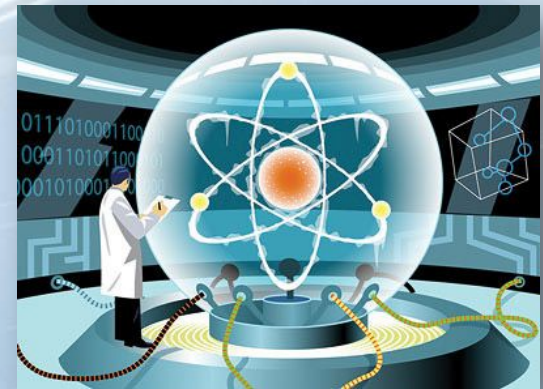
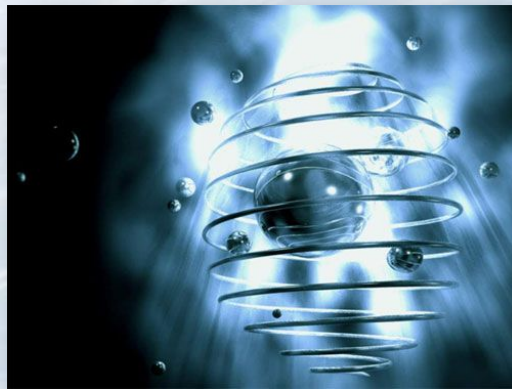
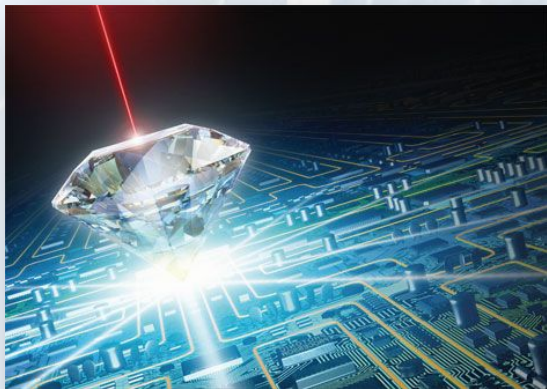


