, примерно через 5-10 лет технология квантовой коммуникации станет такой же привычной полезной частью жизни, как широкополосный интернет и мобильная связь.[2]

Список использованной литературы:

1.К.А.Валиев.Квантовые компьютеры и квантовые вычисления./ Успехи физических наук, январь 2005. Том 175, №1;

2. С.А. Селезнев. Первая квантовая сеть в России./ Статья из газеты “Известия”, август 2016;

Дата поступления в редакцию: 04.06.2017 г.
Опубликовано: 07.06.2017 г.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru