Квантовая криптография

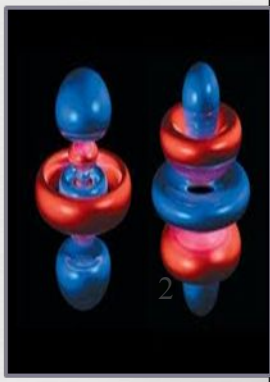
Введение

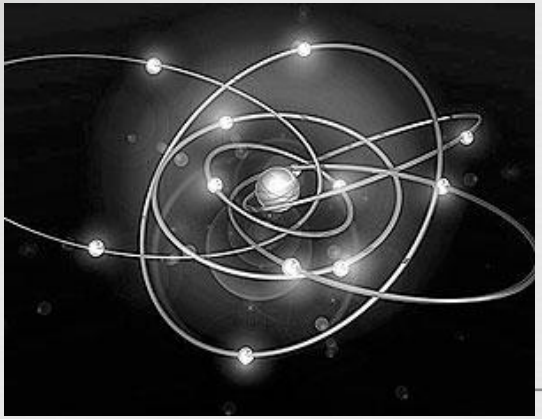
Квантовая криптография — метод защиты коммуникаций, основанный на принципах квантовой физики.

Технология квантовой криптографии опирается на принципиальную неопределённость поведения квантовой системы — невозможно одновременно получить координаты и импульс частицы, невозможно измерить один параметр фотона, не исказив другой.

Процесс отправки и приёма информации всегда выполняется физическими средствами, например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи.

Используя квантовые явления, можно спроектировать и создать такую систему связи, которая всегда может обнаруживать подслушивание.





История развития

- Впервые идея защиты информации с помощью квантовых объектов была предложена Стефаном Вейснером в 1970 году.
- В 1984 году Чарльз Беннет и Жиль Брассард на основе теории Вейснера создали алгоритм BB84
- 1989 г – первое устройство квантовой криптографии
- 1991 г – алгоритм Беннета, протокол E91, предложенный А. Экертом
- 17.06.2011 – взлом шифра квантового шифрования сингапурскими учеными-физиками

Развитие квантовой криптографии пошло по двум основным направлениям:

Первое направление основано на кодировании квантового состояния одиночной частицы и базируется на принципе невозможности различить абсолютно надёжно два неортогональных квантовых состояния.

Второе направление развития основано на эффекте квантового перепутывания (запутывания). Две квантово-механические системы (в том числе и разделённые пространственно) могут находиться в состоянии корреляции, так что измерение выбранной величины, осуществляемое над одной из систем, определит результат измерения этой величины на другой. Ни одна из запутанных систем не находится в определённом состоянии

Основным протоколом квантовой криптографии на одночастичных состояниях является протокол BB84

Базовым протоколом квантового распределения ключей на основе эффекта квантового запутывания является протокол EPR (Einstein-Podolsky-Rosen), второе его название E91

Алгоритм BB84 (1984г) – первый протокол квантового распределения ключа

Назад к истории

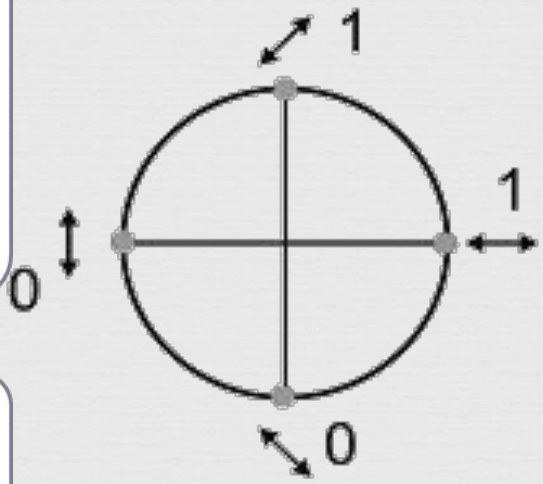
Носителями информации являются 2-х уровневые системы, называемые кубитами (квантовыми битами)

Протокол использует 4 квантовые состояния, образующие 2 базиса, например поляризационные состояния света.

