Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Казанский национальный исследовательский технологический
университет»

«НАУКА БЕЗ ГРАНИЦ»

Номинация «Просто о сложном»

# Научно – исследовательская работа
# «Квантовый компьютер»

Выполнили: Масальский Егор Алексеевич
студент 701 группы
Шарафутдинов Ильяс Ильнурович
Студент 914 группы
Казанского технологического колледжа
г. Казани
Научный руководитель:
преподаватель истории Каримуллина Камилла Эмилевна

Казань, 2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ ..... 3
1 ИСТОРИЯ РАЗВИТИЯ КВАНТОВОЙ ФИЗИКИ ..... 4
2 РАЗВИТИЕ КВАНТОВОГО КОМПЬЮТЕРА ..... 6
3 ОСНОВОПОЛАГАЮЩИЕ КВАНТОВЫХ МАШИН ..... 8
3.1 Квантовые компьютерные системы ..... 8
3.2 Кубит ..... 10
3.3 Суперпозиция ..... 11
3.4 Запутанность ..... 12
3.5 Декогеренция ..... 13
3.6 Квантовое превосходство ..... 14
4 СИМУЛЯТОРЫ КВАНТОВЫХ КОМПЬЮТЕРОВ ..... 16
5 АЛГОРИТМ ШОРА И УРАВНЕНИЕ ШРЕНДИНГЕРА ..... 19
6 ИМИТАЦИЯ И ВИЗУАЛИЗАЦИЯ ЭЛЕМЕНТОВ КВАНТОВОГО КОМПЬЮТЕРА С ПОМОЩЬЮ ИГРЫ ..... 20
6.1 Лазер ..... 20
6.2 Детектор ..... 21
6.3 Мина (ошибка) ..... 22
6.4 Зеркало ..... 22
6.5 Разделитель луча ..... 23
6.6 Применение элементов в игре ..... 25
7 ПРИМЕНЕНИЕ КВАНТОВЫХ ВЫЧИСЛЕНИЙ ..... 27
ЗАКЛЮЧЕНИЕ ..... 29
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ ..... 30

# ВВЕДЕНИЕ

Насколько можно повысить производительность компьютера? Согласно закону Мура, если производительность продолжает улучшаться с помощью технологических инноваций, которые были сделаны за последние несколько десятилетий, количество транзисторов на микросхеме может удваиваться каждые 18 месяцев. Кроме того, тактовая частота процессора может достигать 40 ГГц в течение 10 лет. К тому времени один атом может представлять один бит. Одна из возможных проблем может заключаться в том, что, поскольку электроны описываются не классической физикой, а квантовой механикой, квантово-механическое явление может привести к “туннелированию” происходящие на чипе. В таких случаях электроны могут вытекать из цепей. Принимая во внимание квантово-механические характеристики уровня один атом на бит, квантовые компьютеры были предложены в качестве одного из способов эффективного решения этой проблемы.

Квантовый компьютер – вычислительное устройство, которое использует квантово-вычислительную логику, для передачи, обработки, хранения информации данных. И использует он не обычные биты, такие как 0 и 1, а кубиты, которые благодаря суперпозиции имею сразу и 0 и 1, что по теории дает невероятную скорость вычисления алгоритма, а точнее мгновенно перебирать все возможные исходы.

Таким образом, квантовые компьютеры могут быть использованы для решения определенных вычислительно сложных задач, когда классические компьютеры требуют большого количества времени обработки.

Квантовые компьютеры часто понимают. Когда люди слышат слово «компьютер», они думают о ноутбуках или телефонах, но дело в том, что эти устройства и даже самые большие суперкомпьютеры в мире работают по одной и той же фундаментальной схеме. В использованных источниках и литературе квантовые компьютеры имеют фундаментальные отличия и их нельзя называть компьютерами в привычном понимании этого слова.

# 1 ИСТОРИЯ РАЗВИТИЯ КВАНТОВОЙ ФИЗИКИ

История развития квантовой физики начинается в 1900 году 14 декабря, благодаря открытию Макса Планка. В то время была проблема, ультрафиолетовой катастрофы - парадокс, в котором, полная энергия теплового излучения, по закону Рэлея, должна быть бесконечной, чего не может быть. Планк как занялся ее решением, вывел формулу для распределения энергии (E = h v), и ввел знаменитый квант действия, постоянную планка, h. Чем и спонсировал развитие квантовой физики. Работу планка продолжил великий немецкий ученый Альберт Эйнштейн, он воспользовался открытием Планка для решения некоторых аспектов фотоэффекта - это взаимодействия света или электромагнитного излучения с веществом, при котором энергия передается мелкими порциями (квантами) электронам веществах. Есть внешний и внутренний фотоэффект. Внешний - это когда фотоны попадают в металл или полупроводник, и передают свою энергию электронам. Часть энергии уходит, для освобождения электрона от атомной связи и позволяет ему уйти с поверхности металла, а остаток уходит на ускорение электрона (формула соотношения энергий: h * f = Ekin + Wa). Внутренний - возникает в полупроводниках — материалах, электропроводность которых меньше, чем у проводников, и больше, чем у изоляторов. Тут действие фотонов схоже с внешним фотоэффектом, только вот тут благодаря обогащению энергией фотонов, электроны меняют свое состояние и способны проводить электрический ток. Этот эксперимент подтвердил карпоскулярное свойство света.

Дальше по графику идет Нильс Бор, со своей теорией атома. Он предполагал, кванты излучаются лишь при переходе с одной орбиты атома на другую. И вывел формулу энергии кванта hv= Ен – Ек. где Ен и Ек - энергия электрона на его начальной и конечной орбитах. Там есть два постулата, которые гласят что о существование стационарных состояний, и об излучательных переходов с орбит. Но вскоре эту теорию опровергли, так как результаты эксперимента расходились с теорией, и она не могла полностью уточнить природу излучения. Но благодаря этой “неудачной теории” ученик бора Вернер Гейзенберг, анализируя недочеты учителя,

воссоздал новую теорию квантов – квантовую механику. Вскоре появилась новая особенность квантовой теории, которая была заслугой Луи де Бройля. Который выдвинул гипотезу о волновой природе материи, если электромагнитные волны, такие как свет ведут себя на подобии частицы, что доказал Эйнштейн, то электрон, может вести себя как электрическая волна, что переворачивала взгляд на квантовый мир и мир в целом. В формулировке де Бройля частота, соответствующая частице, связана с её энергией, как в случае фотона (частицы света), но предложенное де Бройлем математическое выражение было эквивалентным соотношением между длиной волны, массой частицы и её скоростью (импульсом). Существование электронных волн было экспериментально доказано в 1927 г. Так же под впечатлениями прочитанных комментариев Эйнштейна над работами де Бройля, Эрнест Шредингер попытался применить волновое представление электронов к квантовой последовательной теории. Он предпринял попытку связать квантовую физику и классическую, путем долгих математических описаний волн, но он потерпел неудачу в 1925 г. Скорость электронов в теории Шредингера требовали включения СТО, и учитывание предсказываемого ею значительного увеличения массы электрона при очень больших скоростях. Одна из основоположных причин провала было выпусканием из вида спина. Позже он исправил ошибки прошлого, путем подставления малых скоростей, что поспособствовало отпаданию СТО, благодаря этому он получил волнове уравнение, которое назвали в честь ученого. Данные вычисления оказали влияние на развитие квантовой теории. В настоящее время волновая функция лежит в основе квантово-механического описания микросистем, подобно уравнениям Гамильтона в классической механике. Обе эти теории были эквивалентны, и дали крепкую основу для описания квантовых явлений. Прошло немного времени после создания квантовой механики, Шредингером и Гейзенбергом, как тут же на арену выходит Поль Дирак, который предложил общую теорию для описания квантового мира, в своей работе он провел параллель между СТО и волновой механикой, и сделал их сочетаемыми. Спин и магнитные свойства электрона следовали из теории Дирака, без каких бы то ни было дополнительных предположений.

