Эссе студента 013 группы
Скотарева Ю.С.
на тему :
«Влияние квантовой теории на криптографию»

1.Предисловие.

Данная работа - это попытка показать широкой публике лицо относительно молодой области науки, квантовой криптографии (КК). Автор не ставит себе задачу детально описать теоретические основы КК, виртуозно используя математический аппарат квантовой физики. Наоборот, математические выкладки будут сведены к минимуму, дабы не выявлять у читателей склонности к суицидальным фантазиям. Целью данной работы является описание основных принципов КК, обзор нескольких квантовых протоколов связи и тех положительных изменений, что произошли в КК за последние несколько лет.

2.Введение.

Начала квантовой криптогафии могут быть прослежены в работе Виснера (Wiesner), который предположил, что, если бы квантовые состояния могли быть изолированы и сохранены в течение длительных периодов времени, они могли бы использоваться как деньги. Виснер издал свои идеи в 1983, но они имели в большей степени академический интерес. Однако, Беннетт (Bennett) и Брассард (Brassard) понимали, что вместо того, чтобы использовать отдельные кванты для хранения информации, лучше использовать их для передачи информации. В 1984 они создали первый квантовый криптографический протокол, теперь известный как “BB84”. Дальнейший прогресс в теории квантовой криптографии, происходит в 1991, когда Экерт (Ekert) предположил, что связанные состояния Эйнштейна-Подольского-Розена (EPR) двух частиц могли бы использоваться в квантовом криптографическом протоколе. Безопасность такого протокола была основана на неравенствах Бэлла (Bell). Также в 1991, Беннетт со товарищи, продемонстрировал, что квантовое распределение ключей (КРК) практически осуществимо. Они сконструировали рабочий прототип системы протокола BB84, используя поляризованные фотоны, которые передавались в одной из 4х поляризаций.

В 1992 Беннетт опубликовал “минимальную” схему КРК (назвав ее уже “B92”) и предположил, что она может быть реализована, используя передатчик одиночных фотонов и оптоволокно в качестве среды распространения фотонов на большие расстояния. В этой схеме биты ключа кодировались в 2 не ортогональных направления поляризации фотона. С тех пор были опубликованы и другие протоколы КРК, а группы ученых из Великобритании, Швейцарии, Японии и США разработали новые прототипы КРК систем.

Надежность квантовых алгоритмов передачи секретных данных базируется не на изощренных математических преобразованиях, а на законах физики, которые теоретически невозможно обойти. Квантово-криптографические системы - это побочный продукт разрабатываемого в настоящее время так называемого квантового компьютера.

Основной строительной единицей квантового компьютера является кубит (qubit, Quantum Bit). Классический бит имеет, как известно, лишь два состояния - 0 и 1, тогда как множество состояний кубита значительно больше. Это означает, что кубит в одну единицу времени равен и 0, и 1, а классический бит в ту же единицу времени равен либо 0, либо 1. Основная причина бурных исследований в области квантовых компьютеров - это естественный параллелизм квантовых вычислений. Например, если квантовая память состоит из двух кубитов, то мы параллельно работаем со всеми ее возможными состояниями: 00, 01, 10, 11. За счет возможности параллельной работы с большим числом вариантов квантовому компьютеру необходимо гораздо меньше времени для решения задач определенного класса. К таким задачам, например, относятся задачи разложения числа на простые множители, поиск в большой базе данных и др. Так, при использовании алгоритма Шора [3,4,5] для разложения на множители 256-разрядного двоичного числа компьютеру, аналогичному суперкомпьютеру Blue Gene корпорации IBM, потребуется 10 млн. лет. Квантовый компьютер способен сделать то же самое всего за 10 секунд.

