УДК 004.056.55:530.145.6+629.78

ПЕРЕДАЧА ДАННЫХ С ИСПОЛЬЗОВАНИЕМ КВАНТОВОГО ШИФРОВАНИЯ С НАНОСПУТНИКОМ В ВИДЕ ПОСРЕДНИКА

Каширских И.Е., ученик МБНОУ “ГКЛ”, 9Д класс
Ушаков А.Г., доцент кафедры химической технологии твердого топлива
КузГТУ имени Т.Ф. Горбачева
г. Кемерово

В современном мире засекреченные данные передаются традиционным путем – с помощью радиоволн или проводов, в редком случае – используя оптоволокно. При этом используются различные математические алгоритмы шифрования. Такие алгоритмы имеют существенную проблему, заключающуюся в том, что даже не имея ключа, но перехватив закодированные данные, злоумышленник может рано или поздно подобрать ключ, причем, чем больше вычислительных ресурсов имеется, тем меньше времени понадобится, что вполне логично.

В последние 40 лет в мир физики стремительно вошел новый раздел – квантовая физика, изучающий явления микромира и природу самых фундаментальных частиц – квантов. На сегодняшний день исследования в этой сфере активно применяются в создании прототипов квантовых компьютеров, могут применяться в медицине (особенно в томографии), а также в быстрой и безопасной передаче данных.

Вместе с развитием квантовой физики родилась на свет идея квантового шифрования, основанная на принципе запутанности квантов. Квантовая запутанность - квантовомеханическое явление, при котором квантовые состояния двух или большего числа объектов оказываются взаимозависимыми.

Сегодня множество компаний активно вкладывает ресурсы в разработки в данном направлении. Например, разработки специализированных квантовых вычислителей для конкретной задачи ведет D-Wave, а универсальных квантовых компьютеров для решения разных задач – IBM и Google.

Первый двухкубитный квантовый компьютер появился в 1998 году. Он работал на явлении ядерного магнитного резонанса. Компьютер использовался в Оксфордском университете, в исследовательском центре IBM и Калифорнийским университетом в Беркли вместе с сотрудниками из Стэнфордского университета и Массачусетского технологического института. В 2018 году IBM предложила сторонним компаниям использовать ее 20-кубитный квантовый компьютер через облако. Затем Google представила 53-кубитный компьютер Sycamore и заявила о достижении квантового превосходства. Квантовое превосходство подразумевает способность квантовых вычислительных устройств решать те проблемы, которые не могут решить классические компьютеры. Sycamore потребовалось около 200 секунд, чтобы выполнить выборку одного экземпляра схемы миллион раз. Самому мощному

суперкомпьютеру Summit для той же задачи понадобилось бы около 10 тысяч лет. В 2021 году в МФТИ был разработан прототип квантового процессора на базе пяти сверхпроводниковых кубитов. Данная система полностью управляема.э

На данный момент в России имеются не только разработки квантовых процессоров, но и квантовых криптографических сетей. Например, компания «Инфотекс» и Центр квантовых технологий МГУ представили первый в России телефон с квантовой защитой связи ViPNet QSS Phone. Устройство представляет собой стационарный IP-телефон, подключенный к клиенту квантового распределения ключей и серверу.

В 2016 году в Китае был запущен QSS (Quantum Science Satellite) “Мо-Цзы” - спутник для квантовой связи Пекина с Веной, правда, пока что экспериментально. Масса аппарата - 600 кг, а стоимость проекта составила $100 млн.

Следуя данным тенденциям была поставлена **цель проекта** – ***разработка системы передачи данных с использованием протокола квантового шифрования с наноспутником в виде посредника.***

Исходя из поставленной цели были определены **задачи** как этапы реализации:

1. Рассчитать необходимые параметры для определения характеристик компонентов спутника и бортовой электроники;
2. Разработать схему и 3D модель спутника;
3. Разработать примерную схему ПО для работы спутника с устройствами на земле;

Рассмотрим схему физической реализации квантовой криптографии. Слева находится отправитель, справа — получатель. Для того, чтобы передатчик имел возможность импульсно варьировать поляризацию квантового потока, то есть посылать фотоны в нужной поляризации в зависимости от кодируемой информации, а приёмник мог анализировать импульсы поляризации – считывать информацию, зашифрованную в состоянии частицы, – используются ячейки Поккельса. Ячейки Поккельса – устройства, основанные на эффекте Поккельса. Он заключается в том, что при появлении магнитного поля поляризация частицы меняется. Передатчиком формируется одно из четырёх возможных состояний поляризации. На ячейки данные поступают в виде управляющих магнитным полем сигналов. Для организации канала связи обычно используется волокно, а в качестве источника света берут лазер. На стороне получателя после ячейки Поккельса расположена кальцитовая призма, которая должна расщеплять пучок на две составляющие, улавливаемые двумя фото детекторами (ФЭУ), а те, в свою очередь, измеряют ортогональные составляющие поляризации, то есть по сути состояние фотона, которое ему дали при шифровке. Вначале необходимо решить проблему интенсивности передаваемых импульсов квантов, возникающую при их формировании. Если в