# 2 РАЗВИТИЕ КВАНТОВОГО КОМПЬЮТЕРА

Первое упоминание о квантовых вычислениях высказал наш советский ученый Юрий Манин(1980), но о ней заговорили только после доклада нобелевского лауреата Ричарда Фейнмана проведенной в Массачусетском технологическом университете(1981), он предположил, что на данный момент моделировать квантовую систему на обычных компьютерах является невозможным. Потом в 1982 Пауль Бениофф предложил теоретическую схему работы квантового компьютера, Вуттерс и Зурек доказали теорему о запрете клонирования, что легло в основу квантовой криптографии. В 1984 Чарльз Беннетом и Жилем Брассард предложили протокол квантового распределения ключа, полноценный криптографический способ передачи данных, основанный на квантовой физики. В 1985 Девид Дойч описал квантовую машину Тьюринга, это абстрактный квантовый компьютер, который может провести любые квантовые вычисления.1991 Артур Экерт описал безопасную систему связи на основе эффекта квантовой запутанности. 1994 Питер Шор открыл важнейший квантовый алгоритм, носящий гордое название алгоритм Шора. Этот алгоритм одновременно решил две важные задачи — проблему факторизации целых чисел и задачу дискретного логарифмирования.

Список достижений 21 века:

1. 01 год. IBM представил выполнение алгоритма Шора для числа 15.
2. 07-16 годы D-Wave создает компьютер и модифицирует его с 128-2000 кубитов.
3. 12 год. В Университете Калифорнии реализовали алгоритм Шора для 21.
4. 16год. Google создал молекулу водорода на девяти кубитном компьютере.
5. 17год. IBM создала гидрид бериллия BeH2.
6. 19году. IBM Q System One. Двадцати кубитный компьютер в облаке.
7. 19году. Google Sycamore. Пятидесяти-трех кубитный компьютер.

Можно увидеть насколько продвинулись квантовые вычисления, хоть и не значительно, но они имеют огромную ценность для развития человечества, ведь это довольно новая технология

Есть два основных направления развития квантовых машин:

1. Специальные квантовые компьютеры, которые предназначены для решения одной конкретной задачи, как пример, задачи оптимизации.
2. Универсальные — способны выполнить квантовые алгоритмы, например Шора.
3. Другие ветки развития:

- квантовые сенсоры
- квантовая сеть - основа квантовой криптографии
- и т.д.

# 3 ОСНОВОПОЛАГАЮЩИЕ КВАНТОВЫХ МАШИН

## 3.1 Квантовые компьютерные системы

Квантовый компьютер вместо обычных носителей информации использует квантовые объекты, а для вычислений квантовые объекты должны быть собраны в единую квантовую систему.

Квантовая система - материальный объект, который описывается с помощью специального аппарата квантовой механики.

Квантовый объект — объект микромира (квантового мира), который проявляет квантовые свойства:

1. Имеет определенное состояние с двумя конечными уровнями
2. Находится в суперпозиции своего состояния до момента изменения состояния.
3. Запутывается с объектами для создания квантовых систем
4. Воспроизводит теорему  запрета клонирования .

Состояние Суперпозиции В классических компьютерах электрические сигналы, такие как напряжения, представляют состояния 0 и 1 в виде однобитовой информации. Два бита указывают на четыре состояния 00, 01, 10 и 11, а n битов могут представлять 2n состояний. В квантовом компьютере квантовый бит, называемый “кубит”, который представляет собой систему с двумя состояниями, представляет однобитовую информацию. Например, вместо электрического сигнала в классических компьютерах в качестве кубита можно использовать электрон. Увеличение и уменьшение вращения электрона представляют два состояния: 0 и 1 соответственно. Также можно использовать фотон как кубит, так и горизонтальная и вертикальная поляризация фотона могут использоваться для представления обоих состояний. Используя кубиты, квантовые компьютеры могут выполнять арифметические и логические операции, как это делает классический компьютер. Важное отличие, однако, заключается в том, что один кубит также может представлять суперпозицию состояний 0 и 1. Когда мы представляем состояния 0 и 1 в виде векторов состояний $|0\rangle$ и $|1\rangle$ соответственно, такое состояние суперпозиции выражается как линейная комбинация $|0\rangle$ и $|1\rangle$ ,

$|\psi\rangle = a|0\rangle + b|1\rangle$ . “ $|\ \rangle$” называется “ket-вектор” в Дираке обозначения и коэффициенты a и b называются амплитудами вероятности. $|a|^2$ указывает на вероятность того, что мы получим $|\psi\rangle = |0\rangle$в результате измерения на кубите $|\psi\rangle = a|0\rangle + b|1\rangle$ . Они также удовлетворяют$|a|^2 + |b|^2 = 1$. Например, когда амплитуды вероятности: a и b равны $\frac{1}{\sqrt{2}}$, мы можем выразить состояние суперпозиции двух состояний следующим образом: $\left|\psi\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}|1\rangle$, где векторы $\left|0\right\rangle = (1,0)^T$ и $\left|1\right\rangle = (0,1)^T$. Короче говоря, когда мы измеряем состояние $|\psi\rangle$, состояние будет наблюдаться как $|0\rangle$ с вероятностью $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ и как $|1\rangle$ с вероятностью $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$.

Эта причудливая характеристика квантовых компьютеров делает параллельные вычисления возможными в реальном смысле этого слова. Поскольку каждый кубит представляет два состояния одновременно, два кубита могут представлять четыре состояния одновременно. Например, когда мы используем два кубита, которые являются суперпозицией состояний 0 и 1, в качестве входных данных для операции, мы можем получить результат четырех операций для четырех входных данных всего за один вычислительный шаг по сравнению с четырьмя операциями, необходимыми классическому компьютеру. Аналогично, при использовании n кубитов мы можем создать суперпозицию $2^n$ состояний в качестве входных данных и обработайте входные данные всего за один шаг, чтобы решить проблему, для которой классический компьютер требует $2^n$ шагов. В этом свете квантовый компьютер может обрабатывать n входных данных только с одним вычислительным шагом после принятия состояния суперпозиции n входных данных.