Бурное развитие квантовых технологий и волоконно-оптических линий связи привело к появлению квантово-криптографических систем. Они являются предельным случаем защищенных ВОЛС. Использование квантовой механики для защиты информации позволяет получать результаты, недостижимые как техническими методами защиты ВОЛС, так и традиционными методами математической криптографии. Защита такого класса применяется в ограниченном количестве, в основном для защиты наиболее критичных с точки зрения обеспечения безопасности систем передачи информации в ВОЛС.

3.Основные принципы КК.

При переходе от сигналов, где информация кодируется импульсами, содержащими тысячи фотонов, к сигналам, где среднее число фотонов, приходящихся на один импульс, много меньше единицы (порядка 0,1), вступают в действие законы квантовой физики. Именно на использовании этих законов в сочетании с процедурами классической криптографии основана природа секретности квантового канала связи (ККС). В квантово-криптографическом аппарате применим принцип неопределенности Гейзенберга, согласно которому попытка произвести измерения в квантовой системе вносит в нее нарушения, и полученная в результате такого измерения информация определяется принимаемой стороной как дезинформация.

Итак, две конечных цели квантовой (как и классической) криптографии:

1) обеспечить отправителю и адресату защищенный канал обмена информацией;
2) обеспечить механизм проверки секретности такого обмена.

Секретным и абсолютно защищенным, в принципе, можно сделать любой канал передачи информации. Достаточно лишь чтоб обмен шел сообщениями, зашифрованными криптостойким шифром и качественным секретным ключом. Секретным считаем ключ, известный лишь отправителю и адресату. Качественный ключ - представляет собой абсолютно случайную последовательность 0 и 1.

Основное применение квантовой криптографии - быстрое и безопасное получение общего (для адресата и отправителя) секретного ключа. Используя этот секретный ключ, участники обмена могут абсолютно спокойно общаться по открытому (незащищенному) каналу связи.

За относительно недолгое время существования квантовой криптографии разработано несколько квантовых протоколов, или, другими словами, алгоритмов выработки общего секретного ключа (ОСК) с помощью квантов и квантовых каналов связи (ККС).

4.Квантовые протоколы.

1) Квантовый протокол BB84.

Система включает передатчик и приемник. Передатчик может использовать генератор, чтобы посылать фотоны в одной из четырех поляризаций: 0, 45, 90, или 135 градусов, выбираемой в зависимости от передаваемого бита (90 или 135 для "1"; 45 или 0 для "0"). Приемник на другом конце использует фиксатор, чтобы измерять поляризацию. Согласно законам квантовой механики, приемник может различать вид прямолинейной поляризации (0 или 90), или вид диагональной поляризации (45 или 135); тем не менее, различить оба типа он не может никогда.

Распределение ключей требует несколько шагов.

а) Передатчик посылает фотоны с одной из четырех поляризаций, которая выбирается произвольно.
б) Для каждого поступающего фотона, получатель выбирает произвольно тип измерения: прямолинейный или диагональный. Получатель записывает результаты измерений, но держит их в секрете.
с) Получатель публично (по открытому каналу) заявляет использованный тип измерения для каждого фотона (но не результаты).
д) Передатчик сообщает получателю (опять по открытому каналу), какие замеры были правильного типа.
е) Пользователи (передатчик и получатель), выбирают все случаи, в которых замеры

получателя были правильного типа. Эти случаи - затем переводят в биты (1 и 0) и таким образом получают ключ.

Злоумышленник, пытающийся перехватить сообщение, обязательно вызовет ошибки в этой передаче, поскольку он не знает заранее тип поляризации каждого фотона, а квантовая механика не позволит ему замерить тип поляризации двух несвязанных между собой видов (прямолинейная и диагональная поляризация). Два законных пользователя квантового канала тестируют его на возможность подслушивания, показывая по открытому каналу произвольное подмножество ключевых битов и проверяя уровень ошибок. Хотя они не могут предотвратить подслушивания, они никогда не могут быть обмануты злоумышленником, поскольку любое подключение к каналу будет обнаружено.

