Протоколы квантового распределения ключей

Апанович Василий Юрьевич
группа МКБ18-01

apanovich@mail.ru

Квантовая криптография

Привлекательность идеи квантовой криптографии состоит в создании нового метода генерирования абсолютно случайных секретных ключей между пользователями квантовой линии связи, которые ранее никогда не встречались и не имеют общей секретной информации.

Секретность метода и невозможность незаметного съема информации с линии связи основаны на законах квантовой физики, в противоположность используемым в настоящее время методам криптографии, которые основаны на математических закономерностях и поддаются расшифровке.

Квантовое распределение ключей

Квантовое распределение ключей — метод передачи ключа, который использует квантовые явления для гарантии безопасной связи. Этот метод позволяет двум сторонам, соединенным по открытому каналу связи, создать общий случайный ключ, который известен только им, и использовать его для шифрования и расшифрования сообщений.

Важным и уникальным свойством квантового распределения ключей является возможность обнаружить присутствие третьей стороны, пытающейся получить информацию о ключе. Здесь используется фундаментальный аспект квантовой механики: процесс измерения квантовой системы нарушает её. Третья сторона, пытающаяся получить ключ, должна измерить передаваемые по каналу связи квантовые состояния, что ведет к их изменению и появлению аномалии. С помощью квантовой суперпозиции, квантовой запутанности и передачи данных в квантовых состояниях можно осуществить канал связи, который обнаруживает аномалии. Если количество аномалий ниже определённого порога, то ключ будет создан, что гарантирует безопасность (третья сторона не имеет информации об этом), иначе секретный ключ не будет создан и связь прекращается.

Обмен квантовыми ключами

Квантовая передача включает шифрование информации в квантовые состояния, или кубиты, в отличие от классической передачи, использующая биты. Как правило, используются фотоны для квантовых состояний. Квантовое распределение ключей использует определённые свойства квантовых состояний для обеспечения безопасности. Существует различные подходы квантового распределения ключей, но они могут быть разделены на две основные категории, в зависимости от свойств, которые они используют.

1. Протокол подготовки и измерения

В отличие от физики, измерение является неотъемлемой частью квантовой физики. Измерение неизвестного квантового состояние изменяет его в некотором роде. Это известно как квантовый индетерминизм и лежит в основе результатов, таких как принцип неопределенности Гейзенберга и теоремы о запрете клонирования. Это может быть использовано для того чтобы обнаружить любые прослушки на связи и, что более важно, для расчета количества информации, которая была перехвачена.

2. Протоколы, основанные на запутанности

Квантовые состояния двух (или более) отдельных объектов могут быть соединены таким образом, что они будут описываться с помощью комбинированного квантового состояния, а не как индивидуальный объект. Это называется запутанностью и означает, что измерения на один объект влияет и на другой. Если спутанная пара объектов является общей между двумя участниками, то перехват любого объекта меняет систему в целом, раскрывая присутствие третьих лиц (и количество информации, которое они получили).

История возникновения

Впервые квантовая криптография была предложена Стивеном Визнером. В Колумбийском университете, в начале 1970-х ввел понятие квантового сопряженного кодирования. Его основополагающая статья была отклонена журналом IEEE Information Theory, так как изложенные в ней предположения казались фантастическими, а не научными. Однако в 1983 году его работа «Conjugate coding» была опубликована в Sigact News и получила высокую оценку в научных кругах.

Спустя десятилетие Чарльз Беннет (IBM) и Жиль Брассар (Монреальский университет), знакомые с работой Визнера, предложили передавать секретный ключ с использованием квантовых объектов. В 1984 году они предположили возможность создания фундаментально защищённого канала с помощью квантовых состояний. После этого ими была предложена схема (BB84), в которой легальные пользователи (Алиса и Боб) обмениваются сообщениями, представленными в виде поляризованных фотонов, по квантовому каналу.

ПРИНЦИПЫ КВАНТОВОЙ КРИПТОГРАФИИ

Основу для квантовой криптографии составляют следующие главные квантово-механические принципы:

Принцип 1. Невозможность различить абсолютно надёжно два неортогональных квантовых состояния.