КВАНТОВЫЕ КОМПЬЮТЕРЫ



Содержание

1

Введение

2

Как все начиналось

3

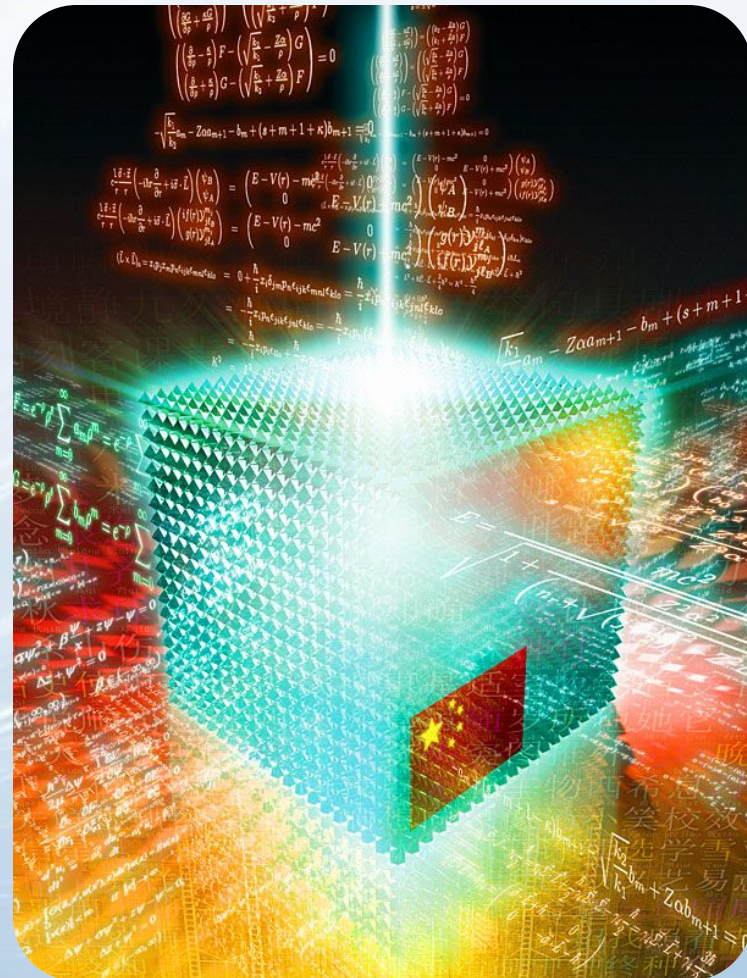
Устройство квантового компьютера

4

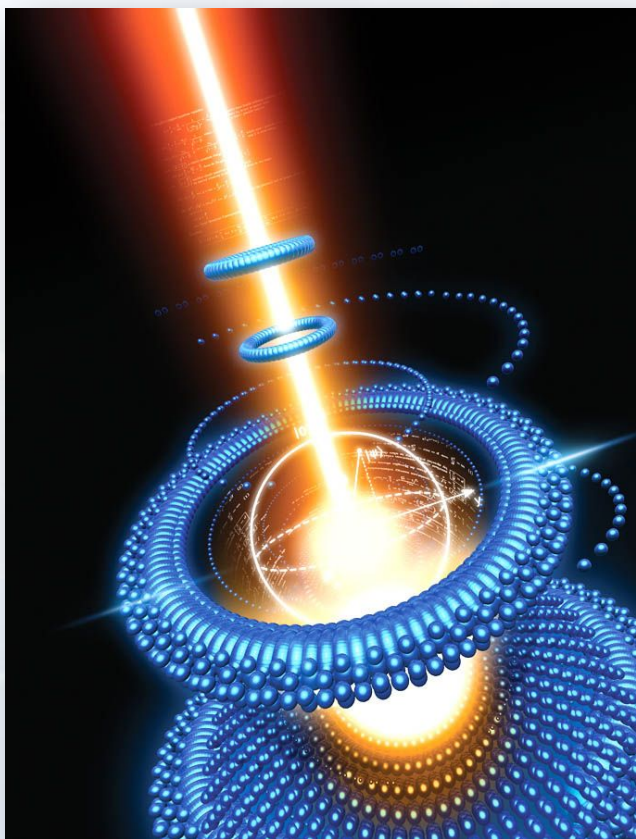
Квантовые компьютеры сегодня

5

Взгляд в будущее

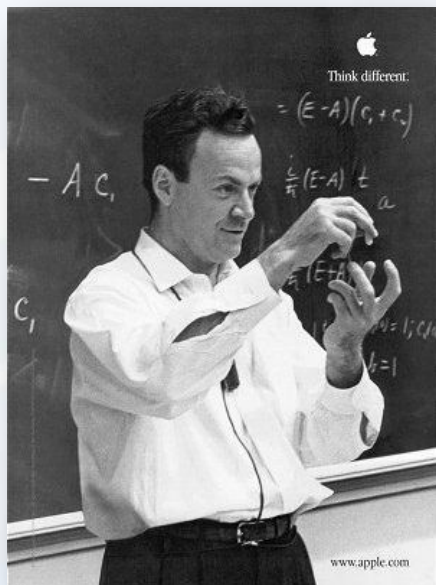


Введение



Используя законы квантовой механики, можно создать принципиально новый тип вычислительных машин, которые позволят решать некоторые задачи, недоступные даже самым мощным современным суперкомпьютерам. Резко возрастет скорость многих сложных вычислений; сообщения, посланные по линиям квантовой связи, невозможно будет ни перехватить, ни скопировать. Сегодня уже созданы прототипы этих квантовых компьютеров будущего.

Как все начиналось



- ◆ **1900 г.-** Макс Планк, открытие квантовых свойств теплового излучения;
- ◆ **1930-е гг.-** венгерский математик Джон фон Нейман обратил внимание на возможность разработки квантовой логики;
- ◆ **1980-е гг.-** начало разработки теории квантовых компьютеров (русский математик Ю.И.Манин, американский физик П.Бенев, английский ученый Д.Дойч, лауреат Нобелевской премии по физике Р.Фейнман);
- ◆ **1994 г.-** квантовый алгоритм факторизации П.Шора;
- ◆ **1996 г.-** поисковый алгоритм Л. Гровера;
- ◆ **1998 г.-** Айзек Чуанг, первый двухкубитный квантовый компьютер.