Схема алгоритма состоит из двух этапов:

Первичная квантовая передача

Оценка попыток перехватить информацию



4 состояния лежат на экваторе сферы Пуанкаре

I этап

Назад к истории

Алиса посылает отдельные фотоны Бобу в произвольно выбранном базисе (имеющие любую из 4 видов поляризаций), используя при выборе генератор случайных чисел

|	/	-	\	-	-	/	|	|

Боб измеряет принимаемые фотоны в одном из двух базисов, также выбираемых произвольно: (+) - прямолинейная поляризация, x - диагональная

+	+	x	x	+	x	x	x	+

Боб записывает результаты измерения и сохраняет в тайне

|	-	/	\	-	/	/	/	|

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

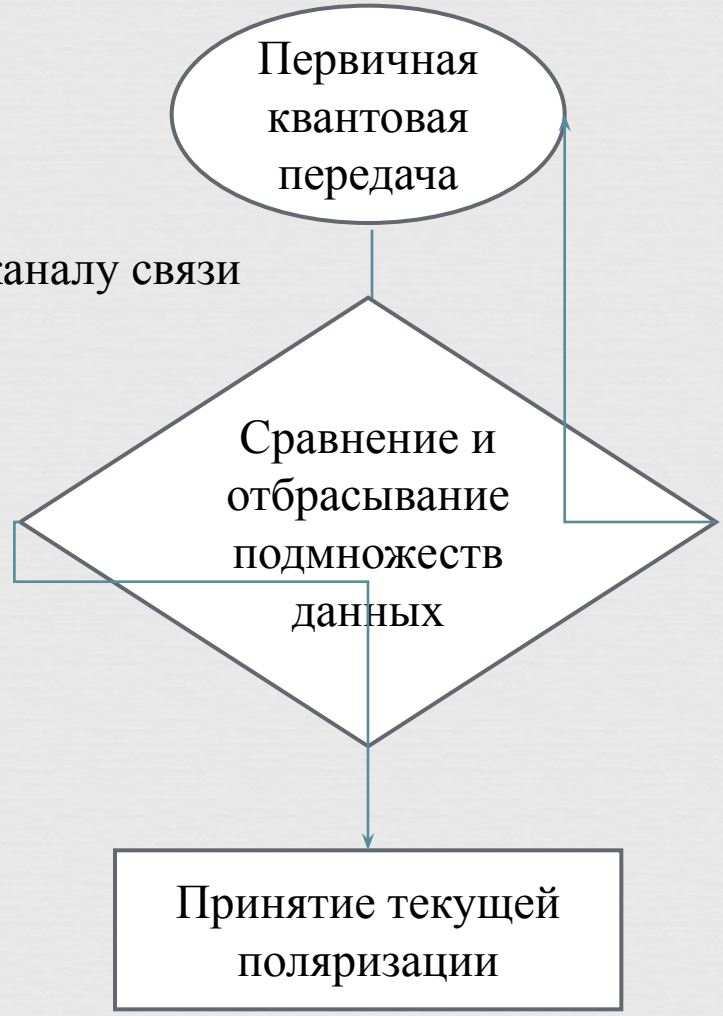
V			V	V		V		V

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.

|			\	-		/		|
1			1	0		0		1

II этап

Назад к истории



Если подслушивание имело место, то по величине ошибки можно оценить максимальное количество информации, доступное Еве.

Согласно принципу неопределённости Гейзенберга, криптоаналитик не может измерить как диагональную, так и прямоугольную поляризацию одного и того же фотона. С вероятностью $1 - 2^{-k}$ (где k — число сравненных битов) канал не прослушивался.

Если ошибка в канале меньше ≈11 %, то информация, доступная Еве, заведомо не превосходит взаимной информации между Алисой и Бобом, и секретная передача данных возможна.

Первое устройство квантовой криптографии

Назад к истории

Первая работающая квантово-криптографическая схема была построена в 1989 году в Исследовательском центре компании IBM Беннетом и Брассардом.

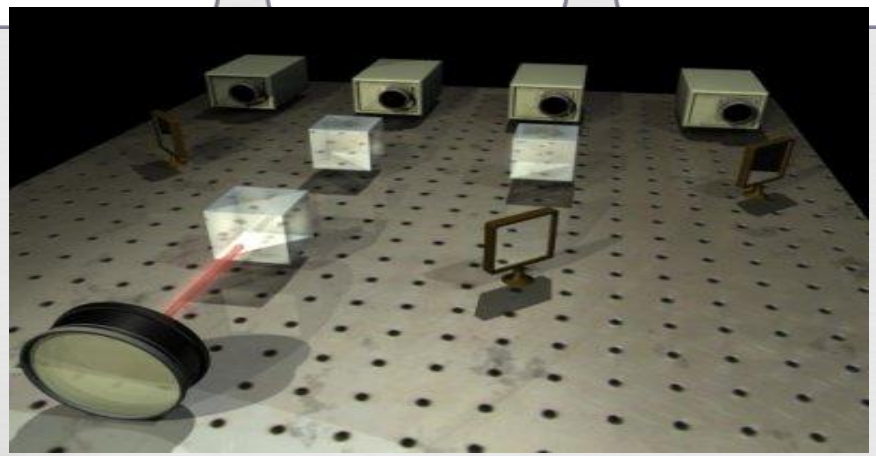
Схема представляла собой квантовый канал, на одном конце которого был передающий аппарат Алисы, на другом принимающий аппарат Боба. Оба аппарата размещены на оптической скамье длиной около 1 м, в светонепроницаемом кожухе размерами 1,5x0,5x0,5 м.