Принцип 2. Теорема запрета на клонирование. Благодаря унитарности и линейности квантовой механики, невозможно создать точную копию неизвестного квантового состояния без воздействия на исходное состояние.

Принцип 3. Квантовое запутывание. Две квантово-механические системы (даже разделённые пространственно) могут находиться в состоянии корреляции, так что измерение выбранной величины, осуществляемое над одной из систем, определит результат измерения этой величины на другой.

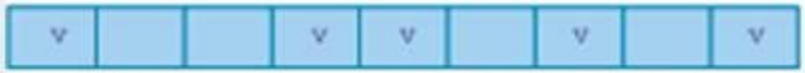
ПРОТОКОЛ КВАНТОВОЙ КРИПТОГРАФИИ BB84

Алиса посылает фотоны, имеющие одну из четырех возможных 0, 45, 90 или 135° поляризаций, которую она выбирает случайным образом

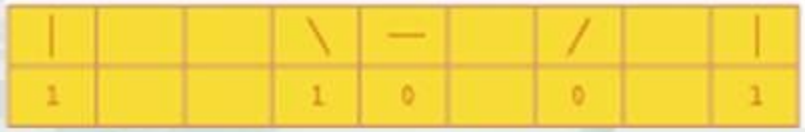
Для каждого фотона Боб выбирает случайным образом тип измерения: он изменяет либо прямолинейную поляризацию (+) , либо диагональную (×)

Боб записывает результаты изменения и сохраняет в тайне

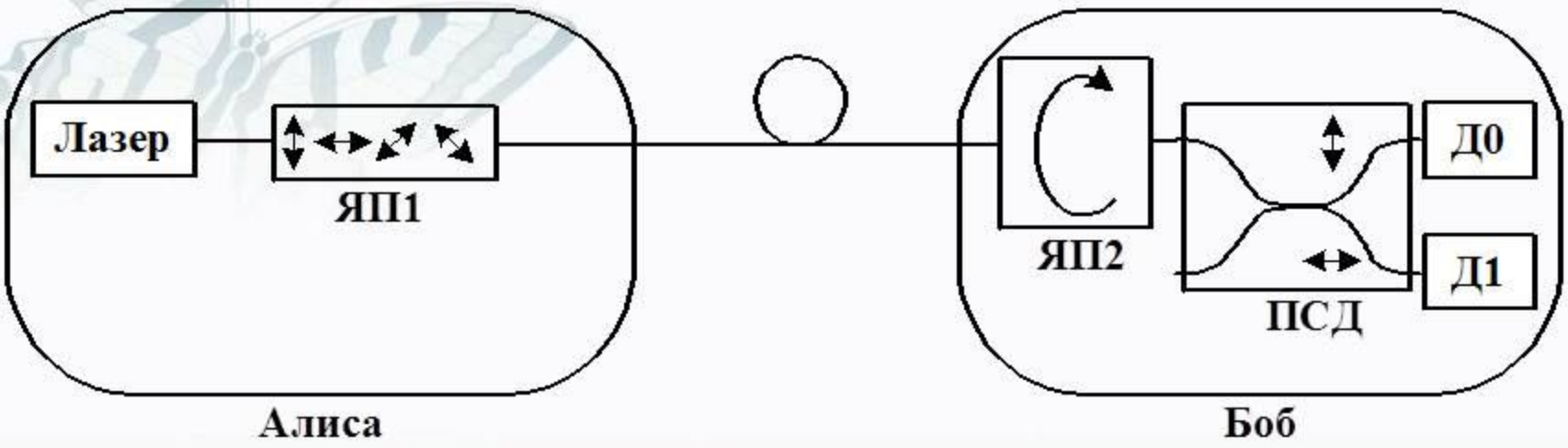
Боб открыто объявляет, какого типа измерения он проводил, а Алиса сообщает ему, какие измерения были правильными

