УДК 535.375.30

КВАНТОВЫЕ ЭФФЕКТЫ В ПЕРЕДАЧИ И ЗАЩИТЫ ИНФОРМАЦИИ В КРИПТОСИСТЕМЕ

Самигуллин Шынгыс Самигуллаевич
chingiz.samigullin97@gmail.com
Студент кафедры РЭТ ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Кабылбекова О.М.

Квантовые компьютеры и связанные с ними технологии в последнее время становятся все актуальнее. Исследования в этой области не прекращаются вот уже десятилетия, и ряд революционных достижений налицо. Квантовая криптография — одно из них. Владимир Красавин «Квантовая криптография»:

– Квантовые основы сигналов в криптозащите информации;

– Принципы использования квантовой криптографии и современные проблемы криптосистемы;

– рекомендации и предложения;

Действительно в последнее время все чаще мы слышим такие понятия как «Квантовый компьютер», «Квантовые вычисления» и конечно же «Квантовая криптография».И если с первыми двумя понятиями в принципе всё понятно, то «Квантовая криптография» — понятие, которое хоть и имеет точную формулировку, до сих пор остается для большинства людей темным и не совсем понятным этакий.

Основные понятия квантовых сигналов

В квантовой системе процесс отправки и приёма информации всегда выполняется физическими средствами: при помощи электронов в электрическом токе Рис.1 или фотонов в линиях волоконно-оптической связи

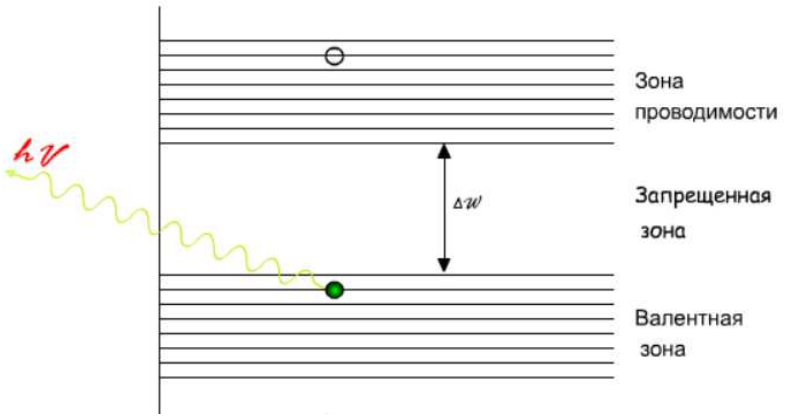

Рисунок 1 – График излучения фотона hv

Фото́н – элементарная частица, квант электромагнитного излучения (в узком смысле – света) в виде поперечных электромагнитных волн. Это безмассовая частица, способная существовать в вакууме только двигаясь со скоростью света. Электрический заряд фотона также равен нулю.

