МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКИЙ ИНЖЕНЕРНО ФИЗИЧЕСКИЙ ИНСТИТУТ

**(ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ)**

|  |  |
| --- | --- |
|  | Факультет КИБЕРНЕТИКИ**Кафедра «Компьютерные системы и технологии»** |

# РЕФЕРАТ

по курсу:

## Архитектура ВС

*на тему:*

**Архитектура квантовых компьютеров.**

*Студент группы К9-122 Островский А.В.*

### Москва 2001

### **Содержание**

#### **ВВЕДЕНИЕ**

#### **ГЛАВА 1: История появления теории квантовых компьютеров:**

* 1. Рождение квантовой физики;
	2. Появление теории квантовых компьютеров;
	3. Квантовая физика и квантовая информатика;

#### **ГЛАВА 2: Принципы и понятия, положенные в основу работы**

#### **квантовых компьютеров:**

* 1. Единицы квантовой информации. Кубит;
	2. Единицы квантовой информации. Квантовый регистр;
	3. Квантовая коррекция ошибок в квантовом компьютере;

**ГЛАВА 3: Архитектура квантовых копьютеров:**

* 1. Принципиальная схема квантового компьютера;
	2. Общие требования к элементной базе квантового компьютера;
	3. Основные направления в развитии элементной базы квантовых компьютеров:
		1. Квантовые компьютере на основе ионов, захваченных ионными ловушками;
		2. Квантовые компьютеры на основе молекул органических жидкостей с косвенным скалярным взаимодействием между ними и методов ядерного магнитного резонанса (ЯМР) для управления кубитами;
		3. Квантовые компьютеры на основе зарядовых состояний куперовских пар;
		4. Твердотельные ЯМР квантовые компьютеры;

##### **ГЛАВА 4: Перспективы развития квантовых компьютеров:**

* 1. Нерешенные проблемы на пути построения квантовых компьютеров;
	2. Квантовая связь и криптография;
	3. Будущее квантовых компьютеров;

###### ЗАКЛЮЧЕНИЕ

ЛИТЕРАТУРА

#### **ВВЕДЕНИЕ**

Элементная база современных информационных систем построена на лампах, транзисторах, лазерах, фотоэлементах, являющихся классическими, в том смысле, что их внешние параметры (токи, напряжение, излучение) являются классическими величинами. С этими величинами связываются информационные символы, что позволяет отображать информационные процессы на физические системы. Аналогично, информационные символы можно связать с дискретными состояниями квантовых систем, подчиняющихся уравнению Шредингера, а с их управляемой извне квантовой эволюцией связать информационный (вычислительный) процесс. Такое отображение превращает квантовую систему (частицу) в квантовый прибор. Совокупность квантовых приборов, используемых для построения квантовых информационных систем, можно назвать квантовой элементной базой.

**ГЛАВА 1. История появления теории квантовых компьютеров**

* 1. **Рождение квантовой физики.**

В канун XX века 14 декабря 1900 года немецкий физик и будущий нобелевский лауреат Макс Планк доложил на заседании Берлинского физического общества о фундаментальном открытии квантовых свойств теплового излучения. Этот день считается днем рождения квантовой теории. В физике родилось понятие *кванта* энергии и среди других фундаментальных постоянных поля вилась постоянная Планка h = 1,38062\*10-23Дж/К.

В 1925 году В.Гайзенберг предложил матричный вариант квантовой механики, а в 1926 году Э.Шредингер сформулировал свое знаменитое волновое уравнение для описания движения электрона во внешнем поле. В это же время Э.Ферми и П.Дирак получили *квантово-статистическое распределение* для электронного газа, учитывающее при заполнении отдельных квантовых состояний квантовый принцип, сформулированный тогда же В.Паули. Анализ квантовомеханической задачи о движении электрона во внешнем периодическом поле, создаваемом атомными остатками в кристаллической решетке, выполненный Ф.Блохом в 1928 году, показал, что электронный энергетический спектр в кристаллическом твердом теле имеет *зонную структуру*. Это привело к существенным изменениям наших представлений о Природе вообще и о твердом теле, в частности.