Однако, прежде чем мы сможем использовать эту чрезвычайно ценную характеристику квантовых компьютеров, остается решающая проблема. Из ввода одного состояния суперпозиции, представляющего четыре состояния, и обработки за один шаг мы получаем суперпозицию из четырех результаты. Когда мы измеряем выходные кубиты, квантово-механическая суперпозиция разрушается, и каждый кубит будет наблюдаться либо как 0, либо как 1, поскольку кубит представляет собой систему с двумя состояниями. Следовательно, мы получаем только один из четырех

возможных результатов: 00, 01, 10 или 11(для n=2) с той же вероятностью. Соответственно, суперпозиция кубитов определяется вероятностью, и измерение необходимо для определения того, какое из возможных состояний представлено. Эта трудность возникает из-за использования квантово-механического суперпозиция. Однако, если мы сможем увеличить вероятность получения ожидаемого результата, разработав алгоритм, мы можем воспользоваться функцией квантово-механической суперпозиции. Таким образом, как обсуждалось выше, мы можем использовать возможности квантовых компьютеров для решения проблемы, которая требует чрезмерного количества вычислительного времени и энергии для определенных классов задач на классических компьютерах.

## 3.2 Кубит

Современные компьютеры используют биты — поток электрических или оптических импульсов, представляющих 1с или 0с. Все, от ваших твитов и электронных писем до ваших песен iTunes и видео YouTube, по сути, являются длинными строками этих двоичных цифр.

С другой стороны, квантовые компьютеры используют кубиты, которые обычно представляют собой субатомные частицы, такие как электроны или фотоны. Генерация и управление кубитами - это научная и инженерная задача. Некоторые компании, такие как IBM, Google и Rigetti Computing, используют сверхпроводящие схемы, охлажденные до температур холоднее, чем в глубоком космосе. Другие, такие как IonQ, захватывают отдельные атомы в электромагнитных полях на кремниевом чипе в сверхвысоковакуумных камерах. В обоих случаях цель состоит в том, чтобы изолировать кубиты в контролируемом квантовом состоянии.

Кубиты имеют некоторые причудливые квантовые свойства, которые означают, что связанная группа из них может обеспечить большую вычислительную мощность, чем такое же количество двоичных битов. Одно из этих свойств известно как суперпозиция, а другое - запутанность.

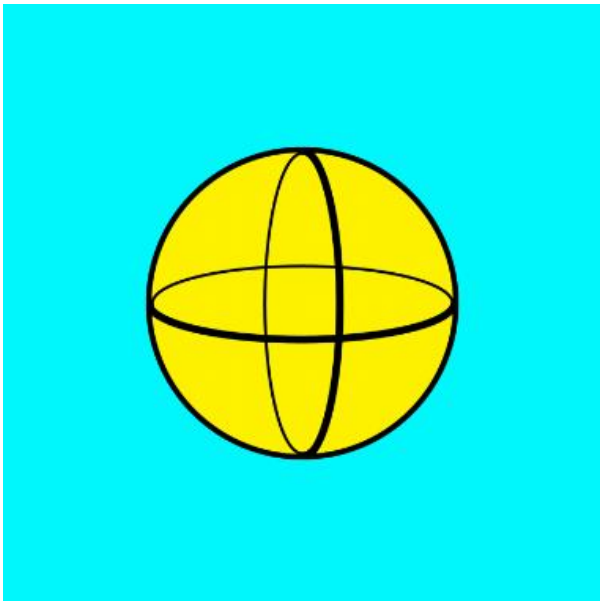

Рисунок 1 – Кубит.

## 3.3 Суперпозиция

Кубиты могут представлять множество возможных комбинаций 1 и 0 одновременно. Эта способность одновременно находиться в нескольких состояниях называется суперпозицией. Чтобы поместить кубиты в суперпозицию, исследователи манипулируют ими с помощью прецизионных лазеров или микроволновых лучей.

Благодаря этому парадоксальному явлению квантовый компьютер с несколькими кубитами в суперпозиции может одновременно обрабатывать огромное количество потенциальных результатов. Конечный результат вычисления появляется только после измерения кубитов, что немедленно приводит к тому, что их квантовое состояние “коллапсирует” до 1 или 0.

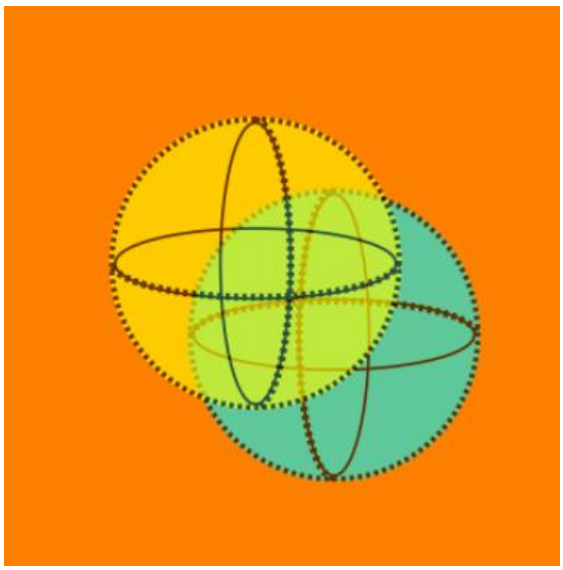

Рисунок 2 – Суперпозиция.

## 3.4 Запутанность

Исследователи могут генерировать пары кубитов, которые “запутаны”, что означает, что два члена пары существуют в одном квантовом состоянии. Изменение состояния одного из кубитов мгновенно изменит состояние другого предсказуемым образом. Это происходит, даже если они разделены очень большими расстояниями.

Никто не знает, как и почему работает запутанность. Это даже озадачило Эйнштейна, который классно описал его как “жуткое действие на расстоянии”. Но это ключ к мощи квантовых компьютеров. В обычном компьютере удвоение числа битов удваивает его вычислительную мощность. Но благодаря запутанности добавление дополнительных кубитов в квантовую машину приводит к экспоненциальному увеличению ее способности к сокращению числа.

Квантовые компьютеры используют запутанные кубиты в своего рода квантовой цепочке, чтобы творить свою магию. Способность машин ускорять вычисления с использованием специально разработанных квантовых алгоритмов - вот почему так много шума об их потенциале.

Это хорошая новость. Плохая новость заключается в том, что квантовые машины более подвержены ошибкам, чем классические компьютеры, из-за декогеренции.

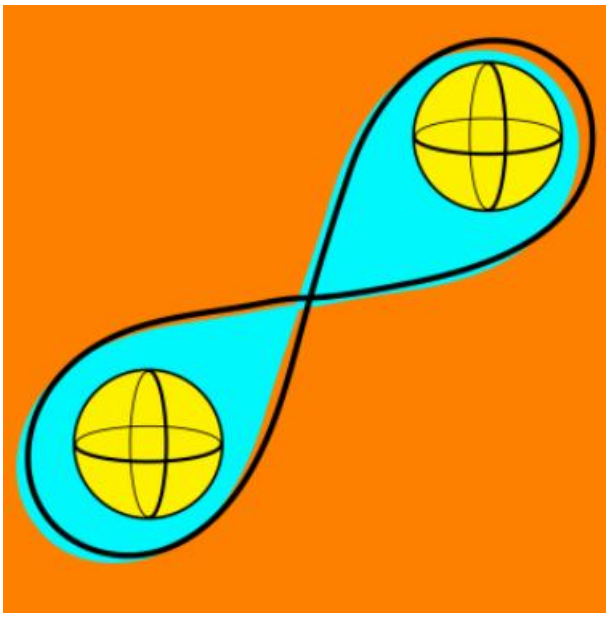

Рисунок 3 – Запутанность.