Что такое квантовый компьютер?

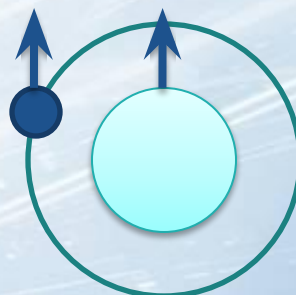
Квантовый компьютер — устройство, которое выполняет вычисления, основываясь на законах квантовой механики.

Основным элементом квантового компьютера являются квантовые биты, или **кубиты** (quantum bit, qubit).

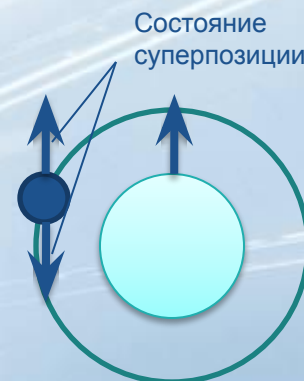
Кубит допускает два собственных состояния, обозначаемые $|0\rangle$ и $|1\rangle$, но при этом может находиться и в их суперпозиции, то есть в состоянии $A*|0\rangle + B*|1\rangle$, где A и B - любые комплексные числа, удовлетворяющие условию $|A|^2 + |B|^2 = 1$.



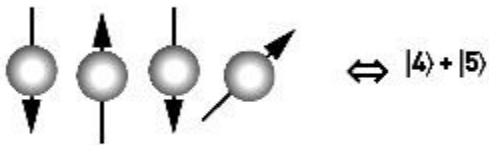
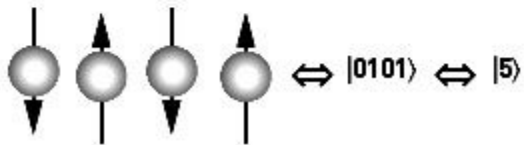
Кубит = $|0\rangle$



Кубит = $|1\rangle$



Кубит = $A*|0\rangle + B*|1\rangle$



Свойство квантовых частиц быть одновременно во многих состояниях называется **квантовым параллелизмом**

3 кубита квантового регистра против 3 битов классического

Каждый кубит может находиться в суперпозиции "классически" разрешённых состояний (верхняя картинка), потому пространство состояний регистра, состоящего всего из трёх кубитов (правая картинка), радикально "больше" единственно возможного (на каждый момент времени) состояния регистра, построенного из трёх битов классических

Classical register

101



Quantum register

000 001 010 011
100 101 110 111

Классический компьютер хранит в памяти **L бит**, которые за каждый такт работы процессора подвергаются изменению.

В квантовом компьютере в памяти (регистр состояния) хранятся значения **L кубитов**, однако квантовая система находится в состоянии, являющемся **суперпозицией** всех базовых **2^L состояний**, и изменение квантового состояния системы, производимое квантовым процессором, касается *всех 2^L базовых состояний одновременно*.

Соответственно в квантовом компьютере вычислительная мощность достигается за счет реализации **параллельных** вычислений, причем теоретически квантовый компьютер может работать в экспоненциальное число раз быстрее, чем классическая схема.



Квантовый компьютер, благодаря своим качествам, способен разложить **250-значное число** на множители не за **800 тысяч лет**, как современные самые мощные ЭВМ, а за **30 минут(!)**. С такой машиной спецслужбы могут быстро взломать любой, самый сложный шифр.

В настоящее время в исследования квантовой криптографии вкладываются большие средства, и значительная часть исследований осуществляется на средства оборонных ведомств и спецслужб.