импульсе содержится 1000 квантов, существует вероятность того, что 100 из них будут отведены криптоаналитиком (злоумышленником) на свой приёмник. После чего, проводя анализ открытых переговоров, он сможет получить все необходимые ему данные. Из этого следует, что идеален вариант, когда в импульсе количество квантов стремится к одному. Тогда любая попытка перехватить часть квантов неизбежно изменит состояние всей системы и соответственно спровоцирует увеличение числа ошибок у получателя. В этой ситуации следует не рассматривать принятые данные, а заново повторить передачу.

Кроме простейшего алгоритма BB84 существуют протоколы квантового шифрования, использующие эффект Эйнштейна - Подольского - Розена (EPR). Например, протокол B92 или E91. Эффект заключается в следующем. Как изветно из закона квантовой механики, при измерении импульса частицы нарушаются ее координаты и наоборот. Как следствие, невозможно точно измерить каждый параметр частицы. Но, допустим, что при распаде некоторой частицы C образуется частица A и частица B. Тогда по закону сохранения импульса $P_A + P_B = P_C$. Исходя из этого, измерив импульс одной частицы, возможно рассчитать импульс второй без взаимодействия с ней. Теперь, измерив координату второй частицы, можно получить для этой частицы значения двух неизмеримых одновременно величин, что по законам квантовой механики невозможно. Это создает впечатление мгновенного воздействия первой частицы на вторую.

Протокол B92

Протокол использует четыре квантовых состояния фотона, направление вектора поляризации, одно из которых выбирается в зависимости от передаваемого бита: 90 градусов или 135 градусов для 1, 45 или 0 для 0. Одна пара соответствует 0(+) и 1(+) и принадлежит базису +. Другая пара - соответственно 0(×) и 1(×) и принадлежит базису ×. Квантовые состояния системы можно описать следующим образом:

Двоичный сигнал Алисы				
Поляризационный код Алисы				
Детектирование Бобом				

Двоичный сигнал Боба				

Таким образом, в результате передачи ключа Бобом в случае отсутствия помех и искажений будут правильно зарегистрированы в среднем 50 % фотонов.

Протокол BB84

Существует также альтернативный вариант – при помощи квантового канала связи осуществить лишь распределение секретных ключей между двумя общающимися устройствами, а сами пакеты данных передавать обычным способом. Этот способ является безустловным лидером в случаях, когда имеется возможность соединить двух собеседников каналом из оптоволокна, так как для распределения ключей требуется осуществлять передачи по одной частице. Такое условие подразумевает высочайшую точночть и недопустимость помех при передаче, что в данном случае недостижимо.

Система состоит из двух наземных устройств и спутника-передатчика. Спутник в формате CubeSat состоит из 12 стандартных юнитов – кубов 10 см * 10 см * 10 см, расположенных в два ряда по 6 юнитов. Крайние юниты с одного торца будут предназначены для получения и отправки сигнала, а остальные будут содержать в себе аккумулятор, бортовую электронику – микрокомпьютер, обвязку и маховик – устройство для стабилизации. На корпусе спутника расположены солнечные батареи с каждой стороны юнита. Наземные устройства будут представлять собой небольшие установки размерами ~ 30 см * 30 см * 30 см с подвижной верхней частью для прицеливания в принимающий торец спутника или подстраиваемые под направление луча лазера спутника.

Излучатель включает в себя лазер мощностью 18Вт, создающий ИК-излучение с длиной волны в 915 нм. Такая длина выбрана с целью минимизировать рассеивание пучков при проходе через различные слои атмосферы. Коэффициент расхождения луча – 1 мрад. После выхождения частиц из лазера они проходят поляризатор и ячейку Поккельса, питаемую с помощью специального адаптера, способного выдать нужное напряжение в пике. На ячейку подается напряжение с частотой в зависимости от передаваемых битов. То есть если передаваемый бит – 0, то напряжение на ячейке – 0В. А если 1 – 2,5кВ. А значит угол поляризации при нулевом бите – 0 градусов, а на единичном – 45 градусов. Система излучает два луча: запутанные частицы попарно – обыкновенный и необыкновенный луч, то есть две частицы с перпендикулярными друг другу поляризациями. В случае если одна частица из пары по пути будет перехвачена, она нарушит состояние суперпозиции и изменит состояние второй частицы в паре. Приемник заметит аномалию в пришедших частицах и будет понятно, что сигнал перехвачен. Диаметр покрываемой лазером поверхности на Земле равен примерно 18 км при высоте орбиты спутника 160 км (160 * tg 0,057° * 2).

