# Лекция 10. Квантовая криптография

## Общее описание

Квантовая криптография — метод защиты коммуникаций, основанный на принципах квантовой физики (информация переносится с помощью объектов квантового микромира – фотоны и электроны).

Традиционная криптография использует **математические методы**, а квантовая криптография сосредоточена на **физических свойствах квантовых частиц**.

## Принцип неопределенности Гейзенберга

Технология квантовой криптографии опирается на принципиальную неопределённость поведения квантовой системы - невозможно одновременно точно измерить сопряженные характеристики. Например, измерить:

- **координаты и импульс частицы**

- ток и напряжение,

- электрическое и магнитное поля

- один параметр фотона, не исказив другой

1927 – Гейзенберг - Принцип неопределённости: dx\*dp<=~~h~~/2

Постоя́нная Дира́ка (редуцированная/ рационализированная/ приведённая постоянная Планка): ~~h~~= h/2\*pi

связывает угловую частоту omega = 2\*pi\*nu (где nu — частота фотона или другого кванта) с его энергией: E=~~h~~\*omega.

h — (нередуцированная) постоянная Планка.

Постоянная нижняя граница произведения «неопределённостей» двух **сопряжённых характеристик**

Принцип непоняток Гейзенберга — метафизическая аксиома, не позволяющая одновременно знать точный ответ на все наиболее интересующие тебя вопросы. Зависимость между **числом ответов** и их **точностью** обратно пропорциональна.

Популярной надписью на стенах физических факультетов является: «Здесь, возможно, был Гейзенберг».

**Цель** – создать систему связи, способную обнаруживать подслушивание (попытка измерения взаимосвязанных параметров в квантовой системе вносит в неё нарушения, а значит, по помехам в канале легитимные пользователи могут распознать степень активности перехватчика).

Используется как средство для распространения ключей (quantum key distribution, QKD).

## История

1970 - Стивен Визнер - идея использования квантовых объектов

1980 - Чарльз Беннет (IBM) и Жиль Брассар (Монреальский университет) - предложили передавать секретный ключ квантовыми объектами - «квантовое распространение ключа» (quantum key distribution)

1984- предложили схему BB84:

- легальные пользователи обмениваются сообщениями в виде поляризованных фотонов

- злоумышленник при измерении фотонов искажает сообщение

- легальные пользователи выявляют перехват по открытому каналу, обсуждая сигналы, переданные по квантовому каналу для определения

-> нет ошибок - секретность соблюдена

## Схема ВВ84

Фотоны могут иметь ортогональную (+) или диагональную (Х) поляризацию

Информация кодируется в ортогональные квантовые состояния.

Принцип: криптоаналитик (Ева) не может измерить диагональную и ортогональную поляризацию одного и того же фотона, поэтому после перехвата Ева с вероятностью 50% вернет в канал ошибку.

Алгоритм:

1. отправитель и получатель выбирают схему кодирования битов поляризованными фотонами: выбор из ортогональной и диагональной 0 (0b), 45 (0b), 90 (1b)и 135°(1b).
2. первичная квантовая передача
   1. отправитель (Алиса) выбирает свой набор поляризаторов (ортогональных (+) или диагональных (х)) для каждого **передаваемого** бита (случайно) и передает по квантовому каналу фотоны с выбранной поляризацией

https://upload.wikimedia.org/wikipedia/commons/f/f3/FrameSmall2.gif

https://upload.wikimedia.org/wikipedia/commons/3/37/FrameSmall3.gif

* 1. получатель (Боб) выбирает свой набор поляризаторов для каждого **принимаемого** бита (случайно) и принимает фотоны из квантового канала
  2. получатель по открытому каналу сообщает о том, какой способ он выбрал для каждого фотона (результаты измерения в секрете)
  3. отправитель по открытому каналу сообщает, для каких фотонов был выбран правильный поляризатор.

[FrameSmall4.gif](https://commons.wikimedia.org/wiki/File:FrameSmall4.gif?uselang=ru)

* 1. отбрасываются те биты, для которых поляризаторы выбраны неверно.

[FrameSmal5.gif](https://commons.wikimedia.org/wiki/File:FrameSmal5.gif?uselang=ru)

Если не было компрометации квантового канала, то секретной информацией будут оставшиеся биты.

1. сверка полученных данных

Несовпадение данных означает перехват – требуется новая первичная квантовая передача.

С вероятностью 1 — 2-k (где k — число сравненных битов) канал не прослушивался.