Устройство квантового компьютера

*Схематическая структура
квантового компьютера*

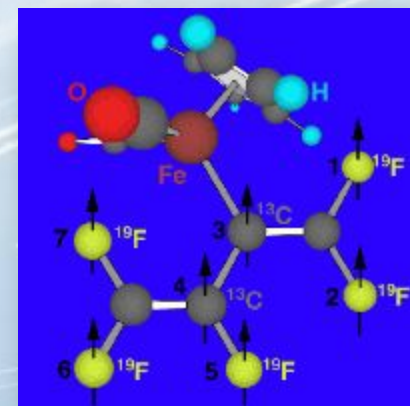
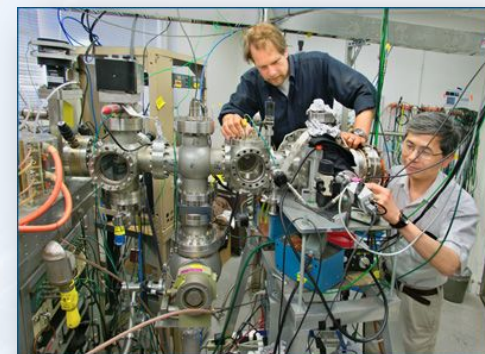


Квантовый компьютер состоит из n кубит и позволяет проводить одно- и двухкубитовые операции над любым из них (или любой парой). Эти операции выполняются под воздействием импульсов внешнего поля, управляемого классическим компьютером.

Устройство квантового компьютера

Теоретические модели квантового компьютера:

- ❖ Компьютер на основе молекул органических жидкостей и методов ядерно-магнитном резонанса для управления кубитами;
- ❖ На основе ионов, захваченных ионными ловушками;
- ❖ На основе зарядовых состояний куперовских пар;
- ❖ На основе миниатюрных сверхпроводимых колец;
- ❖ Компьютер на твердом теле.



«Сердце» квантового компьютера из 7 кубит

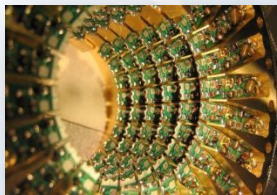
Устройство квантового компьютера

К физической системе, реализующей полномасштабный квантовый компьютер (превосходящий по производительности любой классический компьютер), предъявляются следующие требования:

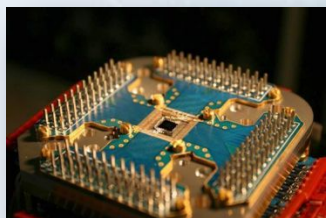
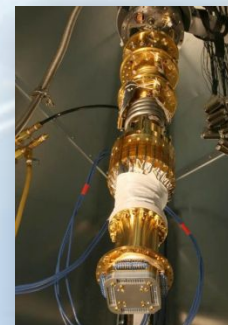
- ❖ Система состоит из точно известного числа частиц ($L > 10^3$);
- ❖ Возможность привести систему в точно известное начальное состояние;
- ❖ Степень изоляции от внешней среды должна быть очень высока;
- ❖ Обеспечение измерений с достаточно высокой надежностью состояния квантовой системы на выходе. Измерение конечного квантового состояния является одной из основных проблем квантовых вычислений.

Квантовые компьютеры сегодня

Прототипы квантовых компьютеров существуют уже сегодня. Правда, пока что экспериментально удастся собирать лишь небольшие регистры, состоящие всего из нескольких квантовых битов. К сожалению, существующие квантовые системы еще не способны обеспечить надежные вычисления, так как они либо недостаточно управляемы, либо очень подвержены влиянию шумов. Однако физических запретов на построение эффективного квантового компьютера нет, необходимо лишь преодолеть технологические трудности.



2001 г. - корпорация IBM создала управляемый ядерно-магнитным резонансом (ЯМР) квантовый компьютер из **7 кубит**, реализующий факторизацию числа 15 посредством алгоритма Шора.

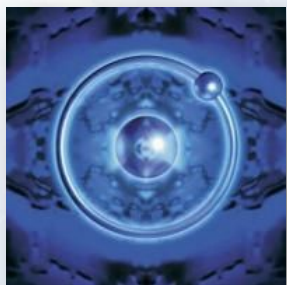
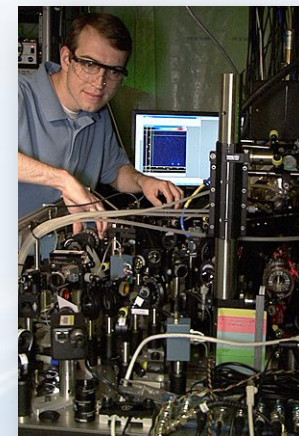


Февраль 2007 г. - Канадская компания D-Wave заявила о создании первого в истории образца коммерческого квантового компьютера, состоящего из 16 кубит. Однако информация об этом устройстве не отвечала строгим требованиям точного научного сообщения; новость не получила научного признания.