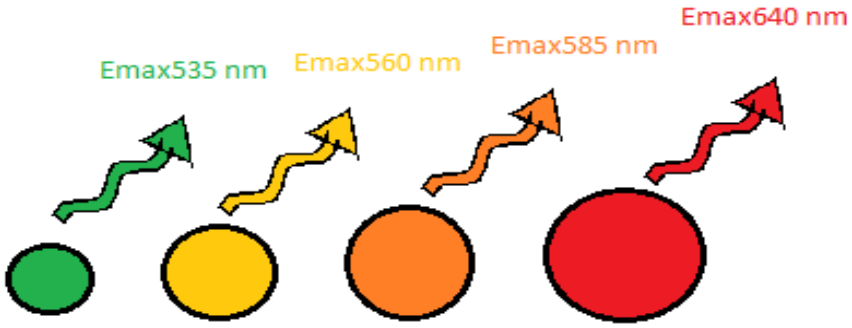

Рисунок 2 – Длина волны излучения фотона квантовых точек

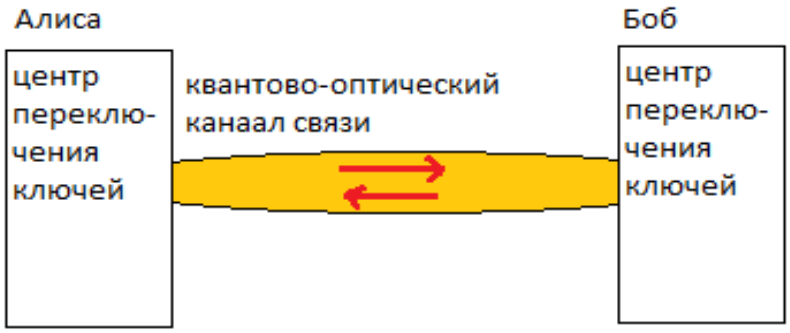

Рисунок 3 – Фотон в линии волоконно-оптической связи

Основные квантовые явления;

Два основных явлении квантовой природы: суперпозиция и запутанность. Суперпозиция – эта способность кубита (элемента хранения информации в квантовом компьютере) существовать в состоянии с неопределенным значением; если у бита два значения - 0 и 1, то кубит может находиться в состояниях, соответствующих нулю, единице или их суперпозиции. Запутанность – эта таинственная связь между квантовыми системами, при которой изменение состояния одной без измеримой задержки приводит к изменению состояния других при этом достигая огромной скорости.

Важно помнить, однако, что суперпозиция, которая встречается в квантовой механике, существенным образом отличается от суперпозиции, встречающейся в любой классической теории. Это видно из того факта, что квантовый принцип суперпозиции требует неопределённости результатов измерений.

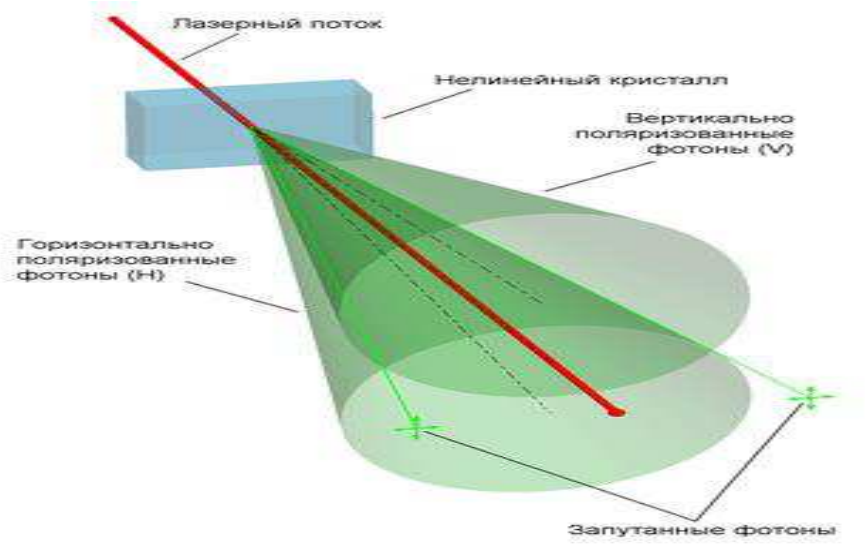

Рисунок 4 – Генерация запутанных фотонов в результате спонтанного параметрического рассеяния (СПР) лазерного потока в нелинейном кристалле

Принципы использования квантовой криптографии и современные проблемы криптосистемы;

Квантовая криптография – метод защиты коммуникаций, основанный на принципах квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике, рассматривая случаи, когда информация переносится с помощью объектов квантовой механики.