* 1. **Появление теории квантовых компьютеров.**

Кардинально новой оказалась идея о *квантовых вычисления*х, впервые высказанная советским математиком Ю.И.Маниным в 1980 году, и которая стала активно обсуждаться лишь после опубликования в 1982 году статьи американского физика-теоретика нобелевского лауреата Р.Фейнмана. Он обратил внимание на способность изолированной квантовой системы из *L* двухуровневых квантовых элементов находиться в когерентной *суперпозиции* из 2*L* булевых состояний, характеризующейся 2*L* комплексными числами и увеличенной до 2*L* размерностью соответствующего гильбертова пространства. Ясно, что для описания такого квантового состояния в классическом вычислительном устройстве потребовалось бы задать 2*L* комплексных чисел, то есть, понадобились бы *экспоненциально большие* вычислительные ресурсы. Отсюда был сделан обратный вывод о том, что эффективное численное моделирование квантовых систем, содержащих до сотни двухуровневых элементов, практически недоступно классическим компьютерам, но может эффективно осуществляться путем выполнения логических операций на квантовых системах, которые действуют на суперпозиции многих квантовых состояний.

Поскольку законы квантовой физики на микроскопическом уровне являются линейными и обратимыми, то и соответствующие квантовые логические устройства оказываются также *логически и термодинамически обратимыми*, а квантовые вычислительные операции представляются *унитарными операторами* (или матрицами 2*L* ╠ 2*L*) в 2*L*-мерном гильбертовом пространстве. Квантовые вентили аналогичны соответствующим обратимым классическим вентилям, но в отличие от классических они способны совершать *унитарные операции над суперпозициями состояний*. Выполнение унитарных логических операций предполагается осуществлять с помощью соответствующих внешних воздействий, которыми управляют классические компьютеры.

* 1. **Квантовая физика и квантовая информатика**

Возможность построения квантовых компьютеров и систем связи подтверждается современными теоретическими и экспериментальными исследованиями. Новая техника XXI в. рождается путем синтеза новых идей в математике, физике, информатике, технологии. Взаимодействие фундаментальных отраслей науки и технологии, рождающее новую технику, показано в таблице 3. Важно подчеркнуть, что в процессе решения задач квантовой информатики происходит развитие и углубление понимания основ квантовой физики, подвергаются новому анализу и экспериментальной проверке основные ее проблемы - локальности (причинности), скрытых параметров, реальности, неопределенности, дополнительности, измерений, коллапса волновой функции.


#### **ГЛАВА 2: Принципы, положенные в основу работы квантовых компьютеров**

**2.1 Единицы квантовой информации. Кубит.**

Любая классическая двухуровневая система, как и квантовая, имеет основное |0 и не основное |1 базисные состояния. Примером классической двухуровневой системы является известный в микроэлектронике инвертор, осуществляющий операцию НЕ. В зависимости от того заняты ли эти состояния с вероятностями *P*(0) = 1, *P*(1) = 0 или *P*(0) = 0, *P*(1) = 1, мы имеем *булевые логические* состояния "0" или "1".

В квантовом случае возникает намного более богатая ситуация. Волновая функция квантовых состояний двухуровневой системы - квантового бита, получившего в дальнейшем название *кубита* (quantum bit или qubit), может представлять собой *суперпозицию* базисных состояний (вектор состояния) следующего вида | = |0 + |1, где , - комплексные амплитуды состояний, при этом ||2 + ||2 = 1. Помимо вероятностей *P*(0) = ||2 и *P*(1) = ||2, заполнения базисных состояний |0 и |1, состояние кубита характеризуется *когерентными* или *интерференционными* слагаемыми в вероятности состояния |, определяемых произведениями комплексных амплитуд \* и \*. Состояние квантового бита в отличие от классического может изменяться не только путем изменения вероятностей *P*(0) и *P*(1), но и более тонко путем изменения амплитуд состояний  и , что соответствует поворотам вектора состояния | в так называемом гильбертовом двухмерном пространстве состояний. В этом и состоит принципиальное различие классического и квантового бита.