Управление происходило с помощью компьютера, в который были загружены программные представления легальных пользователей и злоумышленника

Сохранность тайны передаваемых данных напрямую зависит от интенсивности вспышек света, используемых для передачи.

Слабые вспышки, хоть и делают трудным перехват сообщений, все же приводят к росту числа ошибок у легального пользователя, при измерении правильной поляризации.

Повышение интенсивности вспышек значительно упрощает перехват путем расщепления начального одиночного фотона (или пучка света) на два: первого по-прежнему направленному легальному пользователю, а второго анализируемого злоумышленнику.



Назад к истории

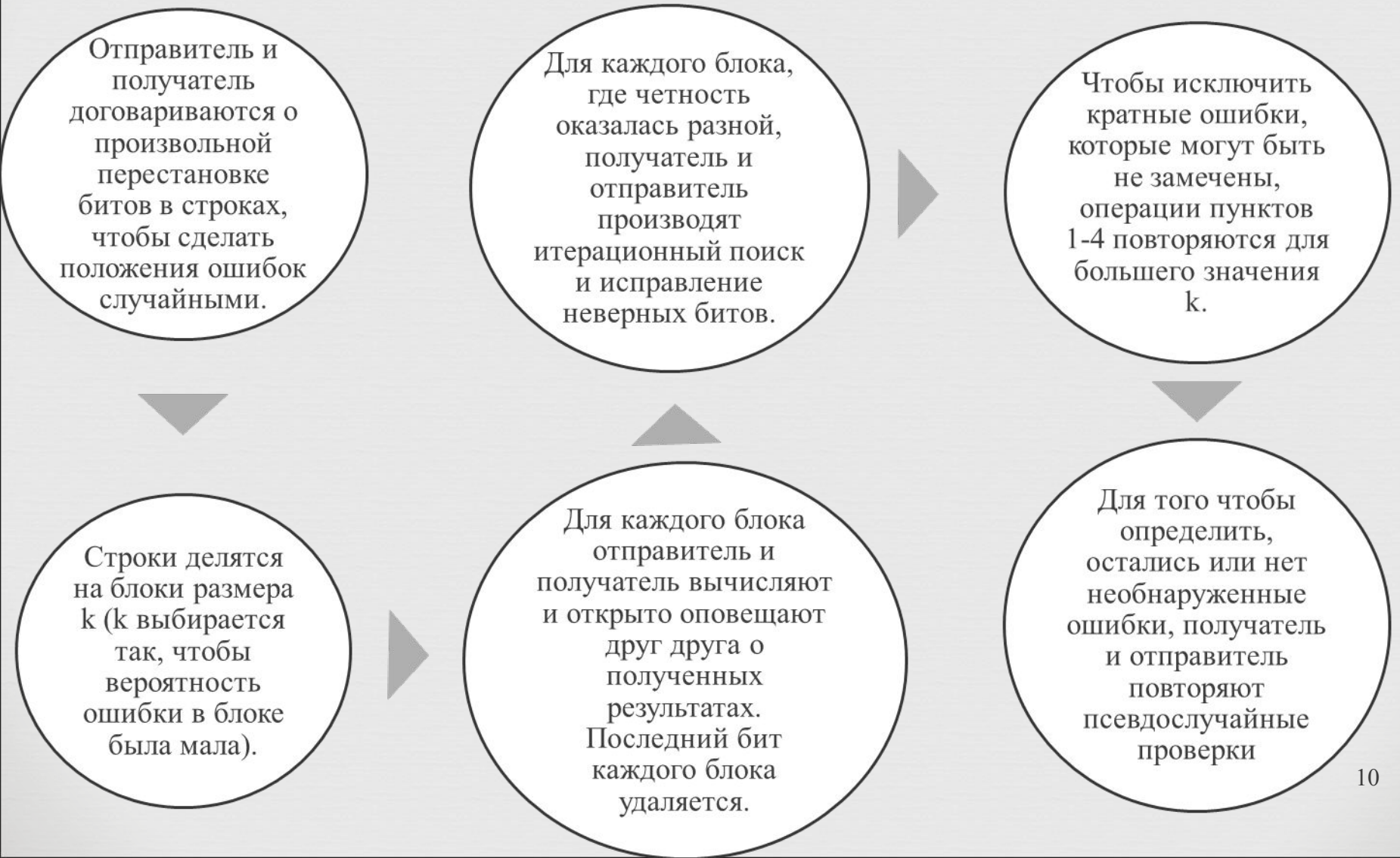
Легальные пользователи могут исправлять ошибки с помощью специальных кодов, обсуждая по открытому каналу результаты кодирования.