В 1991 году Беннет предложил алгоритм выявления искажений данных:

1. данные разбиваются на блоки длины k. Где k выбирается так, чтобы минимизировать вероятность ошибки.
2. отправитель и получатель определят четность каждого блока, и сообщают её друг другу по открытому каналу связи.
3. отправитель и получатель в каждом блоке удаляют последний бит и повторяют проверку
4. если четность сверяемых блоков различается, отправитель и получатель производят итерационный поиск неверных битов и исправляют/исключают их.
5. выбирается большее значение k и проверка повторяется (чтобы исключить ранее незамеченные кратные ошибки).
6. для контроля проводится псевдослучайная проверка (отправитель и получатель открыто сообщают о произвольной перестановке половины бит в строках, а затем вновь открыто сравнивают четности (Если строки различны, четности обязаны не совпадать с вероятностью 0,5)).
7. если четности отличаются, отправитель и получатель производят двоичный поиск и удаляют неверные биты.

Если различий не наблюдается, после n итераций отправитель и получатель будут иметь одинаковые строки с вероятностью ошибки 2-n.

## Физические реализации

### Квантовый поток (ячейки Покеля)

Отправитель

**Ячейки Покеля** позволяют импульсно варьировать поляризацию (4 возможных состояния) излучаемого квантового потока.

**На ячейки данные поступают в виде управляющих сигналов**.

Канал связи - **волокно**, источник света - **лазер**

Получатель

После **ячейки Покеля** расположена кальцитовая призма: **расщепляет пучок** на два **фотодетектора** (ФЭУ) для **измерения ортогональных составляющих поляризации**

**Проблема интенсивности** передаваемых импульсов квантов

Секретность данных зависит от интенсивности вспышек света передатчика:

* **Слабые вспышки** усложняют перехват сообщений, но приводят к росту числа ошибок у легального пользователя (снижается число успешно долетевших фотонов).
* **Повышение интенсивности** вспышек упрощает перехват путем расщепления начального одиночного фотона (или пучка света).

Если в импульсе 1000 квантов, вероятно, что 100 из них будут отведены криптоаналитиком на свой приёмник – проанализировав открытые переговоры, можно получить переданные данные.

Если в импульсе количество квантов стремится к одному, любая попытка перехватить кванты изменит сигнал, увеличив число ошибок у получателя.

Чувствительность приёмника повышается до максимума, и встает проблема «темного» шума (получатель принимает сигнал, который не был отправлен отправителем).

Для повышения надёжности логические нули и единицы представляются в виде **не одного, а последовательности частиц**, что позволяет исправлять одинарные/кратные ошибки.

### Сферический атом. Эффект Эйнштейна-Подольского-Розена

Экерт предлжил: сферический атом излучает в противоположных направлениях два фотона. Начальная поляризация фотонов не определена, но в силу симметрии их поляризации всегда противоположны (узнается после измерения).

Схема:

1. Отправитель генерирует несколько фотонных пар
2. Один фотон из каждой пары он откладывает себе, а второй пересылает адресату (если у отправителя фотон с поляризацией «1», то у получателя будет фотон с поляризацией «0» и наоборот)

Легальные пользователи получают одинаковые псевдослучайные последовательности.

Проблема: на практике эффективность регистрации и измерения поляризации фотона очень мала.

Для решения проблем предлагались различные практические реализации метода.

## Практические реализации

1. 1989 (Исследовательский центр IBM): Первая **работающая** квантово-криптографическая схема построена Беннетом и Брассаром.

Передатчик и приемник размещены на концах оптического канала (свободный воздушный канал длиной около 32 см) в светонепроницаемом кожухе размерами 1,5×0,5×0,5 м.

Проблема: при увеличении расстояния между приёмником и передатчиком не сохранялась поляризация фотонов.

1. 1995? - Компния GAP-Optique (создана при участии Женевского университета под руководством Николаса Гисина) реализовала квантовый канал связи с помощью оптоволоконного кабеля длинной 23 км, проложенного по дну озера между Женевой и Нионом.

Сгенерировали секретный ключ, уровень ошибок которого не превышал 1,4%.

Проблема: малая скорость передачи информации

Середина 90-х (Университет Женевы - профессор Николя Жизен) передали ключ на 67 км из Женевы в Лозанну с помощью почти промышленного образца аппаратуры.

Mitsubishi Electric передала квантовый ключ на 87 км на скорости в 1 байт в секунду.