Двум значениям кубита могут соответствовать, например, основное и возбужденное состояния атома, направления вверх и вниз спина атомного ядра, направление тока в сверхпроводящем кольце, два возможных положения электрона в полупроводнике, различающихся поляризацией фотона или фазой сверхпроводника. Квантовая система может быть макроскопической (сверхпроводники, сверхтекучие жидкости, бозе-газ), отдельной атомной частицей или колебательной модой:

Простейшим случаем двухуровневой квантовой системы является спин ядра атома или электрона **I = ½** в постоянном внешнем поле ***B*0**: два уровня энергии и состояния соответствуют проекциям спина на направление ***B*0** (рис. 1).

*Рис. 1.* Состояния спина ***I*z = ±½** - и его уровни энергии ***E*0,1 = ±i*B*0/2**
во внешнем поле ***B*0** представляют логические состояния кубита **|0>** и **|1>**

Два оптических уровня энергии и состояния электрона в ионе также могут быть выбраны в качестве двух состояний кубита (рис. 2).

*Рис. 2*. Состояния иона **Са+**, соответствующие уровням энергии **2*S*1/2** (основной) и **2*D*5/2** (метастабильный) выбраны за логические **|0>** и **|1>**. Числа у стрелок показывают длину волны лазера, вызывающего переход, и время жизни иона на соответствующем уровне

**2.2 Единицы квантовой информации. Квантовый регистр.**

Квантовый регистр устроен почти так же, как и классический. Это цепочка квантовых битов, над которыми можно проводить одно- и двухбитовые логические операции (подобно применению операций НЕ, 2И-НЕ и т.п. в классическом регистре).

*Рис. 3*. Квантовый регистр - цепочка квантовых битов. Одно- или двухкубитовые квантовые вентили (NOT 1/2, NOT, CNOT и др.) осуществляют логические операции над кубитами или парами кубитов.

К базовым состояниям квантового регистра, образованного L кубитами, относятся, так же как и в классическом, все возможные последовательности нулей и единиц длиной L. Всего может быть 2L различных комбинаций. Их можно считать записью чисел в двоичной форме от 0 до 2L-1 и обозначать 0,1,2,3, ... 2L-1. Однако эти базовые состояния не исчерпывают всех возможных значений квантового регистра (в отличие от классического), поскольку существуют еще и состояния суперпозиции, задаваемые комплексными амплитудами, связанными условием нормировки. Классического аналога у большинства возможных значений квантового регистра (за исключением базовых) просто не существует. Состояния классического регистра - лишь жалкая тень всего богатства состояний квантового компьютера.

Представим, что на регистр осуществляется внешнее воздействие, например, в часть пространства поданы электрические импульсы или направлены лазерные лучи. Если это классический регистр, импульс, который можно рассматривать как вычислительную операцию, изменит L переменных. Если же это квантовый регистр, то тот же импульс может одновременно преобразовать до 2L переменных. Таким образом, квантовый регистр, в принципе, способен обрабатывать информацию в 2L / L раз быстрее по сравнению со своим классическим аналогом. Отсюда сразу видно, что маленькие квантовые регистры (L<20) могут служить лишь для демонстрации отдельных узлов и принципов работы квантового компьютера, но не принесут большой практической пользы, так как не сумеют обогнать современные ЭВМ, а стоить будут заведомо дороже. В действительности квантовое ускорение обычно значительно меньше, чем приведенная грубая оценка сверху (это связано со сложностью получения большого количества амплитуд и считывания результата), поэтому практически полезный квантовый компьютер должен содержать тысячи кубитов. Но, с другой стороны, понятно, что для достижения действительного ускорения вычислений нет необходимости собирать миллионы квантовых битов. Компьютер с памятью, измеряемой всего лишь в килокубитах, будет в некоторых задачах несоизмеримо быстрее, чем классический суперкомпьютер с терабайтами памяти.