Но все-таки при этом часть информации попадает к криптоаналитику. Тем не менее, легальные пользователи Алиса и Боб, изучая количество выявленных и исправленных ошибок, а так же интенсивность вспышек света, могут дать оценку количеству информации, попавшей к злоумышленнику.

Алгоритм Беннета (1991)

Назад к истории

В 1991 году Ч. Беннетом был предложен следующий алгоритм для выявления искажений в переданных по квантовому каналу данных:



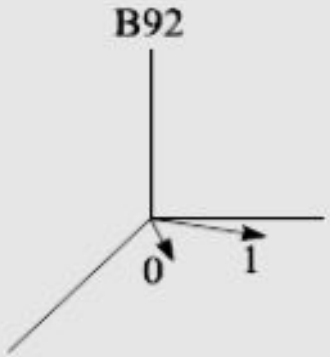
Назад к истории

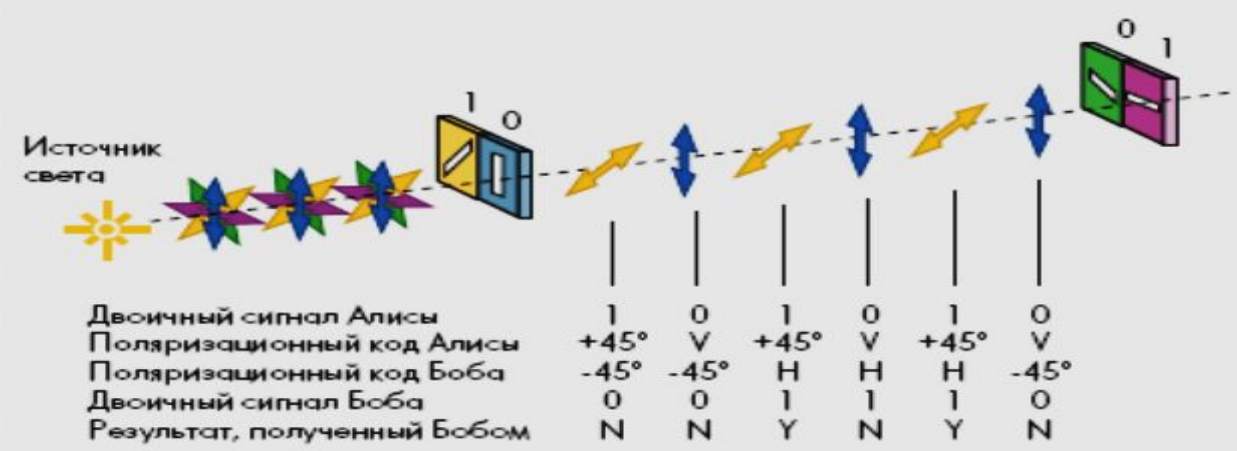
Псевдослучайная проверка:

- Получатель и отправитель открыто объявляют о случайном перемешивании позиций половины бит в их строках.
- Получатель и отправитель открыто сравнивают четности. Если строки отличаются, четности должны не совпадать с вероятностью 1/2.
- Если имеет место отличие, получатель и отправитель, использует двоичный поиск и удаление неверных битов.
- Если отличий нет, после m итераций получатель и отправитель получают идентичные строки с вероятностью ошибки 2^{-m}.

Алгоритм B92

- В протоколе используются фотоны, поляризованные в двух различных направлениях для представления нулей и единиц. Фотоны, поляризованные вдоль направления +45°, несут информацию о единичном бите, фотоны, поляризованные вдоль направления 0° (V) – о нулевом бите.
- Для определения поляризации станция Боб анализирует принимаемые фотоны, используя выбранный случайным образом один из двух неортогональных базисов «+» или «x»





Двоичный сигнал станции Алиса	1	0	1	0
Поляризационный код станции Алиса	⇗	⇕	⇗	⇕
Поляризационный код станции Боб	⇘	⇘	↔	↔
Двоичный сигнал станции Боб	0	0	1	1
Результат, полученный станцией Боб	-	-	+	-

Станция Алиса посылает фотоны, поляризованные в направлениях 0 и +45°, представляющие 0 и 1.

Станция Боб принимает фотоны через фильтры ориентированные под углом 90°и 135°(-45°).

Если фотон будет анализирован при помощи фильтра, ориентированного под углом 90°по отношению к передаваемому фотону, то фотон не пройдет через фильтр. Если же этот угол составит 45°, то фотон пройдет через фильтр с вероятностью 0,5.

Если станция Боб анализирует посланный фотон фильтром с ортогональным направлением поляризации, то он не может точно определить, какое значение данный фотон представляет

Если фотон был принят удачно (направления поляризации между посланным фотоном и фильтром неортогональны), то очередной бит ключа кодируется 0 либо 1