Первый протокол квантового распределения ключей был создан Жилем Брассаром и Чарльзом Беннетом в 1984 году и получил название BB84. Для передачи данных используются фотоны, поляризованные в четырёх разных направлениях, в двух базисах — под углом 0 и 90 градусов (обозначается знаком +) либо 45 и 135 градусов (x). Отправитель сообщения A (традиционно его называют «Алиса») поляризует каждый фотон в случайно выбранном базисе, а затем отправляет его получателю B — «Бобу». Боб измеряет каждый фотон, тоже в случайно выбранном базисе. После этого Алиса по открытому каналу сообщает Бобу последовательность своих базисов, и Боб отбрасывает неправильные (не совпавшие) базисы и сообщает Алисе, какие данные «не прошли». При этом сами значения, полученные в результате измерений, они по открытому каналу не обсуждают. Если шпион (его обычно называют «Евой», от английского eavesdropping — подслушивание) захочет перехватить секретный ключ, он должен будет измерять поляризацию фотонов. Поскольку он не знает базиса, он должен будет определять его случайным образом. Если базис будет определён неправильно, то Ева не получит верных данных, а кроме того, изменит поляризацию фотона. Появившиеся ошибки сразу обнаружат и Алиса, и Боб (рис. 5).

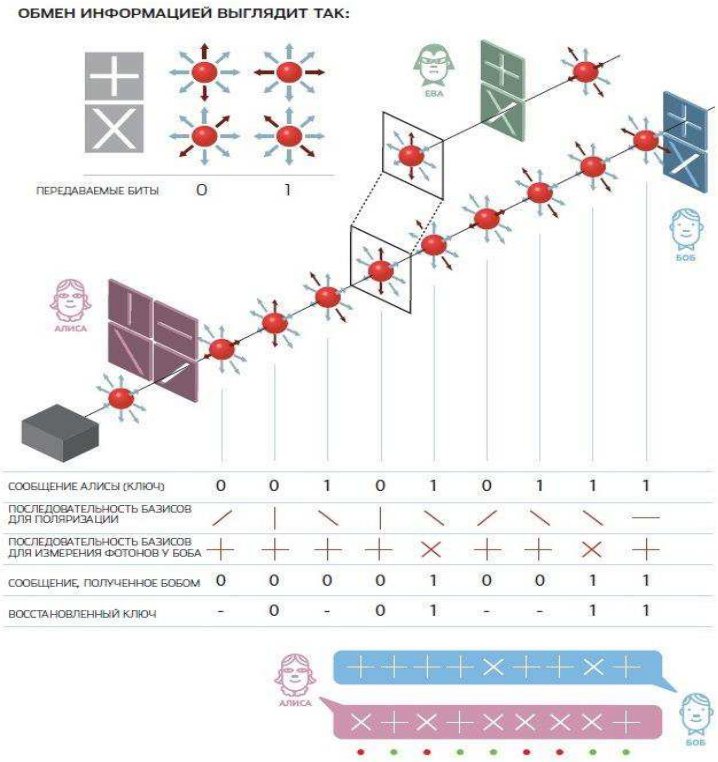

Рисунок 5 – Квантовая структура передачи фотонов

Закрытый конверт

Квантовые системы связи основаны на использовании квантовых свойств носителей информации. Если в обычных телекоммуникационных сетях данные кодируются в амплитуде и частоте излучения или электрических колебаний, то в квантовых — в амплитуде электромагнитного поля или в поляризации фотонов.

Разумеется,потребуется значительно более дорогая и сложная аппаратура, но эти ухищрения оправданны: дело в том, что передача информации по квантовым каналам обеспечивает стопроцентную защиту от «прослушки». Согласно законам квантовой механики измерение свойств того или иного квантового объекта, например измерение поляризации фотона, неминуемо меняет его состояние. Получатель увидит, что состояние фотонов изменилось, и предотвратить это нельзя в принципе — таковы фундаментальные законы природы. Это можно описать такой аналогией: представьте себе, что вы пересылаете письмо в закрытом конверте. Если кто-то откроет письмо и прочитает его, цвет бумаги изменится, и получатель неминуемо поймёт, что послание читал кто-то третий.