**2.3 Квантовая коррекция ошибок в квантовом компьютере**

В самом начале развития идей о квантовом компьютере физики обнаружили и грозного противника этой машины. Имя этого противника –*декогерентизация*. Кубиты компьютера нельзя полностью изолировать от внешнего мира: кубиты работают в условиях шумового воздействия внешней среды. Флуктуации напряжений на электродах, шумовые токи, неточности выполнения самих импульсных воздействий на кубиты в ходе вычислительного процесса - все это вносит неконтролируемые ошибки в фазы и амплитуды состояний кубитов в ходе вычислительного процесса. По истечении времени, равном времени декогерентизации квантовых состояний системы кубитов, контролируемый вычислительный процесс прекратится, эволюция квантового компьютера приобретет случайный (диффузионный) характер. Время декогерентизации, как правило, будет меньше времени, необходимого для выполнения сложного алгоритма, состоящего из большого числа (-109) вентилей.

Выход из этой, казавшейся тупиковой, ситуации был найден в применении методов квантовой коррекции ошибок. Методы коррекции ошибок хорошо известны из теории обычных (классических) компьютеров. Смысл их в том, что логические **|0>** и **|1>** кодируются большим числом битов; анализ кодовых комбинаций позволяет найти и удалить ошибку. Эти методы удалось разработать в квантовом варианте, где ошибки могут быть фазовыми и амплитудными. Выяснилось, что если вероятность ошибки при выполнении одной элементарной операции ниже некоторого порогового уровня, вычислительный процесс можно длить сколь угодно долго. Это означает, что операции квантовой коррекции ошибок удаляют из компьютера больше ошибок, чем вносят. Этот вывод очень важен: по существу, он имеет силу теоремы существования полномасштабного квантового компьютера.

**ГЛАВА 3: Архитектура квантовых компьютеров**

**3.1 Принципиальная схема квантового компьютера**

*Квантовые методы* выполнения вычислительных операций, а также передачи и обработки информации, уже начинают воплощаться в реально функционирующих экспериментальных устройствах, что стимулирует усилия по реализации квантовых компьютеров. Квантовый компьютер состоит из n кубитов 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.

Принципиальная схема работы любого квантового компьютера может быть представлена следующим образом (рис.4). Основной его частью является квантовый регистр - совокупность некоторого числа *L* кубитов. До ввода информации в компьютер все кубиты регистра должны быть приведены в основные базисные (булевые) состояния. Эта операция называется подготовкой начального состояния или *инициализацией* (initializing). Далее каждый кубит подвергается селективному воздействию, например, с помощью импульсов внешнего электромагнитного поля, управляемых классическим компьютером, которое переведет основные базисные состояния определенных кубитов в не основное состояния |0  |1. При этом состояние всего регистра перейдет в суперпозицию базисных состояний вида |*n* = |*n*1,*n*2,*n*3,...*n*L, где *n*i = 0,1.

*(Рис. 4) – схематическая структура квантового компьютера*

При вводе информации в квантовый компьютер состояние входного регистра, с помощью соответствующих импульсных воздействий преобразуется в соответствующую когерентную суперпозицию базисных ортогональных состояний. В таком виде информация далее подвергается воздействию квантового процессора, выполняющего последовательность квантовых логических операций, определяемую унитарным преобразованием, действующим на состояние всего регистра. К моменту времени *t* в результате преобразований исходное квантовое состояние становится новой суперпозицией, которая и определяет результат преобразования информации на выходе компьютера.

Совокупность всех возможных операций на входе данного компьютера, формирующих исходные состояния, а также осуществляющих унитарные локальные преобразования, соответствующие алгоритму вычисления, способы подавления потери когерентности - так называемой *декогерентизации* (decoherence) квантовых состояний и исправления случайных ошибок, играют здесь ту же роль, что и *"программно*е *обеспечение"* (software) в классическом компьютере.

**3.2 Общие требования к элементной базе квантового компьютера**

При выборе конкретной схемы любого квантового компьютера необходимо решить три вопроса: во-первых, выбрать физическую систему, представляющую требуемую систему кубитов, во вторых, определить физический механизм, определяющий взаимодействие между кубитами, необходимое для выполнения двухкубитовых операций, в третьих, определить способы селективного управления кубитами и измерения их состояния на выходе. Все это вместе взятое аналогично *"аппаратному обеспечению"* (hardware) классического компьютера.