1. В национальной лаборатории Лос-Аламоса разработана линия связи длиной около 48 километров со скоростью распределения ключей достигает несколько десятков кбит/с.
2. 2001 - (Эндрю Шилдс - TREL и Кембриджский университет) создан диод, способный испускать единичные фотоны («квантовая точка» — миниатюрный кусочек полупроводникового материала диаметром 15 нм и толщиной 5 нм, который при подаче на него тока захватывать лишь по одной паре электронов и дырок). При демонстрации удалось передать данные со скоростью **75 Кбит/с** (более половины фотонов терялось).
3. Университет Джона Хопкинса – на квантовом канале в 1 км построена вычислительная сеть, в которой каждые 10 минут производится автоматическая подстройка. В результате этого, уровень ошибки снижен до 0,5 % при скорости связи 5 кбит/с.
4. Министерством обороны Великобритании поддерживается исследовательская корпорация QinetiQ, являющаяся частью бывшего британского агентства DERA (Defence Evaluation and Research Agency), которая специализируется на неядерных оборонных исследованиях и активно совершенствует технологию квантового шифрования.
5. Magiq Technologies – выпустила прототип коммерческой квантовой криптотехнологии собственной разработки, названное Navajo (способен в реальном времени генерировать и распространять ключи).
6. Октябрь 2007 года Id Quantique (Швейцария) - на выборах использованы квантовые сети (от избирательных участков до датацентра ЦИК).
7. 2011 год (Токио) – проект «Tokyo QKD Network», квантовое шифрование в телекоммуникационных сетях – обычные оптоволоконные кабели (проведена пробная телеконференция на расстоянии в 45 км). Панировуется применение для мобильной связи.

## Уязвимость реализаций квантовой системы

Слабость: фотодиоды должны реагировать на одиночные фотоны –высокая чувствительность. Но если засветить их, можно манипулировать как принимаемым, так отправляемыми сигналами.

В 2010 году учёные успешно опробовали[[4]](https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F#cite_note-vzlom-4)[[5]](https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F#cite_note-vzlom2-5) один из возможных способов атаки, показав принципиальную уязвимость двух реализаций криптографических систем, разработанных компаниями ID Quantique и MagiQ Technologies[[6]](https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F" \l "cite_note-6). И уже в 2011 году работоспособность метода была проверена в реальных условиях эксплуатации, на развёрнутой в Национальном университете Сингапура системе распространения ключей, которая связывает разные здания отрезком оптоволокна длиной в 290 м.

В эксперименте использовалась физическая уязвимость четырёх однофотонных детекторов (лавинных фотодиодов), установленных на стороне получателя ([Боба](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B8%D1%81%D0%B0,_%D0%91%D0%BE%D0%B1_%D0%B8_%D0%95%D0%B2%D0%B0)). При нормальной работе фотодиода приход фотона вызывает образование электронно-дырочной пары, после чего возникает лавина, а результирующий выброс тока регистрируется компаратором и формирователем импульсов. Лавинный ток «подпитывается» зарядом, хранимым небольшой ёмкостью (≈ 1,2 пФ), и схеме, обнаружившей одиночный фотон, требуется некоторое время на восстановление (~ 1 мкс).

Если на фотодиод подавать такой поток излучения, когда полная перезарядка в коротких промежутках между отдельными фотонами будет невозможна, амплитуда импульса от одиночных квантов света может оказаться ниже порога срабатывания компаратора.

В условиях постоянной засветки лавинные фотодиоды переходят в «классический» режим работы и выдают фототок, пропорциональный мощности падающего излучения. Поступление на такой фотодиод светового импульса с достаточно большой мощностью, превышающей некое пороговое значение, вызовет выброс тока, имитирующий сигнал от одиночного фотона. Это и **позволяет криптоаналитику (**[**Еве**](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B8%D1%81%D0%B0,_%D0%91%D0%BE%D0%B1_%D0%B8_%D0%95%D0%B2%D0%B0)**) манипулировать результатами измерений**, выполненных [Бобом](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B8%D1%81%D0%B0,_%D0%91%D0%BE%D0%B1_%D0%B8_%D0%95%D0%B2%D0%B0): она «**ослепляет**» все его детекторы с помощью лазерного диода, который работает в непрерывном режиме и испускает свет с круговой поляризацией, и по мере надобности добавляет к этому линейно поляризованные импульсы. При использовании четырёх разных лазерных диодов, отвечающих за все возможные типы поляризации (вертикальную, горизонтальную, ±45˚), Ева может искусственно генерировать сигнал в любом выбранном ею детекторе [Боба](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B8%D1%81%D0%B0,_%D0%91%D0%BE%D0%B1_%D0%B8_%D0%95%D0%B2%D0%B0).

Опыты показали, что схема взлома работает очень надёжно и даёт [Еве](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B8%D1%81%D0%B0,_%D0%91%D0%BE%D0%B1_%D0%B8_%D0%95%D0%B2%D0%B0) прекрасную возможность получить точную копию ключа, переданного [Бобу](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B8%D1%81%D0%B0,_%D0%91%D0%BE%D0%B1_%D0%B8_%D0%95%D0%B2%D0%B0). Частота появления ошибок, обусловленных неидеальными параметрами оборудования, оставалась на уровне, который считается «безопасным».