## 3.5 Декогеренция

Взаимодействие кубитов с окружающей средой таким образом, что их квантовое поведение распадается и в конечном итоге исчезает, называется декогеренцией. Их квантовое состояние чрезвычайно хрупкое. Малейшая вибрация или изменение температуры—нарушения, известные как “шум” в квантовой речи, -могут привести к тому, что они выпадут из суперпозиции до того, как их работа будет выполнена должным образом. Вот почему исследователи делают все возможное, чтобы защитить кубиты от внешнего мира в этих переохлажденных холодильниках и вакуумных камерах.

Но, несмотря на их усилия, шум по-прежнему вызывает множество ошибок в вычислениях. Интеллектуальные квантовые алгоритмы могут компенсировать некоторые из них, и добавление большего количества кубитов также помогает. Однако, вероятно, потребуются тысячи стандартных кубитов, чтобы создать один, высоконадежный, известный как “логический”

кубит. Это приведет к снижению вычислительной мощности квантового компьютера.

И вот в чем загвоздка: до сих пор исследователи не смогли сгенерировать более 128 стандартных кубитов (см. Наш счетчик кубитов здесь). Таким образом, нам еще много лет до получения квантовых компьютеров, которые будут широко полезны.

Это не разрушило надежды пионеров на то, чтобы первыми продемонстрировать “квантовое превосходство”.

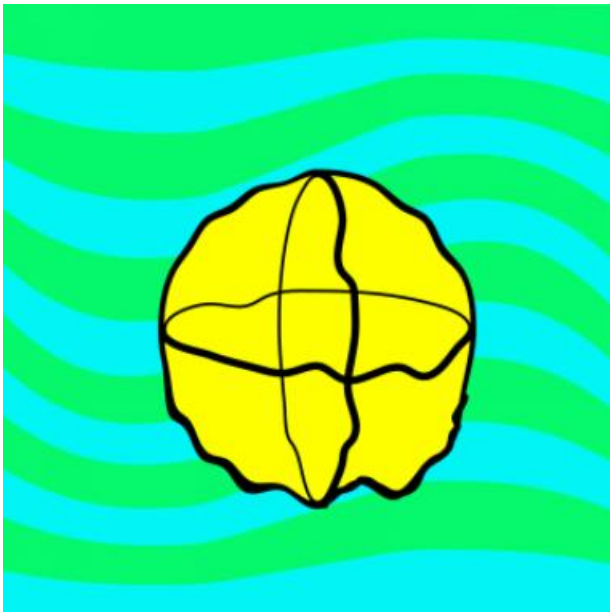

Рисунок 4 – Декогеренция.

## 3.6 Квантовое превосходство

Это точка, в которой квантовый компьютер может выполнить математические вычисления, которые явно недоступны даже самому мощному суперкомпьютеру.

До сих пор неясно, сколько именно кубитов потребуется для достижения этой цели, потому что исследователи продолжают находить новые алгоритмы для повышения производительности классических машин, а суперкомпьютерное оборудование продолжает улучшаться. Но исследователи

и компании упорно работают, чтобы претендовать на титул, проводя тесты против некоторых из самых мощных суперкомпьютеров в мире.

В мире исследований много споров о том, насколько значительным будет достижение этой вехи. Вместо того, чтобы ждать объявления превосходства, компании уже начинают экспериментировать с квантовыми компьютерами, созданными такими компаниями, как IBM, Rigetti и D-Wave, канадской фирмой. Китайские фирмы, такие как Alibaba, также предлагают доступ к квантовым машинам. Некоторые компании покупают квантовые компьютеры, в то время как другие используют те, которые доступны через облачные вычислительные сервисы.

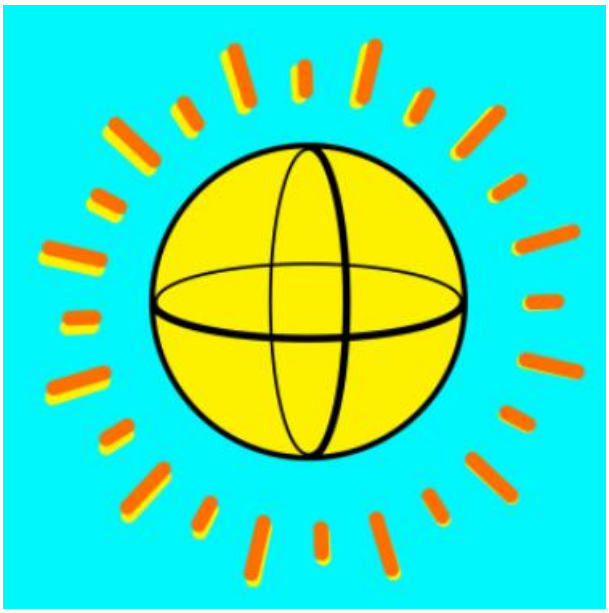

Рисунок 5 – Квантовое превосходство.

# 4 СИМУЛЯТОРЫ КВАНТОВЫХ КОМПЬЮТЕРОВ

Как было сказано выше, число компаний, пытающихся реализовать физические кубиты, увеличилось в последнее время, однако пройдет еще много лет, прежде чем квантовые вентили будут доступны для использования компьютерными учеными/инженерами. А пока нам нужен квантовый компьютерный симулятор для поиска новых алгоритмов. Квантовые компьютерные системы могут быть математически представлены с помощью векторов и матриц. Когда мы определяем $|0\rangle$= (1,0)T и $|1\rangle$ = (0,1)T , операция НЕ для одного кубита может быть выражена с помощью 2×2 унитарной матрицы как :

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

Мы можем представить операцию преобразования начального условия $|1\rangle$ в суперпозицию состояния $|0\rangle \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} |1\rangle$ с помощью матрицы:

$$\mathrm{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

$$\mathrm{H} \cdot \Big|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \Big|0\rangle + \frac{1}{\sqrt{2}} |1\rangle$$

В частности, эта операция известна как преобразование Адамара.

Несколько кубитов представлены как тензорное произведение двух векторов $|0\rangle$ и $|1\rangle$ . Для, например, двух кубитных резистора они представлены следующим образом:

$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}^{\mathrm{T}}$, $|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}^{\mathrm{T}}$

$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix}^{\mathrm{T}}$, $|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}^{\mathrm{T}}$

Операция «управляемое НЕ»

$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle$

Первый бит называется управляемым битом, а второй бит — целевым битом. Унитарная матрица управляемых НЕ-операций для двух кубитов имеет вид:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Для резистора из n кубитов нужна матрица 2n x 2n. Мы также можем определить влияние ошибки на кубите (т. е. переворот бита, сдвиг знака, как переворот бита, так и сдвиг знака) как сумма Матрицы Паули:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Таким образом, используя векторы и унитарные матрицы, можно создать теоретический квантовый компьютер. Который моделируется математически. Было предложено и реализовано множество симуляторов квантовых компьютеров. Некоторые исследователи смоделировали квантовый компьютер с коммерческими пакетами программного обеспечения математики. Например, Уильямс предоставил симулятор записной книжки математика. Этот симулятор показывает некоторые основные операции на квантовых компьютерах и  Алгоритм Шора. Затем было создано коммерческое программное обеспечение «симулятор квантового компьютера». Это программное обеспечение позволяет пользователям моделировать множество типовых алгоритмов (например, алгоритм Шора, алгоритм Гровера) и разработанные пользователем схемы с графическим изображением скалывателя. С графическим пользовательским интерфейсом. Теоретические симуляторы квантовых компьютеров, как правило, выполняют в высшей степени идеализированные унитарные операции. На практике унитарные операции над физической системой более сложные. Поэтому был разработан другой тип симулятора квантового компьютера, как эмулятор аппаратного обеспечения квантового компьютера. Этот тип эмулятора имитирует более реалистичные модели, строго следующие законам квантовой механики. Михильсен моделирует квантовый компьютер, подобный NMR. Аппаратная часть симулятора смоделирована в терминах квантовых спинов, которые эволюционируют во времени в соответствии с зависящим от времени уравнением Шрёдингера. Общая и существенная проблема симуляторов квантовых компьютеров заключается в их неспособности для