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

1. Физическая система, представляющая полномасштабный квантовый компьютер, должна содержать достаточно *большое* число *L* > 103 хорошо различаемых кубитов для выполнения соответствующих квантовых операций.
2. Необходимо обеспечить условия для приготовления входного регистра в исходном основном базисном состоянии |01,02,03,...0L, то есть возможность процесса *инициализации*.
3. Необходимо обеспечить максимальное подавление эффектов декогерентизации квантовых состояний, обусловленное взаимодействием системы кубитов с окружающей средой, что приводит к разрушению суперпозиций квантовых состояний и может сделать невозможной выполнение квантовых алгоритмов. Время декогерентизации должно, по крайней мере, в 104 раз превышать время выполнения основных квантовых операций (времени такта). Для этого система кубитов должна быть достаточно *слабо* связана с окружением.
4. Необходимо обеспечить за время такта выполнение требуемой совокупности квантовых логических операций, определяющей унитарное преобразование. Эта совокупность должна содержать определенный набор только *двухкубитовых* операций, типа контролируемый инвертор или контролируемое НЕ (Controlled NOT  CNOT) (аналог исключающего ИЛИ в классических компьютерах), осуществляющих операции поворота вектора состояния двух взаимодействующих кубитов в четырехмерном гильбертовом пространстве, и *однокубитовых* операций, осуществляющих поворот вектора состояния кубита в двухмерном гильбертовом пространстве, таких как операции НЕ, Адамара и некоторые другие.
5. Необходимо обеспечить с достаточно высокой надежностью *измерение* состояния квантовой системы на выходе. Проблема измерения конечного квантового состояния является одной из основных проблем квантовых вычислений.

**3.3 Основные направления в развитии элементной базы квантовых компьютеров**

***3.3.1 Квантовые компьютере на основе ионов, захваченных ионными ловушками***

Взаимодействие между заряженными ионами в одномерной цепочке этих ловушек осуществляется посредством возбуждения их коллективного движения, а *индивидуальное* управление ими с помощью лазеров инфракрасного диапазона. Первый прототип квантового компьютера на этих принципах был предложен австрийскими физиками И.Цираком и П.Цоллером в 1995 году. В настоящее время интенсивные экспериментальные работы ведутся в Los Alamos Natl.Lab. (LANL) и Natl.Inst.Stand.Tech. (NIST) в США. Преимущество такого подхода состоит в сравнительно простом индивидуальном управлении отдельными кубитами. Основными недостатками этого типа квантовых компьютеров являются необходимость создания сверхнизких температур, обеспечение устойчивости состояний ионов в цепочке и ограниченность возможного числа кубитов значением *L* < 40.

***3.3.2 Квантовые компьютеры на основе молекул органических жидкостей с косвенным скалярным взаимодействием между ними и методов ядерного магнитного резонанса (ЯМР) для управления кубитами:***

В предложенном способе построения квантового компьютера кубитами выступают спины - ядер водорода (протоны) и углерода 13С в молекулах жидкости. Так, в молекуле трихлорэтилена (рис. 5) спины ядер двух атомов 13С и одного протона образуют три кубита. Два атома 13С химически неэквивалентны и поэтому имеют различные частоты ядерного магнитного резонанса **A** и **B** в заданном внешнем постоянном магнитном поле ***B*0**, протон будет иметь третью резонансную частоту **C**. Подавая импульсы внешнего переменного магнитного поля на частотах (ид, tog, о)с, мы селективно управляем квантовой эволюцией любого из этих спинов (выполняем однокубитовые вентили). Между спинами ядер, разделенных одной химической связью 1H-13С и 13С-13С, имеется магнитное контактное взаимодействие, что позволяет построить двухкубитовые вентили.