Самая ценная информация — это шифровальные ключи. Если ключ имеет длину, равную самому сообщению или ещё длиннее, то расшифровать послание, не зная ключа, в принципе невозможно. Показать это очень легко на примере одного передаваемого бита — единицей или нулём. Сложим его по модулю два с ключом — случайно выбранной единицей или нулём. В результате, зная только итог сложения, мы не можем сказать, что у нас было изначально: единица или ноль. Мы не можем различить сообщение и ключ, так как мы не знаем ни ключа, ни сообщения.

Современные проблемы криптосистемы

Во-первых, это проблема устройства, способного отправлять одиночные фотоны. На практике в коммерческих линиях квантовой связи часто пользуются очень слабыми лазерными импульсами, хотя прогресс в разработке однофотонных источников тоже достигнут. А во-вторых, так как передача сигнала осуществляется отдельными фотонами, возникает проблема шума. Оптоволокно по-разному нагревается (тепловые фотоны), может быть по-разному изогнуто и так далее.

Поэтому на нынешний момент существуют аппаратно-независимые пределы пропускной способности квантовой связи в зависимости от расстояния. На практике это 1,26 мегабита в секунду на расстояние 50 километров по стандартному кабелю и — сравните — 1,16 бита в час (!) на расстояние в 404 километра (символично) по специальному кабелю с ультранизкими потерями данных. К примеру, в августе 2017 китайские исследователи опубликовали в Nature результаты эксперимента по реализации протоколов квантовой криптографии между космосом и Землей. Тогда со спутника «Мо Цзы» удалось передать на расстояние в 1200 километров более 300 килобайт секретного ключа. Это стало возможно потому, что и околоземное пространство, и верхние слои атмосферы почти не шумят. По обычному оптоволокну на 1200 километров один бит просеянного ключа передавали бы около шести миллиардов лет

Рекомендации и предложения

Чтобы передавать сигнал на более далёкое расстояние, специалисты по квантовой связи работают над квантовыми повторителями. Можно подумать, что это — квантовые ретрансляторы, однако на самом деле принцип их работы совсем другой.В квантовом мире невозможно клонировать квантовое состояние. А ведь обычный ретранслятор электромагнитного сигнала (радио, например), делает именно это: воспринимает сигнал и воспроизводит его заново. С квантовым посланием так обращаться нельзя. Поэтому квантовый повторитель – это скорее обычный квантовый компьютер, который способен хранить исходный сигнал (кубит). Однако пока что квантовые повторители на практике — дело будущего.

Вывод

−В квантовой системе для усиления волн в области приемника можно использовать поляризацию фотонов (кодирование) т.е. обеспечить «запутанность», правда потребуется значительно более дорогая и сложная аппаратура, но эта технология оправданна поскольку передача информации по квантовым каналам обеспечивает стопроцентную защиту от «прослушки».

−На основе квантовой суперпозиции можно обеспечить адаптивное формирование диаграммы направленности, т.е. регистрируя сигналы, приходящие на приемник различными путями, система автоматически вычисляет положение отправителя в пространстве.

−Увеличение плотности записи информации требующий уменьшения размера области, занимаемой одним битом информации, т.е увеличение соотношения сигнал/шум в перспективе развития систем хранения информации основывается на квантовые свойства, при которой максимальная плотность возможно при умении различать отдельные атомы на поверхности, (позволяет использовать п.п материалы обладающие туннельным эффектом.

Список использованных источников

1. Килин С. Я. «Квантовая информация / Успехи Физических Наук.» – 1999.– Т. 169.– С. 507–527.

2. Румянцев К.Е., Плёнкин А. П. Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей //Телекоммуникации. 2014. №10. С. 11-16.

3. Плёнкин А. П. Использование квантовых ключей для шифрования сетевого соединения // Десятая ежегодная научная конференция студентов и аспирантов базовых кафедр Южного научного центра РАН: Тезисы докладов (г. Ростов-на-Дону, 14–29 апреля 2014 г.). — Ростов н/Д: Изд-во ЮНЦ РАН, 2014. — 410 с. — С. 81 − 82.

4. popmech.ru/technologies/235655-kvantovaya-kriptografiya-chto-eto-takoe