моделирования квантовых компьютеров с большим количеством кубитов (например, 500, 1000 и более, биты, необходимые для алгоритма шифрования RSA). Для представления большого количества кубитов требуется экспоненциально большая память. Поэтому, когда мы моделируем квантовый компьютер с большим количеством кубитов, нам нужно использовать параллельный компьютер. Например, квантовый компьютер до 30 кубитов был смоделирован с использованием 8-процессорного параллельного компьютера

# 5 АЛГОРИТМ ШОРА И УРАВНЕНИЕ ШРЕНДИНГЕРА

Этот алгоритм создан, для факторизации дискретного логарифма. Проще говоря, разбиения, какого то числа на составляющие множители, например 15, это 5 и 3, или 3 и 5 и т.д.

Алгоритм Гровера.

Алгоритм решения задачи методом перебора. Т.е. поиска решения уравнения. F(X) = 1, где F — есть булева функция от n переменных.

Алгоритм Гровера может быть использован для нахождения медианы и среднего арифметического числового ряда. Кроме того, он может применяться для решения NP-полных задач путем исчерпывающего поиска среди множества возможных решений. Это может повлечь значительный прирост скорости по сравнению с классическими алгоритмами, хотя и не предоставляя «полиномиального решения» в общем виде.

Уравнение Шредингера – одномерное стационарное уравнение Шредингера – самый простой. Здесь x - расстояние или координата частицы, m - масса частицы, E и U - соответственно ее полная и потенциальная энергии. Решение этого уравнения – волновая функция (пси) Волновая функция – еще одно фундаментальное понятие в квантовой механике. Так, у любой квантовой системы, находящейся в каком-то состоянии, есть волновая функция, описывающая данное состояние. Например, при решении одномерного стационарного уравнения Шредингера волновая функция описывает положение частицы в пространстве. Точнее говоря, вероятность нахождения частицы в определенной точке пространства. Иными словами, Шредингер показал, что вероятность может быть описана волновым уравнением.

# 6 ИМИТАЦИЯ И ВИЗУАЛИЗАЦИЯ ЭЛЕМЕНТОВ КВАНТОВОГО КОМПЬЮТЕРА С ПОМОЩЬЮ ИГРЫ

Построение моста между конечными пользователями и квантовыми вычислениями с помощью визуальных, простых в использовании инструментов разработки программного обеспечения.

В этой игре используются такие элементы как: лазер, детектор, всенаправленный детектор, Rok (помеха), мина (ошибка), зеркало, угловой куб, разделитель луча, поляризационный разветвитель луча, раствор сахара, вращатель Фарадея, поляризатор, волновая пластина, вакуумная банка, absorber (фильтр, поглощающий 50% света).

## 6.1 Лазер

Однофотонные источники позволяют производить отдельные фотоны. Одиночные фотоны имеют характерное квантовое поведение. Одиночные фотоны были созданы совсем недавно, в 1970-х годах. Они являются “квантом”, или наименьшей единицей электромагнитного поля.

В большинстве случаев существует система, которая испускает один фотон при определенном процессе. Некоторые системы, которые могут производить одиночные фотоны, являются захваченными ионами, ослабленными пучками атомов натрия, молекулами пентацена и более поздними центрами вакансий азота в алмазе, квантовых точках и двумерных материалах.

Одним из процессов, с помощью которых могут быть созданы одиночные фотоны, является параметрическое понижающее преобразование. В этом процессе один фотон, который взаимодействует с нелинейным кристаллом, может быть разделен на два фотона, и наоборот.

Одиночные фотоны обычно используются в квантовых информационных лабораториях, они являются главными героями экспериментов по тестированию Белла и квантовой криптографии.

## 6.2Детектор

Он обнаруживает любой фотон, который падает на него, преобразуя его в электрический сигнал.

Некоторые люди утверждают, что мы, люди, если мы действительно растягиваем наши глаза, можем обнаружить даже одиночные фотоны. “Самое удивительное, что это не похоже на видение света. Это почти ощущение, на пороге воображения”. Поймать один фотон - огромная задача! К счастью, ученые работали на нас и придумали множество устройств, которые могут воспринимать всего один фотон.

Одним из наиболее распространенных однофотонных детекторов является трубка фотоумножителя. Это устройство, которое может переводить фотоны, которые являются светом, в электричество, которое можно точно измерить.

Вряд ли кто-то из нас нуждается в таком устройстве в нашей повседневной жизни, обычно вокруг нас слишком много света, чтобы мы могли видеть одиночные фотоны. Тем не менее, детекторы одиночных фотонов широко используются в лаборатории квантовой физики. С другой стороны, мы находим устройства, которые превращают свет в электричество вокруг нас, например, это именно то, что делают солнечные панели.

Фотоумножители, также называемые PMTS, могут умножать исходный ток в 100 миллионов раз.

Фотоумножительные трубки были первым “электрическим глазом” и на сегодняшний день являются одним из наиболее часто используемых устройств для подсчета фотонов. И тот факт, что мы можем считать фотоны, еще раз демонстрирует, что Эйнштейн был прав, свет-это не только волна, но и квантованная частица.

PMTS, наряду с другими типами детекторов счета фотонов, такими как фотохимические и тепловые детекторы, широко используются в физических лабораториях. Во многих экспериментах по квантовой физике мы должны уметь считать испускаемые фотоны. И они также используются для обнаружения очень

слабых сигналов, например, от проходящих нейтрино, таких как в эксперименте superkamiokande, который представляет собой огромную подземную камеру, заполненную водой и полностью покрытую PMTS!