 *Рис. 5. –* схема ансамблевого ядерно магнитнорезонансного квантового компьютера

Главным преимуществом такого компьютера является то, что огромное число практически независимых молекул-компьютеров жидкости действует, обеспечивая тем самым возможность управления ими с помощью хорошо известных в технике ядерного магнитного резонанса (ЯМР) операций над макроскопическим *объемом* жидкости. Последовательности радиочастотных импульсов, выполняющие в этом случае роль определенных квантовых логических вентилей, осуществляют глобальные унитарные преобразования состояний соответствующих ядерных спинов для всех молекул-компьютеров. Индивидуальное обращение к отдельным кубитам заменяется одновременным обращением к соответствующим кубитам во всех молекулах большого ансамбля. Компьютер такого рода получил название *ансамблевого* (bulk-ensemble quantum computer) *ЯМР квантового компьютера*. Замечательно, что он может в принципе работать при *комнатной температуре*. Время декогерентизации квантовых состояний ядерных спинов в жидкости достаточно велико. Оно может составлять несколько секунд.

В области ЯМР квантовых компьютеров на органических жидкостях к настоящему времени достигнуты наибольшие успехи. Они связаны в основном с хорошо развитой импульсной техникой ЯМР-спектроскопии, обеспечивающей выполнение различных операций над когерентными суперпозициями состояний ядерных спинов и с возможностью использования для этого стандартных ЯМР-спектрометров, работающих при комнатных температурах.

Экспериментально на ЯМР квантовых компьютерах были осуществлены алгоритм Гровера поиска данных, квантовое фурье-преобразование, квантовая коррекция ошибок, квантовая телепортация, квантовое моделирование и другие операции.

Основными ограничениями для этого направления являются:

1. Смешанный характер исходного состояния кубитов, что требует использования определенных неунитарных операций для приготовления начального состояния.
2. Измеряемый на выходе сигнал экспоненциально убывает с ростом числа кубитов *L*.
3. Число ядерных спинов-кубитов в отдельной молекуле с достаточно различающимися резонансными частотами *L* ограничено.
4. Однокубитовые и двукубитовые квантовые операции являются относительно медленными.

Эти ограничения приводят к тому, что ЯМР квантовые компьютеры на молекулах органической жидкости не смогут иметь число кубитов, значительно больше десяти. Их следует рассматривать лишь как прототипы будущих квантовых компьютеров, полезные для отработки принципов квантовых вычислений и проверки квантовых алгоритмов.

***3.3.3 Квантовые компьютеры на основе зарядовых состояний куперовских пар:***

Данный принцип построения квантовых компьютеров основан на использовании в качестве кубитов *зарядовых состояний куперовских пар* в квантовых точках, связанных переходами Джозефсона, предложенное Д.В.Авериным в 1998 году.

Первый твердотельный кубит на этих принципах был создан в NEC Fund.Res.Lab. в Японии в 1999 году. Полагают, что перспективность этого направления состоит в возможности создания электронных квантовых устройств высокой степени интеграции на одном кристалле, при этом для управления кубитами не потребуются громоздкие лазерные или ЯМР установки. Однако на пути создания квантовых компьютеров еще остается нерешенными ряд важных проблем и, в частности, проблема устойчивости состояний кубитов и декогерентизация. Поисковые работы квантовым компьютерам на высокотемпературных сверхпроводниках в России ведутся в Институте теоретической физики им. Л.Д.Ландау РАН

***3.3.5 Твердотельные ЯМР квантовые компьютеры:***

Важные перспективы открываются перед направлением *твердотельных* ЯМР квантовых компьютеров.

Для этого в 1998 г. австралийским физиком Б.Кейном было предложено использовать в качестве кубитов обладающие ядерным спином 1/2 донорные атомы с изотопами 31P, которые имплантируются в кремниевую структуру, Это предложение, которое пока остается нереализованным, открывает потенциальную возможность создания квантовых вычислительных устройств с практически неограниченным числом кубитов.

В рассматриваемом варианте предполагается использовать температуры достаточно низкие для того, чтобы электроны донорных атомов занимали только нижнее спиновое состояние в магнитном поле. В полях *B*  2 Тл это соответствует температурам *T*  0,1 K, гораздо более низким, чем температура вымораживания электронных состояний доноров, которые будут поэтому оставаться в неионизированном основном орбитальном S-состоянии.