Предположим, что злоумышленник разрезал кабель и выполняет измерения с помощью оборудования, аналогичного оборудованию адресата. После этого он посылает получателю фотон в соответствии с результатами своих измерений (используя оборудование, аналогичное оборудованию передатчика). Тогда в 50% случаев злоумышленник выберет неверный анализатор, и будет посылать адресату фотоны в случайно выбранных состояниях. В результате 25% битов ключевой информации будут отличаться у отправителя и адресата.

Теперь пользователи смогут узнать о присутствии злоумышленника посредством случайного выбора половины битов строки ключа (длиной N бит) и публичного оглашения их значений. Если все объявленные значения совпадают, пользователи могут быть уверены, что их никто не подслушивал, поскольку вероятность того, что их подслушивали, а они выбрали N/2 битов с ненарушенным состоянием, равна: $(3/4)^{N/2} \sim= 10^{-125}$, при N=1000.

На практике протокол является более сложным, поскольку злоумышленник может использовать различные стратегии подслушивания (например, не перехватывать все кубиты); кроме того, даже при отсутствии прослушивания, помехи неизбежно исказят некоторые из кубитов. Вместо отказа от ключа в случае, когда многие из оглашенных битов не совпадают, Алисе и Бобу нужно пользоваться им до тех пор, пока уровень ошибок не превысит 25%.

Последующая обработка ключа состоит из двух шагов:
Первый шаг заключается в обнаружении и удалении ошибок посредством публичной проверки на совпадение значений битов из случайно выбранных последовательностей; с одновременным отказом от битов с целью не допустить получения злоумышленником дополнительной информации.
На втором шаге из данного ключа выделяется другой, меньший по длине, составленный из совпадающих значений первоначального ключа. При этом знания злоумышленника о ключе уменьшаются. Таким образом, можно получить новый ключ, составленный примерно из N/4 битов, при этом с большой вероятностью знания подслушивающего о данном ключе составляют менее 10^{-6} бита (Bennett, 1992).

2) Квантовый протокол B92.

Для представления нулей и единиц в этом протоколе используются фотоны, поляризованные в 2-х различных направлениях.

Отправитель использует 2-а поляризационных фильтра для кодировния битов. Причем угол между направлениями поляризации этих фильтров равен 45 градусов (например 0 и 45), т.е. эти направления неортогональны.

Получатель использует фильтры с углами 90 и 135 градусов для приема фотонов. Если различие в поляризации фотона и фильтр составляет 90 градусов, фотон не проходит через фильтр. При различии в поляризации составляющем 45 градусов вероятность прохождения фотона через фильтр составляет 0.5.

Итак, рассмотрим всю последовательность действий протокола B92:

а) Источник передает информацию через 2 фильтра с ориентацией на 0 и +45 градусов, представляющие нули и единицы.

б) Фильтры адресата сориентрованы на 90 и 135 градусов. Инициатор обмена посылает адресату последовательность случайно сориентированных фотонов, представляющих нули и единицы.
в) Для определения поляризации получатель пропускает фотоны, через тот или другой фильтр. Допустим, что через один из фильтров (например 135 гр.) фотон не проходит. Адресат не знает, что послано ему: 1, соотвествующая фотону, который не проходит, или 0, соответствующий фотону, который не проходит с вероятностью 0.5. Если же фотон проходит через фильтр, адресат уверен, что принят фотон, соответствующий 0. Если фотон принят удачно, очередной бит ключа кодируется 0 или 1 в соответствии с примененным фильтром.
г) Легко подсчитать, что адресат получкет примерно 1/4 из переданных ему фотонов.
д) Получив последовательность, адресат может, не таясь (по телефону например), передать отправителю, какие именно 25 из каждых 100 фотонов получены. Они послужит ключом для последуюшего сообщения. При этом не называются фильтры и полученые значения поляризации. Поэтому если злоумышленник и подслушает телефонный разговор, он не сможет составить ключ.
е) После успешной передачи ключа отправитель может открыто посылать свои сообщения, закодированные этим ключом. Никто, кроме адресата, не сможет их раскодировать.