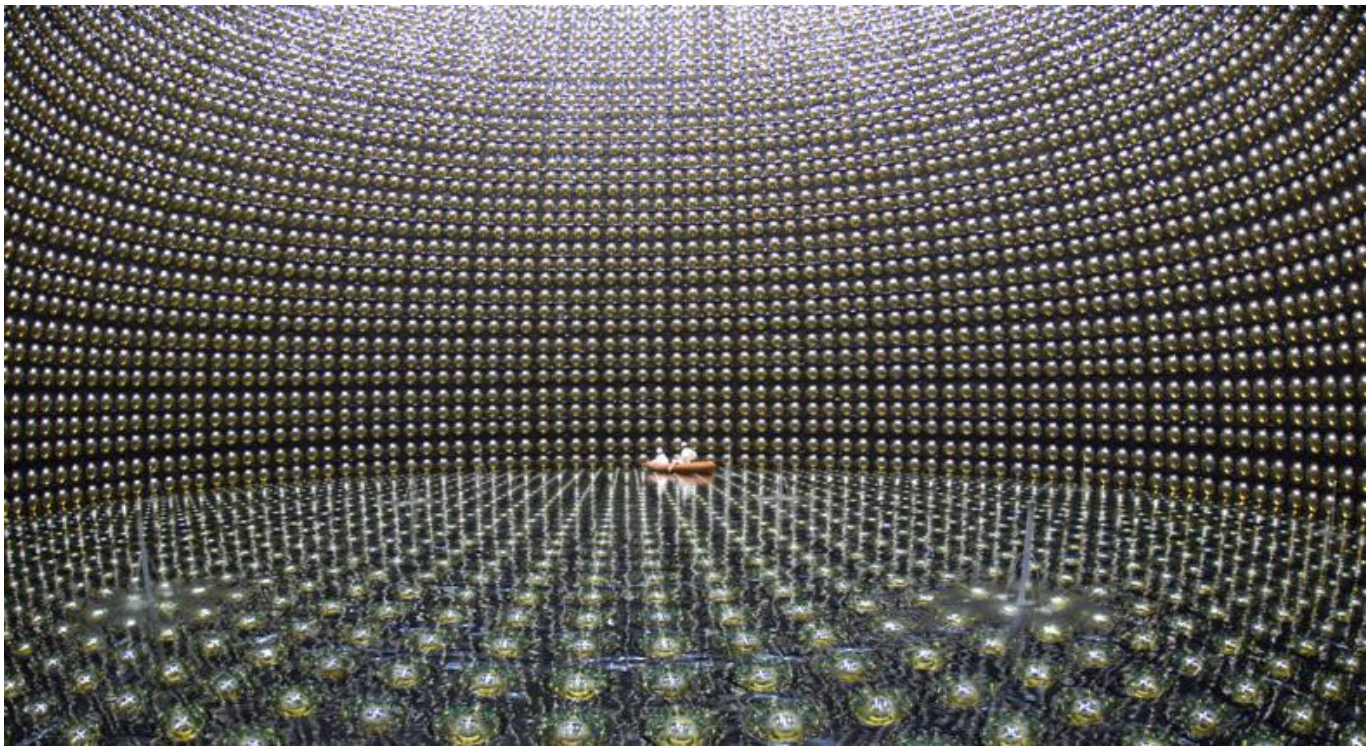

Рисунок 6 – Подземная камера, заполненная водой и полностью покрытая PMTS.

## 6.3 Мина (ошибка)

Мина – фоточувствительная бомба, которая, в случае попадания фотона, выдает ошибку.

В зависимости от вашего мировоззрения, либо есть случайный шанс, что бомба взорвется или нет (например, в копенгагенской интерпретации измерения), либо есть два эквивалентных мира - один, в котором она взрывается, и один, в котором она не взрывается (например, в многомировой интерпретации Эверетта).

## 6.4 Зеркало

Зеркало - это объект, который отражает падающий свет, сохраняя свои свойства.

Зеркало отражает свет, причем угол падения совпадает с углом отражения.

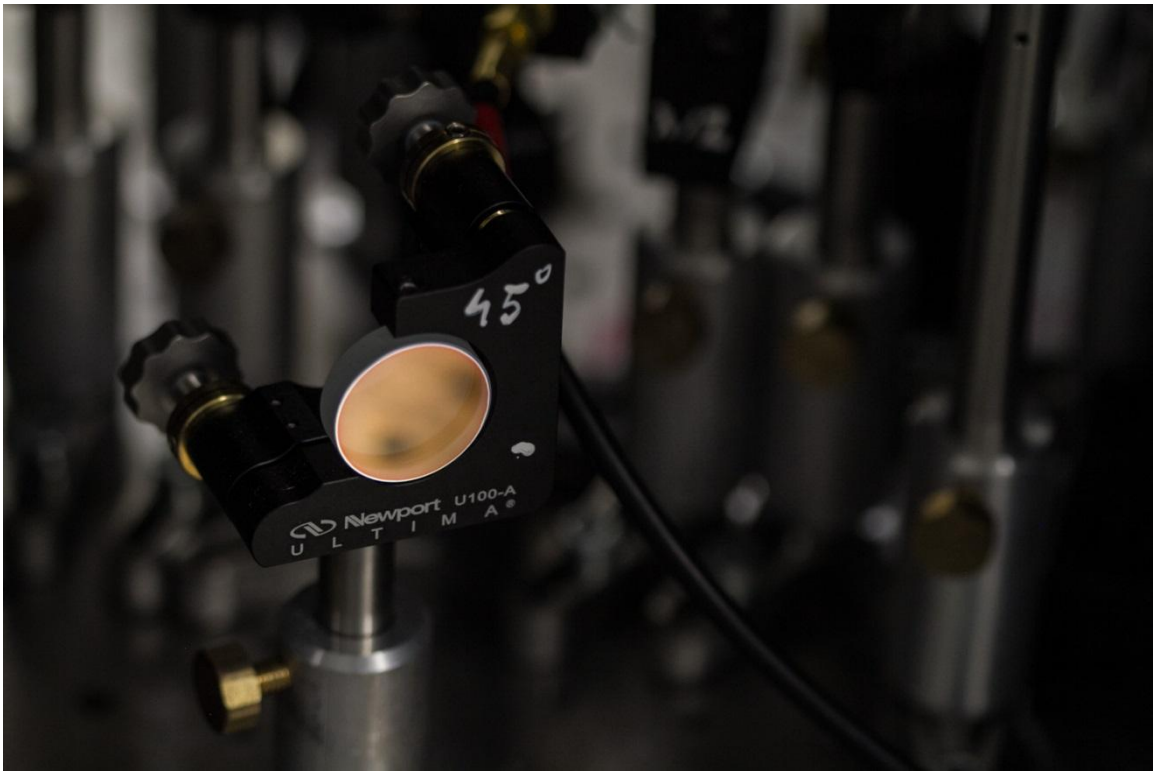


Рисунок 7 – Зеркало.

## 6.5 Разделитель луча

Оптические устройства, используемые для разделения одного луча лазерного света на два луча или для рекомбинации двух лучей в один.

Светоделители - это оптические устройства, используемые для разделения одного луча лазерного света на два луча, независимо от поляризации входящего света. Если два исходящих луча имеют одинаковую интенсивность, это называется 50-50 beamsplitter. Это соотношение между интенсивностью двух лучей может быть настроено произвольно, чтобы получить больше света, проходящего, чем отраженного, или наоборот. Светоделители также можно использовать в обратном порядке, чтобы рекомбинировать два луча в один.

Светоделители используются в интерферометрах.

Рисунок 8– Разделитель луча.

Светоделители являются фундаментальным оптическим элементом во всех лабораториях оптики и квантовой физики. Они обычно используются для создания большего количества лучей из одного входящего луча, так что два исходящих луча могут быть рекомбинированы позже после того, как один из них подвергся дальнейшим манипуляциям.