Каждый донорный атом с ядерным спином - кубит в полупроводниковой структуре предполагается расположить регулярным образом с достаточной точностью под "своим" управляющим металлическим затвором (затвор **A**), отделенным от поверхности кремния тонким диэлектриком (например, окисью кремния толщиной порядка нескольких нанометров). Эти затворы образуют линейную решетку произвольной длины с периодом *l* (Рис. 6.).

*Рис. 2. Схематическое изображение двух ячеек полупроводниковой структуры модели Кейна, lA ~ 10 нм, l ~ 20 нм, c ~ 20 нм.*

С помощью электрического поля, создаваемого потенциалом затворов **A**, можно изменять распределение электронной плотности вблизи ядра в основном состоянии, изменяя, соответственно, резонансную частоту каждого ядерного спина, которая определяется сверхтонким взаимодействием его с электронным спином. Это позволяет осуществлять *индивидуальное* управление квантовыми операциями путем селективного воздействия резонансных радиочастотных импульсов на ядерные спины определенных доноров.

Величиной косвенного взаимодействия между ядерными спинами соседних доноров, которое обеспечивает выполнение двухкубитовых операций, предлагается управлять с помощью затворов **J**, расположенных между затворами **A**. Это возможно, если характерные размеры полупроводниковой структуры лежат в *нанометровой* области. Для формирования таких структур предполагается воспользоваться приемами современной нанотехнологии, в частности, методами эпитаксиального выращивания, сканирующей зондовой нанолитографией в сверхвысоком вакууме на основе сканирующих туннельных и атомных силовых микроскопов, электронно-лучевой и рентгеновской литографией.

Для того чтобы исключить взаимодействие ядерных спинов доноров с окружением сам кремний и окисел кремния должен быть достаточно хорошо очищен от изотопа 29Si, обладающего спином *I* = 1/2, который содержится в количестве 4,7% в естественном кремнии. Возможно использование и других материалов.

Были предложены и несколько вариантов измерения состояний кубитов, но ни один из них пока не реализован, а также ансамблевые варианты твердотельных ЯМР квантовых компьютеров. В России работы в этом направлении ведутся в Физико-технологическом институте РАН.

**ГЛАВА 4: Перспективы развития квантовых компьютеров**

**4.1 Нерешенные проблемы на пути построения квантовых компьютеров**

Среди нерешенных проблем отметим следующие: в настоящее время отсутствует практическая разработка методов квантовых измерения состояний отдельного ядерного спина или их малых групп, не изучено влияние неидеальности управляющих кубитами импульсных последовательностей и многоуровневой сверхтонкой структуры энергетического спектра на декогерентизацию квантовых состояний, не разработаны способы подавления декогерентизации, определяемой шумами в электронной измерительной системе, не опробованы квантовые методы коррекции ошибок для многокубитовых систем.

Прототипы квантовых компьютеров существуют уже сегодня. Правда, пока что экспериментально удается собирать лишь небольшие регистры, состоящие всего из нескольких квантовых битов. Так, недавно группа, возглавляемая американским физиком И. Чангом (IBM), объявила о сборке 5-битового квантового компьютера. Несомненно, это большой успех. 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.

**4.2 Квантовая связь и криптография**

Из обширной области разработки квантовых методов связи и криптографии мы коснемся последствий создания квантовых компьютеров и систем связи для двух современных наиболее популярных криптосистем: для системы с открытым ключом (RSA система, Rivest, Sharnir, Adieman, 1977) и системы с ключом одноразового пользования (Vernam, 1935).

Сразу отметим, что в основе системы RSA лежит предположение о том, что решение математической задачи о разложении больших чисел на простые множители на классических компьютерах невозможно; оно требует экспоненциально большого числа операций и астрономического времени.

Квантовый алгоритм Шора дает возможность вычислить простые множители больших чисел за практически приемлемое время и взломать шифры RSA криптосистем. Расчеты показывают, что с использованием даже тысячи современных рабочих станций и лучшего из известных на сегодня вычислительных алгоритмов одно 250-значное число может быть разложено на множители примерно за 800 тысяч лет, а 1000-значное - за 1025(!) лет. (Для сравнения возраст Вселенной равен ~1010 лет.), в то время как согласно оценкам, квантовый компьютер с памятью объемом всего лишь около 10 тысяч квантовых битов способен разложить 1000-значное число на простые множители в течение всего нескольких часов! Таким образом, для RSA криптосистем квантовый компьютер - плохая новость.