Однако, устранить такую уязвимость системы распространения ключей довольно легко. Можно, к примеру, установить перед детекторами [Боба](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B8%D1%81%D0%B0,_%D0%91%D0%BE%D0%B1_%D0%B8_%D0%95%D0%B2%D0%B0) источник одиночных фотонов и, включая его в случайные моменты времени, проверять, реагируют ли лавинные фотодиоды на отдельные кванты света.

## Plug & Play

Практически все квантово-оптические криптографические системы сложны в управлении и с каждой стороны канала связи **требуют постоянной подстройки**. На выходе канала возникают беспорядочные колебания поляризации ввиду воздействия внешней среды и двойного лучепреломления в оптоволокне. Но недавно[[*когда?*](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%98%D0%B7%D0%B1%D0%B5%D0%B3%D0%B0%D0%B9%D1%82%D0%B5_%D0%BD%D0%B5%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%91%D0%BD%D0%BD%D1%8B%D1%85_%D0%B2%D1%8B%D1%80%D0%B0%D0%B6%D0%B5%D0%BD%D0%B8%D0%B9)] была сконструирована[[*кем?*](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%98%D0%B7%D0%B1%D0%B5%D0%B3%D0%B0%D0%B9%D1%82%D0%B5_%D0%BD%D0%B5%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%91%D0%BD%D0%BD%D1%8B%D1%85_%D0%B2%D1%8B%D1%80%D0%B0%D0%B6%D0%B5%D0%BD%D0%B8%D0%B9)] такая реализация системы, которую смело можно назвать [plug and play](https://ru.wikipedia.org/wiki/Plug_and_Play) («подключай и работай»). Для такой системы не нужна подстройка, а **только синхронизация**. Система построена на использовании **зеркала Фарадея**, которое позволяет избежать двойного лучепреломления и как следствие не требует регулировки поляризации. Это позволяет пересылать криптографические ключи по обычным телекоммуникационным системам связи. Для создания канала достаточно лишь подключить приёмный и передающий модули, провести синхронизацию и можно начинать передачу. Поэтому такую систему можно назвать [plug and play](https://ru.wikipedia.org/wiki/Plug_and_Play).

## Перспективы развития

Сейчас одним из самых важных достижений в области квантовой криптографии является то, что ученые смогли показать возможность передачи данных по квантовому каналу со скоростью до единиц Мбит/с. Это стало возможно благодаря технологии разделения каналов связи по длинам волн и их единовременного использования в общей среде. Что кстати позволяет одновременное использование как открытого, так и закрытого канала связи. Сейчас[[*уточнить*](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D1%82%D0%B5%D1%82%D0%BD%D1%8B%D0%B5_%D0%B8%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B8)] в одном оптическом волокне возможно создать около 50 каналов. Экспериментальные данные позволяют сделать прогноз на достижение лучших параметров в будущем:

* достижение скорости передачи данных по квантовому каналу связи в 50 Мбит/с, при этом единовременные ошибки не должны будут превышать 4 %;
* создание квантового канала связи длиной более 100 км;
* организация десятков подканалов при разделении по длинам волн.

На данном этапе квантовая криптография только приближается к практическому уровню использования. Диапазон разработчиков новых технологий квантовой криптографии охватывает не только крупнейшие мировые институты, но и маленькие компании, только начинающие свою деятельность. И все они уже способны вывести свои проекты из лабораторий на рынок. Все это позволяет сказать, что рынок находится на начальной стадии формирования, когда в нём могут быть на равных представлены и те и другие.

## Квантовый криптоанализ

Квантовый криптоанализ обладает неоспоримыми преимуществами и экспоненциально перед обычным.

Безопасность схемы, предложенной RSA, гарантируется факторизацией больших целых чисел (на простых компьютерах невозможно решить задачу разложения очень большого числа на простые множители, ведь данная операция потребует астрономического времени и экспоненциально большого числа действий).

Другие теоретико-числовые методы криптографии могут быть основаны на проблеме [дискретного логарифмирования](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D0%B5_%D0%BB%D0%BE%D0%B3%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5).

Для решения этих двух проблем был разработан квантовый [алгоритм Шора](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%A8%D0%BE%D1%80%D0%B0) (1994), позволяющий найти за конечное и приемлемое время все простые множители больших чисел или решить задачу логарифмирования, и, как следствие, взломать шифры RSA и [ECC](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%BB%D0%B8%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F).

Создание достаточно крупной (мощной) квантовой криптоаналитической системы является плохой новостью для RSA и других асимметричных систем.

По состоянию на 2012 год наиболее продвинутые квантовые компьютеры смогли разложить на множители числа 15 (в 150 тыс. попыток верный ответ был получен в половине случаев, в соответствии с алгоритмом Шора) и 21.