Квантовые компьютеры сегодня

Ноябрь 2009 г. - Создана модель программируемого квантового процессора.

Физики из *Национального института стандартов и технологий (США)* реализовали обширный набор «программ» на базе двух кубит, представленных ионами бериллия.

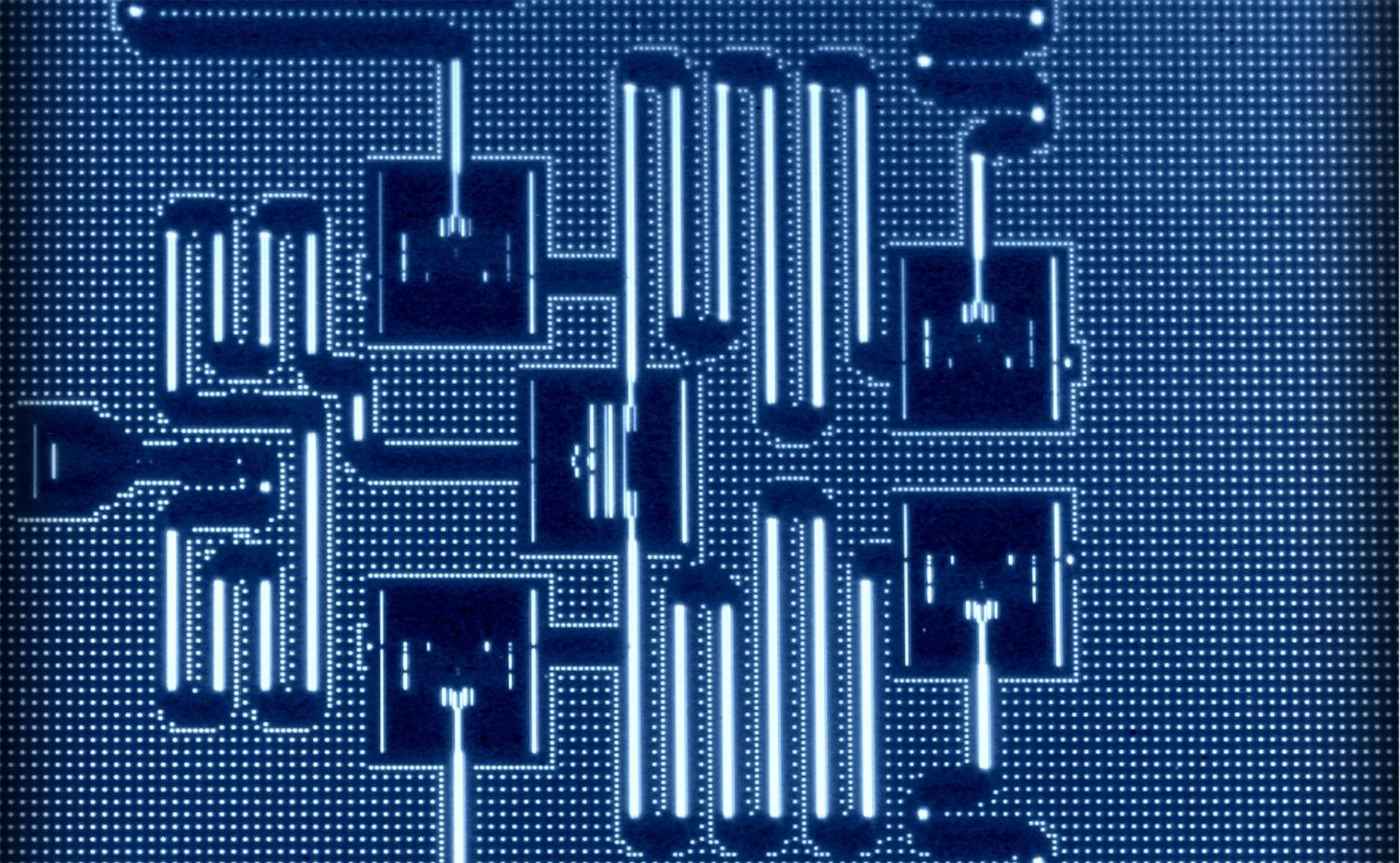


Январь 2010 г. - Примитивный квантовый компьютер был использован для расчета энергии молекулы водорода. Физикам из *Гарвардского университета (США)* и *Университета Квинсленда (Австралия)* удалось реализовать алгоритм вычисления энергии основного и возбужденных состояний молекулы H₂, задействовав в экспериментах всего два фотонных кубита.