Перехват сообщения-ключа злоумышленником пользователи могут обнаружить посредством контроля ошибок. Для этого они (также как и в BB84) сверяют случайно выбранные из ключа биты. При обнаружении несовпадения в каком-либо из них, что может указывать на перехват сообщения, процедура передачи ключа повторяется. Если совпадают все проверяемые биты, ключ принимается в эксплуатацию.

3) Квантовый протокол, преложенный Экертом.

В 1991 году Экерт (Ekert) предложил использовать для выработки общего секретного ключа корреляцию (связь) квантовых частиц. Впервые это свойство было теоретически предсказано в парадоксе Эйнштейна-Подольского-Розена (EPR, 1935), а позже объяснено Белл'ом (Bell, 1969). Коррелированные частицы (или EPR - частицы) находятся в синглетном состоянии. Волновая функция системы таких частиц:
$|Y> = (1/2)^{1/2} \bullet (|0>|1> - |1>|0>)$

Здесь записано поведение частиц согласно парадоксу EPR при их измерении. Как только становится известно состояние одной частицы из этой пары (например, проводится измерение по какому-либо базису), со 100 процентной вероятностью можно вычислить состояние второй частицы. Причем, состояния частиц окажутся взаимноортоганальны. Если измерение состояния первой частицы дало |0>, то измерение второй частицы в этом же базисе даст |1>.

Для работы протокола Экерта необходимо устройство, генерирующие пары таких EPR частиц. Кроме того необходимы: каналы передачи квантов к участникам формирования секретного ключа, а у самих участников должно быть оборудование, позволяющие замерять состояние полученной частицы.

а) Устройство генерирует пару связанных частиц (A и B).
б) Частица A направляется 1-му пользователю (традиционно назовем его Алисой), а частица B - второму (также по-традиции назовем его Боб).
в) Алиса и Боб замеряют свои частицы. Результаты замеров должны согласоваться с парадоксом EPR и неравенством Белла.
г) Часть битов полученной последовательности пользователи сверяют по открытому каналу. Если они не обнаружат нарушений квантовой кореляции, оставшиеся неоглашенными биты объявляются ключом.
Замечание: один из участников обмена должен инвертировать полученную последовательность.

Допустим шпион перехватил канал передачи квантов и измеряет состояния квантов. Но откуда ему знать в каком базисе нужно проводить измерения? Таким образом, минимум в

50% случаев злоумышленник нарушает корреляцию EPR. Присутствие злоумышленника обнаруживается, также как и в BB84, по большому числу ошибок в ключевой последовательности.

4) Протокол плотного кодирования.

Предположим, что существует устройство, которое генерирует кореллированные пары кубитов, находящихся в состоянии |00>+|11> (с этого момента для простоты записи будем опускать коэффициент нормирования, равный корню квадратному из 2), и направляет один кубит из каждый пары для хранения Алисе, а другой - Бобу. До этого Алисе и Бобу никогда не требовалось устанавливать связь друг с другом. В этом случае Алиса может сообщить Бобу информацию о двух классических битах посредством передачи только одного кубита (т.е. передачи своей части зацепленной пары). Объясняется это тем, что для четырех взаимно ортогональных состояний |00> + |11>, |00> - |11>, |01> + |10>, |01> - |10> переход от одного состояния к другому может быть обеспечен посредством операций с одним кубитом. Данный набор состояний называется базисом Белла, поскольку они проявляют наиболее сильную корреляцию Bell-EPR из всех возможных (Braunstein et. al. 1992). Начиная с состояния |00> + |11>, Алиса может получить любое из состояний базиса Белла посредством воздействия на имеющийся кубит одним из квантовых гейтов {1, X, Y, Z}. Поскольку существует только четыре возможных операции, то выбор воздействия будет определять два бита классической информации.