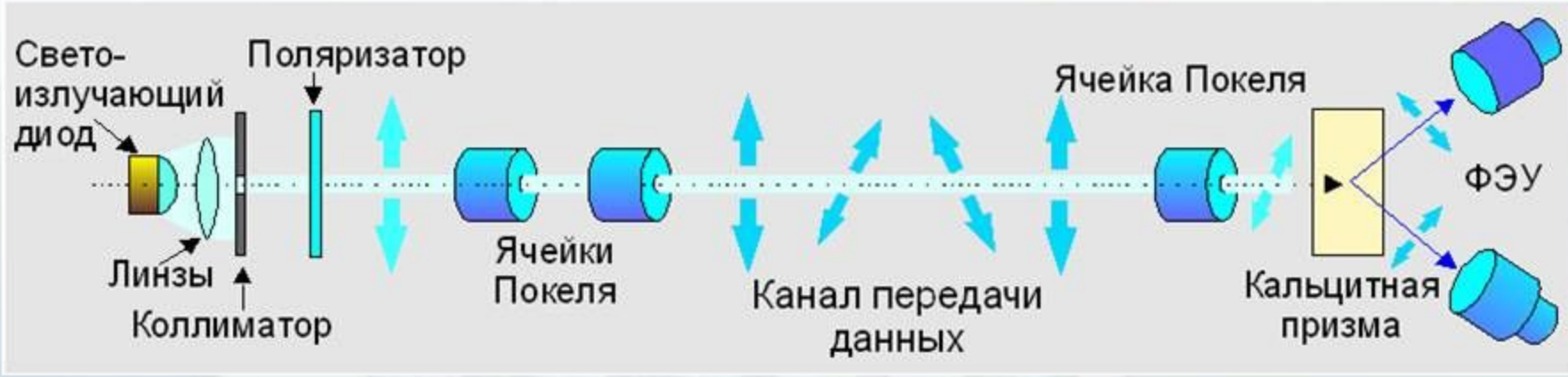


Алиса и Боб сохраняют все данные, полученные в тех случаях, когда Боб применял правильное измерение. Эти данные затем переводятся в биты (0 и 1), последовательность которых и является результатом первичной квантовой передачи



КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧА С ПОЛЯРИЗАЦИОННЫМИ СОСТОЯНИЯМИ ФОТОНОВ (ПРОТОКОЛ BB84)





ЭПР-протокол

В 1991 году Артур Экерт разработал квантовый протокол, основанный на свойствах так называемых «запутанных» состояний квантовых частиц.

Для этого он использовал пару частиц, называемых ЭПР-парой (где ЭПР означает Эйнштейн-Подольский-Розен, которые представили в статье 1935 года одноимённый парадокс). В этой статье они рассмотрели пространственно разделённые пары частиц (ЭПР-пары), чьи состояния связаны между собой таким образом, что измерение выбранной наблюдаемой одной частицы автоматически определяет результат измерения этой же наблюдаемой другой частицы. При этом, пространственная разделённость ЭПР-пар позволяет говорить о «действии на расстоянии» (дальнодействии).

Многомировая интерпретация парадокса ЭПР

Наглядную трактовку парадокса ЭПР даёт многомировая интерпретация. Состояние частиц A и B после распада частицы C представляет собой квантовую суперпозицию всевозможных состояний, отличающихся различными значениями импульса частицы A. Согласно Девитту, это можно интерпретировать как суперпозицию состояний одинаковых не взаимодействующих между собой параллельных вселенных, каждая из которых содержит «альтернативную историю» распада частицы C и характеризуется своим значением импульса pA. Пока не проведено измерение, невозможно установить, в какой именно из этих вселенных осуществляется эксперимент. В момент измерения происходит необратимое «расщепление вселенных», и история обеих частиц A и B с самого распада становится определённой. В рамках этой интерпретации проведение измерения над частицей A не оказывает влияния на состояние частицы B, и противоречие с принципом причинности отсутствует.

Формулировка темы научной работы

Разработка и исследование протоколов квантового распределения ключей и используемых в них алгоритмов.

Благодарю за внимание!