Для криптосистем с ключом одноразового пользования квантовые методы связи оказываются хорошей новостью: они позволяют обнаружить наличие подслушивания при передаче ключа. Эта возможность основана на квантовом принципе неопределенности Гейзенберга, который гласит, что измерение изменяет состояние измеряемой квантовой системы. Пусть ключ передается по световолокну с помощью фотонов, и информация закодирована в поляризации фотонов. Тогда подслушивание заключается в перехвате и измерении поляризации пересылаемых фотонов; после измерения они пересылаются адресату. При наличии подслушивания адресат обнаружит, что 25% фотонов приходят к нему с "неправильной" поляризацией. Если этих ошибок нет, то передача ключа не подслушивается, и им можно пользоваться. Таким образом, квантовые методы обеспечивают гарантированную секретность ключа одноразового пользования. Эксперименты по передаче ключа выполнены на расстояния до 40 км.

Квантовые каналы связи дают и другие возможности.

1. С помощью одного кубита можно передавать 2 бита информации ("плотное квантовое кодирование").

2. Возможна передача неизвестного квантового состояния ("квантовая телепортация") по классическому каналу, если абоненты связи предварительно поделили коррелированную пару квантовых частиц. Потенциальные возможности применения этих феноменов еще не выяснены

* 1. **Будущее квантовых компьютеров**

Можно ожидать, что в будущем появятся также комбинированные варианты твердотельных квантовых компьютеров, использующих, например, в одной структуре и ядерные спины, и квантовые точки с электронными спинами, а также комбинированные методы обращения к кубитам, такие как двойной электрон-ядерный магнитный резонанс, динамическая поляризация ядерных спинов и оптическое детектирование ядерного магнитного резонанса.

Таким образом, весьма возможно, что в перспективе квантовые компьютеры будут изготавливаться с использованием традиционных методов микроэлектронной технологии и содержать множество управляющих электродов, напоминая современный микропроцессор. Для того чтобы снизить уровень шумов, критически важный для нормальной работы квантового компьютера, первые модели, по всей видимости, придется охлаждать жидким гелием. Вероятно, первые квантовые компьютеры будут громоздкими и дорогими устройствами, не умещающимися на письменном столе и обслуживаемыми большим штатом системных программистов и наладчиков оборудования в белых халатах. Доступ к ним получат сначала лишь государственные структуры, затем богатые коммерческие организации. Но примерно так же начиналась и эра обычных компьютеров.

А что же станет с классическими компьютерами? Отомрут ли они? Вряд ли. И для классических, и для квантовых компьютеров найдутся свои сферы применения. Хотя, по всей видимости, соотношение на рынке будет все же постепенно смещаться в сторону последних.

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. Ваша 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.

**ЗАКЛЮЧЕНИЕ**

Окончательный вывод о том, какие из вариантов окажутся в конце концов реализованными в полномасштабном квантовом компьютере сейчас сделать пожалуй не представляется возможным. Для этого предстоит преодолеть еще много уже известных и еще неизвестных трудностей. Однако, в любом случае появление квантовых компьютеров будет означать революцию не только в вычислительной технике, но также и в технике передачи информации, в организации принципиально новых систем связи типа квантового Интернета и может быть началом развития новых пока неизвестных областей Науки и Техники.

Новая техника XXI века рождается путем синтеза новых идей в математике, физике, информатике, технологии. Исключительные возможности квантовых компьютеров будут способствовать и еще более глубокому пониманию физических законов в Природе. Построение квантовых компьютеров было бы еще одним подтверждением принципа неисчерпаемости Природы: Природа имеет средства для осуществления любой корректно сформулированной задачи.

*Список использованной литературы:*

1. Вестник РАН, 2000, т.70, N.8

2. Материалы Интернет-сайта www.ibmh.msk.su

3. Материалы Интернет-сайта Физико-Технологического Института РАН www.qc.ipt.ac.ru