Рассмотрим протокол плотного кодирования по шагам:

а) Алиса и Боб получают от устройства генерации по одному кубиту (a и b) из связаной пары .

б) Алиса воздействует на свой кубит a квантовым гейтом. Какой гейт применить зависит от 2-х бит передаваемой информации.

в) После получения кубита от Алисы Боб должен определить в каком из состояний базиса Белла находятся кубиты. Это можно сделать посредством воздействия на пару кубитов гейтом XOR и измерения результирующего бита (target bit). Таким образом, Боб отличит состояния |00>+-|11> от состояний |01>+-|10>.

г) Для определения знака суперпозиции Боб должен использовать для оставшегося кубита преобразование Адамара "H" [например 7], а затем произвести измерение результата. Итак, Боб однозначно получает информацию о двух классических битах.

Плотное кодирование сложно осуществимо. Есть даже мнение, что оно не имеет практического значения, кроме стандартного метода связи. Однако это не так. Данный протокол обеспечивает защиту связи: получить информацию, содержащуюся в двух передаваемых классических битах, можно только в том случае, если кто-либо обладает кубитом, парным к кубиту, отправляемому Алисой. Таким образом злоумышленик должен перехватить и кубит, предназначенный Бобу от центра генерации пар кубитов, и кубит, пересылаемый Алисой Бобу. Очевидно, что эти кубиты будут передаваться по разным ККС. Кроме того, перехватив хотя бы один кубит, злоумышленник обнаружит себя, т.к. кубит, переданный им взамен перехваченного, не будет кореллирован со вторым кубитом.

Злоумышленник может отправлять Бобу вместо перехваченных пар кубитов другие сцепленные пары. В этом случае сообщение от Алисы действительно может быть перехвачено. Но тогда злоумышленик также должен иметь доступ к устройству генерации сцепленных пар. Алиса и Боб также могут договориться о проверке наличия корелляции между своими кубитами. При работе злоумышленника такая проверка даст отрицательный результат примерно в 50% случаев. Кроме этого, на декодирование кубита, посылаемого Алисой, уйдет некоторое время, в которое злоумышленник не может отправить подмененный кубит. Лишь получив значения 2х битов информации, злоумышленник, проведя преобразование кубита из своей пары, сможет отослать его Бобу. Последниий же, заметив «запаздывание» кубитов в канале, заподозрит их взлом и уведомит об этом Алису.

Лабораторная демонстрация основных свойств описана Mattle et. al. (1996).

5.Обзор работ, ведущихся в области КК.

Квантовая криптография еще не вышла на уровень широкого практического использования, но делает бодрые шаги в этом направлении. В мире существует несколько организаций, где ведутся активные исследования в области квантовой криптографии. Среди них IBM, GAP-Optique, NEC, Организация развития телекоммуникаций Японии, Japan Science and Technology, Mitsubishi, Toshiba, Национальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт (Caltech), а также молодая компания MagiQ и холдинг QinetiQ, поддерживаемый британским министерством обороны. Диапазон участников — от крупнейших мировых вендоров до небольших начинающих компаний — свидетельствует о начальном периоде в формировании рыночного сегмента, когда в нем на равных могут участвовать и те, и другие.

В IBM продолжаются фундаментальные исследования в области квантовых вычислений [8], начатые группой во главе с Чарльзом Беннеттом. О практических достижениях IBM в квантовой криптографии в последние годы известно немногое; эти работы ведутся без излишней рекламы.

Особое место занимает созданная на основе Женевского университета компания GAP (Group of Applied Phisics) Optique. Компания с европейскими академическими корнями сохраняет традиции научных публикаций; для тех, кто серьезно заинтересуется квантовой криптографией, несомненно, будут интересны две статьи авторов из GAP [9,10]. Под руководством Николаса Гисина GAP-Optique совмещает теоретические исследования с практической деятельностью. Компании впервые удалось передать ключ на расстояние 67 километров из Женевы в Лозанну, воспользовавшись почти промышленным образцом аппаратуры [11].