Приемник сигнала – диафрагма, пропускающая только часть света, который далее идет на пластинку с покрытием. На данном этапе часть частиц отражается, а часть проходит дальше. Далее по пути распространения света с обеих сторон стоят поляризаторы: отраженный луч фильтруется и остаются только частицы с поляризацией 0 градусов, а прошедшие фильтруются с оставлением только частиц с поляризацией 45 градусов. Далее каждый поток частиц фиксируется фотоэлектронным умножителем и выдает электрический сигнал.

Итак, чтобы узнать необходимую мощность лазера, нужно понять количество фотонов, испускаемых за секунду и энергию каждого из них. Передаваемые данные будут передаваться пакетами: один пакет – одна полная копия передаваемого сообщения. Здесь требуется понять какой максимальный объем данных будет возможен для передачи, то есть сколько пакетов и соответственно сколько фотонов в каждом пакете и в общей сумме требуется передавать. Поскольку лазер вполне может испутскать вплоть до порядка 10^{20} фотонов, каждый из которых может нести 1 бит, получается, что общий объем выпускаемой информации за секунду может достигать 10 эксабайт (10 000 000 000 гигабайт). Но, к сожалению, объем данных ограничивается частотой дискретизации на АЦП и частотой регистрации ФЭУ. Для гарантированного получения всего пакета данных на приемнике следует разбить передачу на 100 000 000 пакетов с целью достижения объема сообщения размером в 100 гигабайт (следует учитывать необходимость хранения сообщения на спутнике для его перекодирования). Отсюда получаем конкретное число фотонов, которые лазер должен испускать: $8{,}8 * 10^{18}$.

Далее требуется определить энергию одного испускаемого фотона. В первую очередь эта величина зависит от длины волны: $E_{\text{ф}} = \frac{hc}{\lambda}$, где h – постоянная планка, c – скорость света в вакууме, а λ – длина волны. Также известна зависимость – чем больше длина волны, тем меньше рассеивание луча. Следовательно, требуется использовать как можно бóльшую длину волны – инфракрасный диапазон. Существуют лазеры с длиной волны в 915 нм, что вполне достаточно. Отсюда следует, что энергия фотона равна $2{,}2 * 10^{-19}$. Далее считаем мощность лазера: $P = \frac{E\phi \times N}{t}$, где $E_{\text{ф}}$ – энергия одного фотона, N – количество фотонов, а t – время работы лазера. Из этого получаем выходную мощность, равную 18 Вт. Именно такие характеристики имеет мощный твердотельный лазер накачки “Моцарт-ИК” – мощность 18 Вт, длина волны 1064 нм.

Далее требуется обеспечить необходимым напряжением ячейку Поккельса и ФЭУ (фотоэлектронные умножители). Максимальное напряжение ячейки – 2,5 кВ, а постоянное напряжение (в течение 1 секунды) двух ФЭУ – 1,5 кВ. Для подачи такого напряжения для каждого устройства отдельно нужен драйвер. Для ячейки Поккельса – DB-SP-250-3.6, потребляющий 4 Вт, а для каждого ФЭУ – PM3315-WB, потребляющий 8 Вт.

Также для постоянной работы бортового компьютера требуется 2 Вт, для открытия клапанов РСУ (при ориентировании для получения или отправления сигнала) – 3 Вт и для периодической работы маховика – 6 Вт.

Общая потребляемая мощность в пике (при цикле отправления сообщения) – 66 Вт (33 Вт для одной отправки, удвоено, поскольку перед передачей требуется зажечь вспомогательный луч – см. "*Ориентация спутника в пространстве для получения или передачи сообщения*").

Найдем нужную мощность панели:

$P = \frac{Eп * k * Pинс}{Eинс}$, где *E*п – потребляемая энергия, *P*инс – мощность инсоляции на одном квадратном метре, *E*инс – среднемесячная инсоляция.

Отсюда мощность GaAs солнечной панели (используется для сокращения площади с сохранением вырабатываемой мощности) – 200 Вт, которых требуется 2 штуки.