## 6.6 Применение элементов в игре

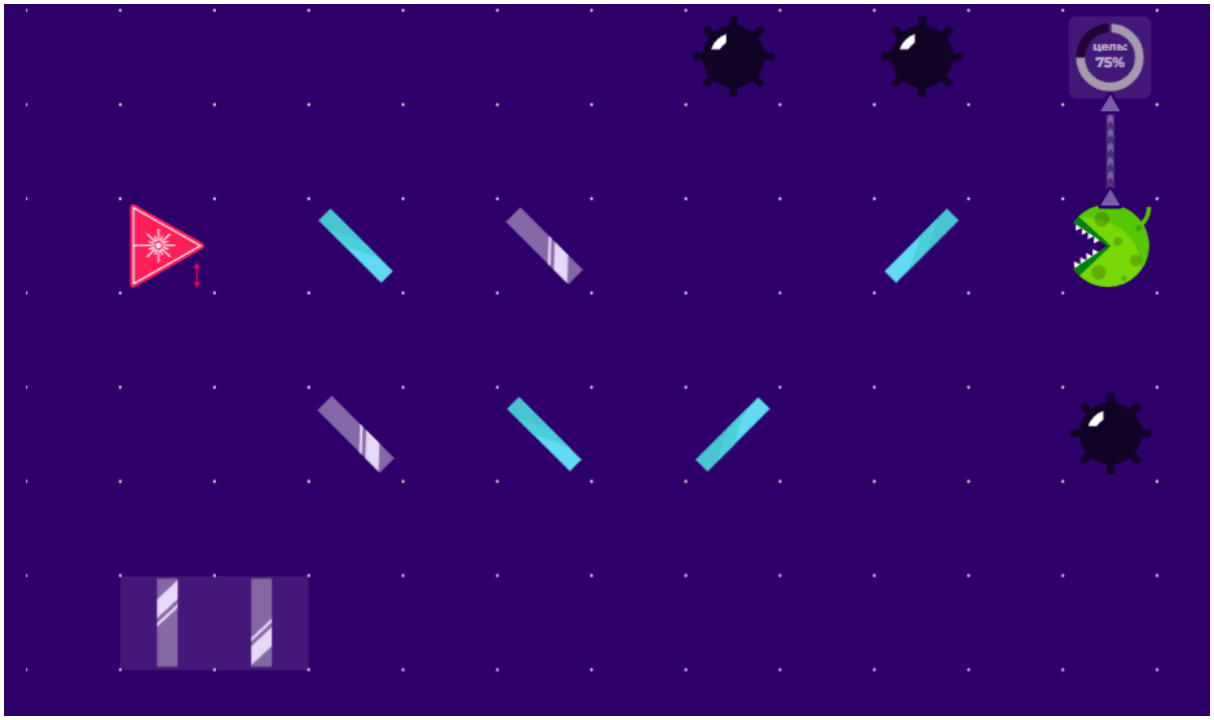


Рисунок 9 – Элементы.

Примерно это вы увидите на одном из уровней. В любом из уровней даны разные элементы для решения головоломки. Они расположены хаотично. Нужно расположить элементы, таким образом, чтобы фотон дошел до принимателя.

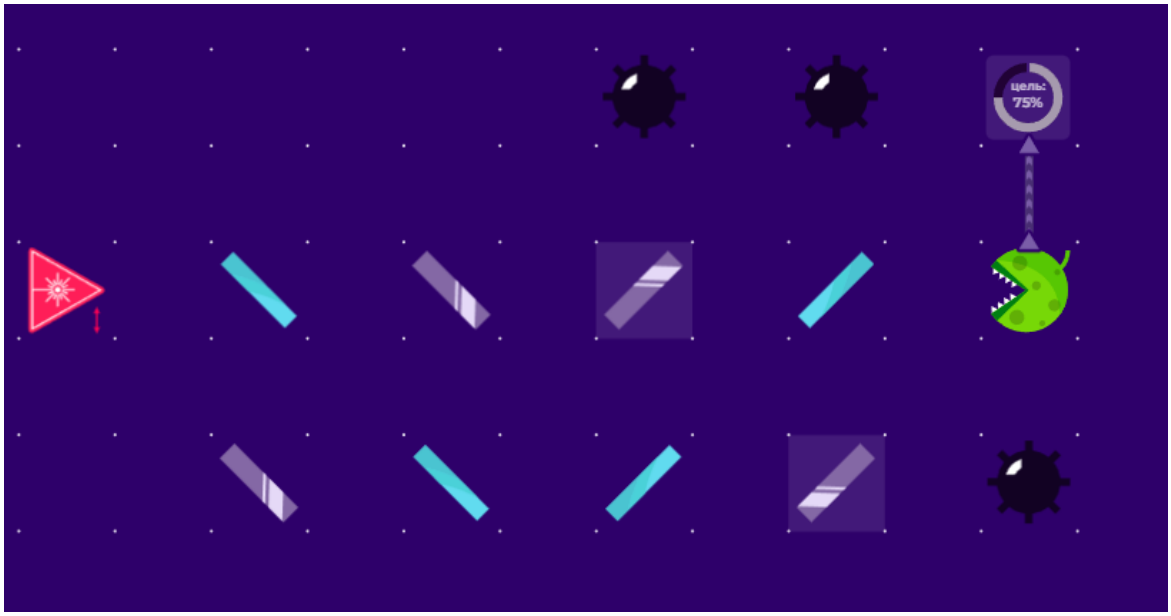


Рисунок 10 – Правильное расположение.