Этот рекорд был побит компанией Mitsubishi Electric, которой удалось передать квантовый ключ на расстояние 87 километров; скорости еще очень невелики, всего 7,2 бит в секунду.

Исследования в области квантовой криптографии ведутся и в европейском исследовательском центре Toshiba Research Europe, расположенном в Кембридже. Отчасти они спонсируются английским правительством; в них участвуют сотрудники Кембриджского университета и Империал-колледжа в Лондоне. Сейчас им удается передавать фотоны на расстояние до 100 километров; есть надежда, что через два года будут выпущены коммерческие продукты.

Корпорация NEC, Организация развития телекоммуникаций Японии и компания Japan Science and Technology успешно испытали систему квантового шифрования данных с передачей на рекордное расстояние - более 100 км. Ученым удалось преодолеть трудности сохранения целостности квантовой связи, связанные с распознаванием индивидуальных фотонов, несмотря на использование стандартного оптического волокна. С применением высококачественного оптоволокна расстояние передачи можно будет увеличить до 200 км с лишним.

Компанией MagiQ Technologies в качестве кодового имени средства для распределения ключей (quantum key distribution, QKD) избрано имя племени индейцев навахо. Navajo способен в реальном времени генерировать и распространять ключи средствами квантовых технологий, он должен обеспечивать защиту от внутренних и внешних злоумышленников. По сообщениям [12], Navajo уже прошла стадию бета-тестирования и является первой коммерчески доступной системой, в которой индивидуальные фотоны используются для передачи числовых ключей. Вице-президентом MagiQ является Алексей Трифонов, наш соотечественник, защитивший докторскую диссертацию Санкт-Петербургском университете в 2000 году.

QinetiQ — своего рода исследовательская корпорация, поддерживаемая министерством обороны Великобритании. Она появилась на свет в результате деления британского агентства DERA (Defence Evaluation and Research Agency) в 2001 году, вобрав в себя все неядерные оборонные исследования. В силу этой специфики в QinetiQ не особенно расположены делиться своими достижениями. Однако, известно [12], что QinetiQ и национальная лаборатория США в Лос-Аламосе, проводили эксперименты по передаче квантовых ключей по воздуху, а не по оптоволоконным каналам.

Литература.

1) Владимир Красавин. Квантовая криптография, http://zi.itsoft.ru.
2) Холево А. С. Введение в квантовую теорию информации // М.: МЦНМО, 2002.-128 с.
3) Nielsen M. A., Chuang I. I. Quantum Computation and Quantum Information.– Cambridge University Press, 2000.
4) Китаев А. Ю. Квантовые вычисления: алгоритмы и исправление ошибок // УМН. — 1997. — Т. 52, № 6.-С. 53-112.
5) Wehrl A. General properties of entropy // Rev. Mod. Phys.– 1978. — V. 50, №. 2. — P. 221–260.
6) Леонид Черняк. Квантовая криптография, почти реальность.Открытые системы, #07-08/2003.
7) К.Е.Борисов. Построение квантовых вычислителей, http://katpop.narod.ru/txt/quant.htm
8) Brad Huntting, David Mertz, Introduction to Quantum Computing. A guide to solving intractable problems simply. *http://www-106.ibm.com/developerworks/linux/library/l-quant.html*
9) I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, N. Gisin, Long-distance teleportation of qubits at telecommunication wavelengths. *http://www.gap-optique.unige.ch/I&Hnature.pdf*
10) Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, Hugo Zbinden, Quantum cryptography. *http://www.gap-optique.unige.ch/Publications/Pdf/QC.pdf*
11) D Stucki, N Gisin, O Guinnard, G Ribordy, H Zbinden, Quantum key distribution over 67 km with a plug&play system. http://www.gapoptic.unige.ch/Publications/Pdf/njp-2002.pdf
12) www.mignews.com.
13) www.open.ru
14) www.osp.ru