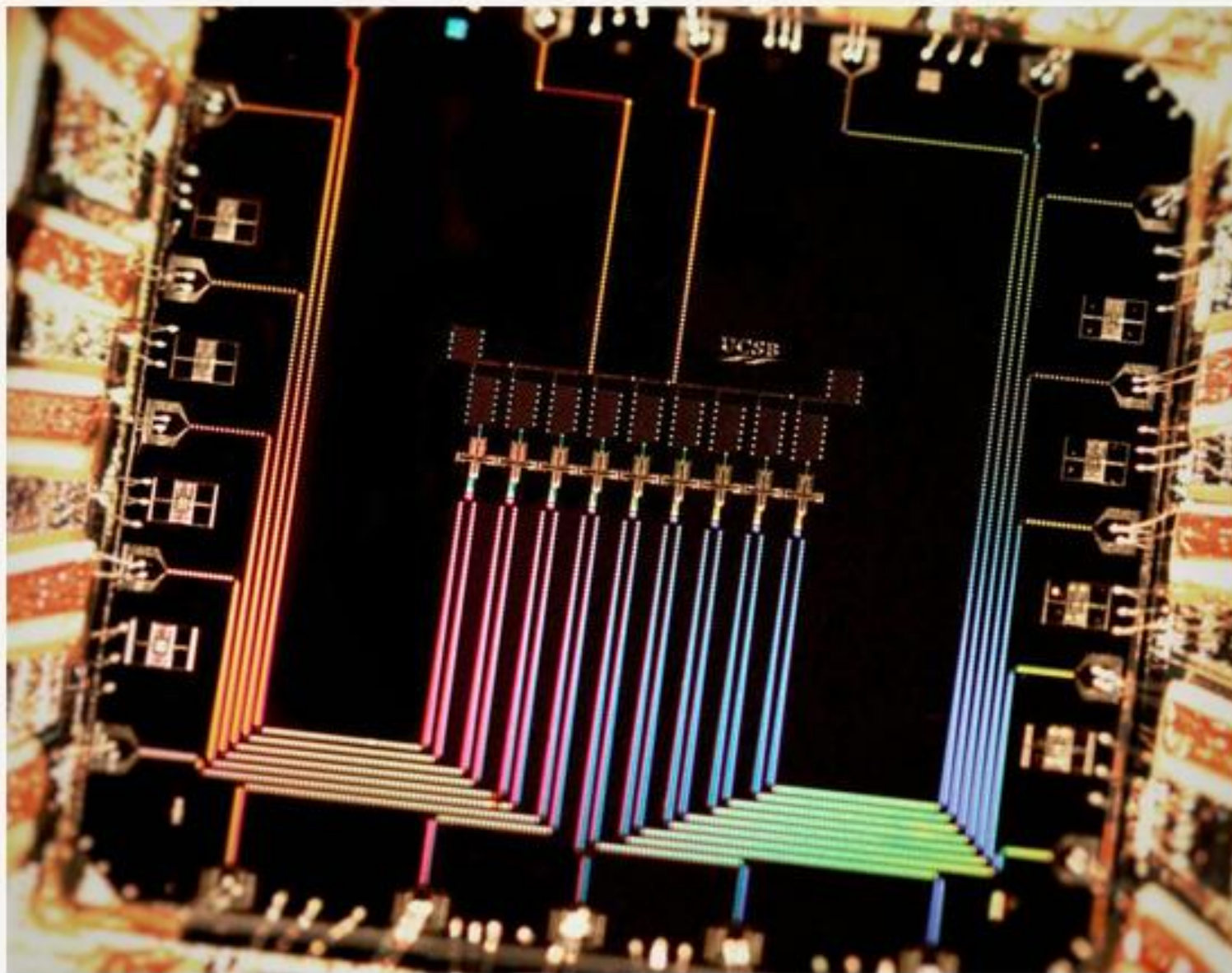
Работают над квантовыми компьютерами и в России. Институт теоретической физики им. Ландау РАН и Физико-технологический институт РАН проводят опыты с разной архитектурой квантовых компьютеров и с различными материалами.