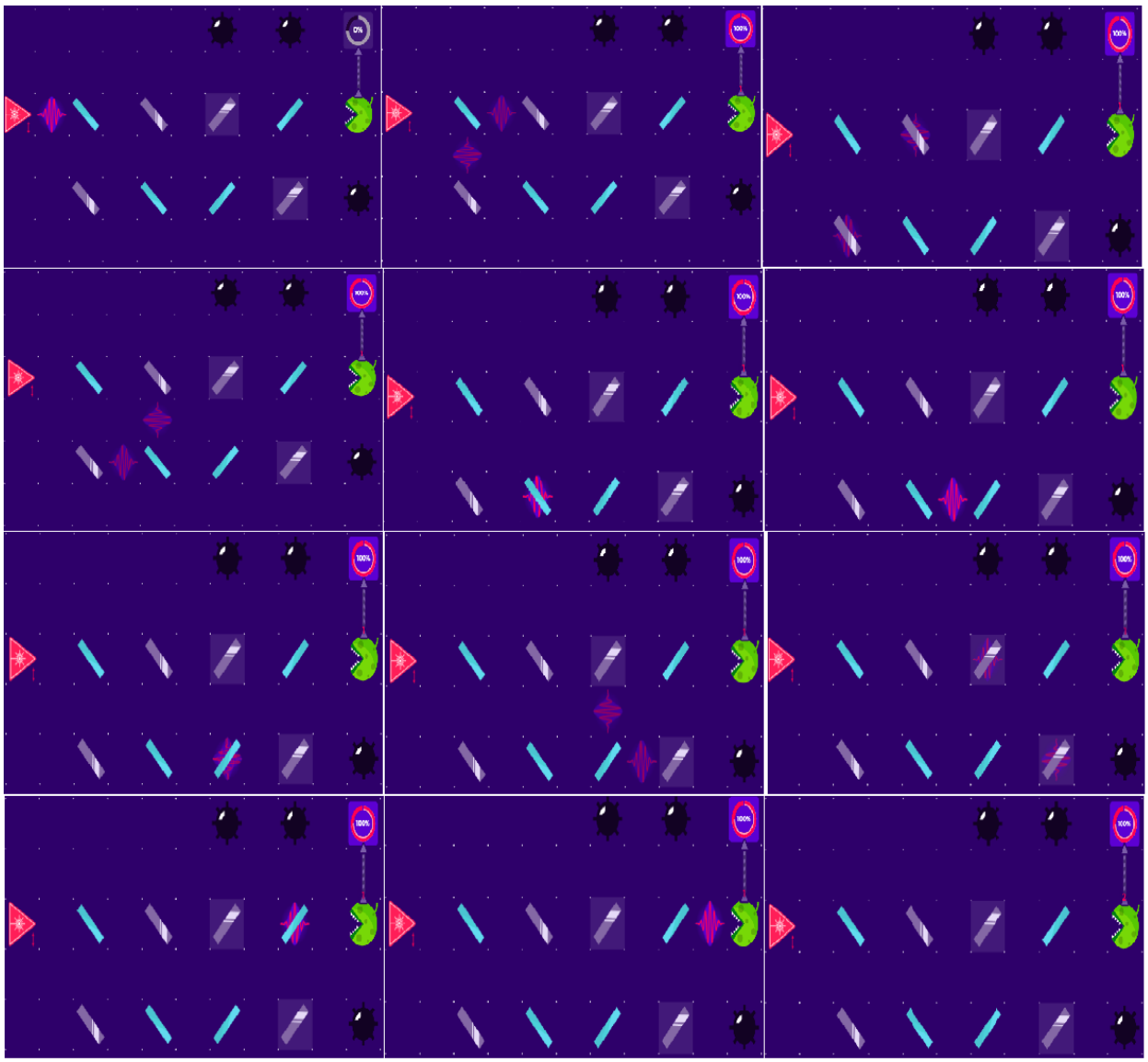

Рисунок 11 – Ход выполнения алгоритма.

# 7 ПРИМЕНЕНИЕ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

1. Квантовые вычисления в коммуникации

Сегодня безопасность данных является большой проблемой и для их защиты данные в зашифрованном виде передаются по волоконно-оптическим кабелям или другим каналам вместе с цифровыми ключами для расшифровки data на конце приемника. Данные и ключи отправляются как классические биты, и это делает их уязвимыми для атаки. Умные хакеры может читать и копировать биты между ними, не оставляя никаких следов. Квантовые вычисления используют законы квантовой физики для защиты данных. Информация или данные в квантовых вычислениях отправляются с помощью кубитов. Эти кубиты могут находиться в состоянии суперпозиция, что означает, что он может представлять несколько комбинаций нулей и единицы одновременно, если какой-либо хакер попытается получить к ним доступ между их сверхчувствительными квантовое состояние коллапсирует до единицы или нуля. Это означает, что хакер не может украсть данные в между ними, не оставляя никаких следов.

2. Квантовые вычисления в телепортации

Телепортация – это название, данное наукой писатели-фантасты к акту заставить объект распадаться в одном месте, в то время как совершенный копия появляется где-то еще. Это основано на явлении, называемом квантовым. запутанность. Квантовая телепортация работает путем создания запутанной пары фотонов и затем отправка одного получателю, а другого получателю. Когда отправитель получает свои запутанные фотон, он позволяет ему взаимодействовать с кубитом памяти, который содержит данные, которые он хочет отправить в приёмник. Это взаимодействие изменяет состояние фотона отправителя, а также потому, что он запутан. с помощью рецептaver's Фотон также будет изменен из-за этого взаимодействия. В в 2014 году ученые успешно продемонстрировали квантовую телепортацию на расстоянии 10 футов с незначительной погрешностью.

3. Квантовые вычисления для открытия лекарств

Квантовые компьютеры используют кубиты, которые могут быть частично нулевым и частично единицей одновременно. Вместо того чтобы работать в изоляции, эти кубиты запутываются и действуют как группа, это дает этим компьютерам экспоненциально более высокая скорость, чем у классических компьютеров. Моделирование пенициллина на классическом компьютере дубль 1086 бит, и это может быть всего 286 кубитов на квантовом компьютере.

4. Квантовая криптография-

Квантовая криптография - Криптография - это процесс шифрования данных или преобразования обычного текста в зашифрованный текст, чтобы его мог прочитать только тот, у кого есть правильный ключ для расшифровки текста. Квантовая криптография использует принципы квантовой механики для шифрования данных и передачи данных способом, который невозможно взломать. Чтобы понять, как работает квантовая криптография или квантовое шифрование, давайте возьмем пример двух друзей по имени Алиса и Боб. Алиса - это отправитель, который хочет отправить секретное сообщение Бобу.С помощью квантового распределения ключей (QKD) Алиса посылает серию поляризованных фотонов по волокнуоптический кабель к Бобу. Этот волоконно-оптический кабель не обязательно должен быть безопасным, потому что фотоны имеют рандомизированное квантовое состояние. Если хакер по имени Ева попытается тайно прочитать сообщение, ей придется прочитать каждый фотон, чтобы прочитать сообщение. Затем она должна передать этот фотон Бобу, поэтому Ева неосознанно изменяет квантовое состояние фотона, что вносит ошибки в квантовый ключ. Это предупреждает Боба и Алису о том, что кто-то читает их сообщение и ключ был скомпрометирован, поэтому они отбрасывают ключ. Теперь Алиса отправляет новый ключ, который не скомпрометирован, чтобы Боб мог прочитать секретное сообщение.

# ЗАКЛЮЧЕНИЕ

Так как квантовые вычисления, могут принести человечеству невероятный подъем в технологическом прогрессе, их изучают многие компании гиганты, такие как: Google и IBM. В 2019 году компания Google, объявила, что достигла квантового превосходства, что означало впервые квантовый компьютер, превзошел классический. Но это лишь по вычислительной мощности, которую пока не могут правильно использовать. Квантовые компьютеры, только родились, и не достаточно созрели, и им потребуются многие десятилетия для смены, классических компьютеров.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ


1. Наука. Величайшие теории: выпуск 1: Пространство – это вопрос времени. Эйнштейн. Теория относительности. / Пер. с исп. – М.: Де Агостини, 2015.- 176 с.
2. Квантовая физика: для тех, кто хочет все успеть. – Москва : Эксмо, 2021. – 128 с. – (Энциклопедия быстрых знаний).
3. Отчет о тенденциях исследований квантовых вычислений [Электронный ресурс]. – Режим доступа: https://www.elsevier.com/solutions/scopus/who-uses/research-and-development/quantum-computing-report (дата обращения 15.02.2022)
4. Исследование по квантовым вычислениям [Электронный ресурс]. – Режим доступа:https://www.researchgate.net/publication/340967035_A_Study_on_Quantum_Computing (дата обращения 02.02.2022)
5. Объяснитель: Что такое квантовый компьютер? [Электронный ресурс]. – Режим доступа: https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/ (дата обращения 01.03.2022)
6. Что такое квантовые вычисления? [Электронный ресурс]. – Режим доступа: https://www.ibm.com/quantum-computing/what-is-quantum-computing/ (дата обращения 08.03.2022)
7. Определение квантовых вычислений [Электронный ресурс]. – Режим доступа: https://www.investopedia.com/terms/q/quantum-computing.asp (дата обращения 10.03.2022)