Несомненно, для того, чтобы передать или получить сообщение, спутнику требуется повернуться рабочей стороной к источнику. Для этого необходимо понимать текущее положение в пространстве, что довольно сложно сделать с высокой точностью. Поэтому был сделан вывод – не требуется всегда знать точное положение, а нужно лишь двигаться вслепую до тех пор, пока не выполнится некое условие, подтверждающее достижение нужной ориентации. Этим условием может послужить "флаг" – испускаемый луч света с земли (из передаточного лазера без изменений поляризаций фотонов), который улавливается детектором (приемником информационного сигнала, настроенным на обычное детектирование света) на торце спутника. Сразу после улавливания происходит передача.

Для передачи с земли на спутник процесс происходит ровно в обратном порядке – спутник зажигает вспомогательный луч и после улавливания его на земле, происходит передача. Повторяясь, следует сказать, что вспомогательные лучи испускаются и улавливаются теми же приемниками и передатчиками соответственно, что и работают с основными лучами приема и передачи.

Управлением спутника занимается микрокомпьютер Raspberry PI 4. Для упрощения работы с перекодированием сообщения логично было бы использовать интерпретируемый язык программирования Python. Его преимущества заключаются в простоте синтаксиса, большом количестве библиотек и относительно простом устройстве на уровне операционной системы. Но у данного варианта есть ключевой недостаток – низкая эффективность и скорость работы, что в данном случае абсолютно недопустимо. Вычисления должны проходить быстро и задействовать как можно меньше оперативной памяти, чем не может похвастать Python. Исходя из этого требования, которое является ключевым и наиболее важным, был выбран язык программирования C++ из-за его быстроты и оптимизированной работы с памятью.

Следует учитывать, что максимальный объем сообщения составляет 100 Гб, что было получено из расчетов выше. Значит требуется внешний носитель информации (один SSD или набор SSD для большей скорости работы), так как встроенный диск Raspberry PI 4 имеет объем всего лишь в 8 Гб в одной из комплектаций, на котором будут храниться системные данные, программа для управления спутником и программа для перекодирования сообщения.

Управление бортовыми устройствами будет реализовано с помощью GPIO пинов Raspberry PI 4. Действующих пинов на плате 26. Этого вполне достаточно: маховик, ячейка поккельса, два ФЭУ, лазер, 4 РСУ двигателя – 9 пинов. Очевидно, сигнал, получаемый из этих пинов будет чисто управляющим и будет регулировать подачу основного тока из аккумулятора на устройства.

В итоге работы были расчитаны параметры и характеристики коспонентов, создана 3Д модель спутника, составлена схема ПО и бортовой электроники.

Согласно расчетам, для минимального эксперимента передачи данных с использованием квантового шифрования в космосе достаточно спутника формата CubeSat в пределах 12-ти юнитов размером. Из проделанного исследования и расчетов стало понятно, что основной проблемой метода является точное наведение луча на приемник. Именно для увеличения точности и гарантии получения полного пакета данных было принято решение передавать данные в несколько заходов и по 10 000 000 пакетов за одну сессию передачи.

Список литературы и источников

1. Савельев И. В. Курс общей физики : в 3 томах. Т. 3. Квантовая оптика. Атомная физика. Физика твердого тела. Физика атомного ядра и элементарных частиц / И. В. Савельев. - Москва: Наука, 1979. – 304 с. : ил. – Текст: непосредственный.

2. Тюрин Ю. И. Физика. Квантовая физика: учебник для студентов высших учебных заведений, обучающихся по техническим направлениям / Ю.И. Тюрин, И.П. Чернов, Ю.Ю. Крючков ; Федеральное агентство по образованию, Государственное образовательное учреждения высшего профессионального образования "Томский политехнический университет". - Томск: Томский политехнический университет, 2009. - 319 с. : ил. ; 21 см. - (Приоритетные национальные программы. Образование). (Инновационная образовательная программа). - ISBN 5-98298-457-4. – Текст: непосредственный.

3. Электрооптические ячейки Поккельса. – Текст: электронный // ООО «Специальные Системы. Фотоника» [сайт]. – Режим доступа: https://sphotonics.ru/catalog/pockels-cells/ (дата обращения: 17.03.2022) 4. Храмов В.Ю. Расчет элементов лазерных систем для информационных и технологических комплексов: учебно-методическое пособие / В. Ю. Храмов. - Санкт-Петербург: СПбГУ ИТМО, 2008. - 79 с. – Текст: непосредственный.