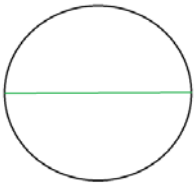
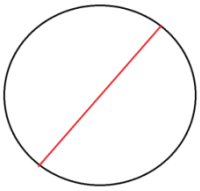
Квантовая криптография. Протокол BB84.
Разработан двумя учёными с фамилией на английскую B в 1984 году, откуда и такое название. Это исторически первый алгоритм квантовой криптографии, и одновременно самый простой для понимания.
Сначала предыстория. Есть алгоритм шифрования, который принципиально невозможно взломать.
Пусть отправитель Алиса написала сообщение в двоичном коде. У неё должен быть ключ – случайный набор нулей и единиц длиной сообщения. Она применяет ключ к исходному сообщению, применяя xor к каждому биту. То, что получилось, отправляет адресату Бобу.
Если у Боба есть тот же ключ, что и у Алисы, очевидно, он сможет расшифровать сообщение. Но как ему получить тот же ключ, что и Алисе? Если Алиса выложит его в открытый доступ, то тот, кто перехватит сообщение, с помощью выложенного в открытый доступ ключа спокойно прочитает сообщение и отправит его вновь Бобу.
Оказывается, что если использовать в качестве носителя информации не простую флешку, а поляризованные фотоны (разным значениям поляризации будет разная поляризация), то если Ева перехватит сообщение, то ей придётся, чтобы узнать поляризацию, провести некое измерение. А измерение квантовой системы приведёт к её изменению: микрообъекты – очень хрупкие создания. Если Алиса и Боб потом узнают, что что-то у них не сходится, они поймут, что их прослушивают.
Эта идея, теперь поподробней займёмся её реализацией. В расположении у Алисы исходное, ею написано сообщение, которое она хочет отправить, и генератор случайных чисел.
Также Алиса может приготовить фотон с произвольной линейной поляризацией. В зависимости от генератора случайных чисел она отсылает Бобу фотон со следующей поляризацией:

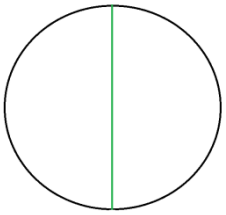
Алисе нужно закодировать 0, генератор выдал 0:

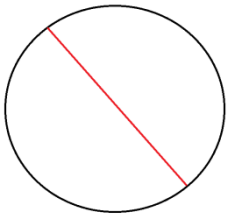


Алисе нужно закодировать 0, генератор выдал 1:

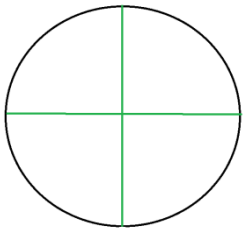


Алисе нужно закодировать 1, генератор выдал 0:

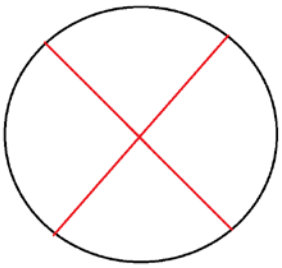




Алисе нужно закодировать 1, генератор выдал 1:
Боб же полученные фотоны считывает. Здесь надо уточнить, как происходит считывание фотонов.
Для считывания используется поляризатор. Его оси обозначают крестом:



- поляризатор «+».



- поляризатор «Х».
Разумеется, оси могут быть повернуты под любым углом, но в данном протоколе используются именно эти два поляризатора.
Если одна из двух осей поляризатора совпадает с осью поляризатора, то в 100% случаев поляризатор даёт верный результат.
Если на оператор «+» подать фотон с вертикальной поляризацией – мы сможем понять, что фотон был вертикально поляризован.
Если это было фотон с горизонтальной поляризацией – также сможем.
(Может возникнуть вопрос, как это сделать чисто физически. Например, фотоны с вертикальной поляризацией будут после поляризатора «+» отражаться, а фотоне с горизонтальной – проходить. Поставив в нужных места детекторы, мы сможем определять).
А вот если фотон под углом, есть рандом. Сработает один из двух детекторов, но какой именно – рандом, зависящий от угла поляризации. Если угол, как в этом протоколе, 45 градусов, то тут фифти-фифти. Таким образом, если мы применим «не тот» поляризатор к фотону, то результаты измерения нам ничего не дадут.
Например, если мы применим поляризатор «Х» к фотону и получим, что поляризация фотона равна «\», мы узнаем, что фотон мог быть «\», «-» и «|» , но точно не «/».
Если мы применяем не «тот» поляризатор к фотону, то поляризатор, помимо выдачи бесполезной информации, ещё работает в качестве проектора и меняет

поляризацию фотона: а именно, его ось отклоняется на 45 градусов, и становится такой же, какой результат нам выдал поляризатор. Это очень важный нюанс: в результате измерения фотон поменял свою ориентацию. Вот как один мой знакомый, который за два года на Физтехе тоже поменял свою ориентацию.

Так вот, у Боба есть два анализатора и также свой генератор случайных чисел. Для каждого фотона он применяет один из двух анализаторов, используя для выбора генератор случайных чисел.
Затем Боб, а потом Алиса публикуют в открытом доступе цепочку 0 и 1 генераторов случайных чисел. Для 50% фотонов Алиса и Боб получили разные значения (что соответствует тому, что Боб использовал «не тот» анализатор для чтения фотона Алисы), и полученная Бобом информация про этот фотон бесполезна. Но оставшиеся 50% сообщения Боб смог прочитать.

Теперь Ева перехватает сообщение Алисы до того, как его успел получить Боб. Она, как и Боб, не знает, какой анализатор использовала Алиса для каждого фотона, и также вынуждена тыкаться наугад своими двумя анализаторами.
И вот, она протыкала всё сообщение и получила набор поляризаций. Теперь она ждёт, пока Алиса выложит в открытый доступ цепочку исходного выбора поляризаторов для кодировки сообщения.
Сможет она прочитать сообщение Алисы после этого? Как и в прошлом случае с Бобом, она прочитает 50% сообщения. Но весь прикол в том, что 50% фотонов, где она не угадала и выбрала «не тот» анализатор для поляризованного Алисой фотона, поменяли свою поляризацию на 45 градусов.
И теперь предположим, что Боб как раз угадал и выбрал для одного из таких фотонов тот анализатор, который был нужен для исходного сообщения от Алисы. Если бы не Ева, то Алиса и Боб, сверив свои наборы 0 и 1, поняли, что они угадали и этот бит можно прочесть. А вот вклинилась Ева и повернула его на 45 градусов. Теперь Боб, хоть и выбрал тот анализатор, который нужен был для чтения фотона от Алисы, из-за Евы может дать с вероятностью 0,5 нужный результат, а может дать с вероятностью 0,5 неправильный ответ, который и будет спален Алисой и Бобом, которые поймут, что их прослушивают. Так что Бобу, получив от Алисы сообщение «превед чё дилаищ», следует подумать: или Алиса пишет на олбанском, или их прослушивают…