Физики из России и США создали первый 51-кубитный квантовый компьютер

- ❖ Устройство пока является самой сложной вычислительной системой такого рода, заявил профессор Гарвардского университета, основатель Российского квантового центра (РКЦ) Михаил Лукин.
Как обнаружили российские и американские ученые, набор атомов, удерживаемых внутри специальных лазерных "клеток" и охлажденных до сверхнизких температур, можно использовать в качестве кубитов квантового компьютера, сохраняющих стабильность работы при достаточно широком наборе условий. Это позволило физикам создать пока самый большой квантовый вычислитель из 51 кубита. Используя набор подобных кубитов, команда Лукина уже решила несколько физических задач, чрезвычайно сложных для моделирования при помощи "классических" суперкомпьютеров. К примеру, российские и американские ученые смогли просчитать то, как ведет себя большое облако частиц, связанных между собой, обнаружить ранее неизвестные эффекты, возникающие внутри него. Оказалось, что при затухании возбуждения в системе могут остаться и удерживаться фактически бесконечно некоторые типы колебаний, о чем раньше ученые не подозревали.



Квантовый процессор на пяти кубитах от IBM



Квантовый процессор на девяти кубитах

Взгляд в будущее

Перспективность квантовых счислений заключается в том, что **квантовые компьютеры смогут решать целые классы задач, которые сейчас являются очень тяжелыми и трудно обрабатываемыми.**

А что же станет с классическими компьютерами? Отомрут ли они? Вряд ли. И для классических, и для квантовых компьютеров найдутся свои сферы применения.

Внедрение квантовых компьютеров не приведет к решению принципиально нерешаемых классических задач; а лишь **ускорит некоторые вычисления.** Кроме того, станет возможна **квантовая связь** - передача кубитов на расстояние, что приведет к возникновению своего рода **квантового Интернета.** Квантовая связь позволит обеспечить защищенное (законами квантовой механики) от подслушивания соединение всех желающих друг с другом. Информация, хранимая в квантовых базах данных, будет надежнее защищена от копирования, чем сейчас. Фирмы, производящие программы для квантовых компьютеров, смогут уберечь их от любого, в том числе и незаконного, копирования.

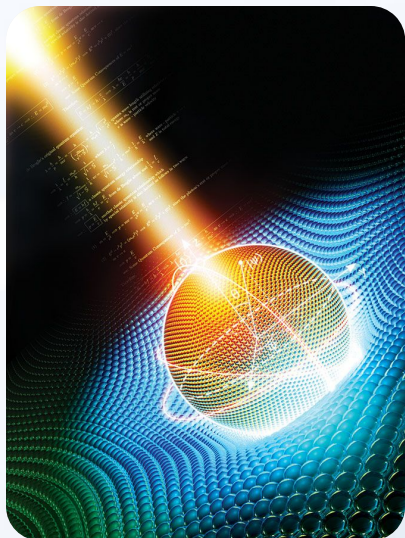
Взгляд в будущее

У квантовых компьютеров есть еще одна сфера применения, огромное значение которой понятно уже сегодня, - **создание экспертных систем нового поколения.**

Квантовый компьютер сможет не только накапливать, хранить и обрабатывать информацию, но и производить с ней операции, совершенно недоступные даже самым мощным современным компьютерам.

Создание подобной экспертной системы произведет крупнейший переворот в технике. Страна, которая первой создаст такую экспертную систему, получит уникальный шанс вырваться в лидеры в научно-технической гонке.

Появление квантовых компьютеров будет означать революцию не только в вычислительной технике, но также и в технике передачи информации, в организации принципиально новых систем связи, и может быть началом развития новых, пока неизвестных, областей Науки и Техники.



Спасибо за внимание!