Алгоритм BB84

Теперь мы готовы к изучению алгоритма квантового распределения ключа. Для того, чтобы передать друг другу ключ, Алиса и Боб будут использовать оптические приборы. Алиса будет отправлять Бобу по одному фотону с определенной поляризацией. Всего у нее будет 4 вида поляризации: горизонтальная (0°), вертикальная (90°), и две диагональные (45° и -45°). Величина угла равна величине угла между направлением поляризации и горизонтальной осью. Направление поляризации Алиса устанавливает с помощью поляризатора. Алиса кодирует каждый фотон по определенному правилу:

$\uparrow$	$\rightarrow$	$\nearrow$	$\searrow$
1	0	1	0

Отправляя определенный фотон, Алиса записывает у себя соответствующий бит. Оборудование Боба включает в себя пластинку $\frac{\lambda}{2}$, поляризационный светоделитель (PBS) и два приемника сигнала (oscilloscope), один из которых будет обозначать 0, другой 1. Если сигнал на приемнике с 0, то Боб записывает 0, если сигнал на приемнике с 1, то Боб записывает 1. Пластинку $\frac{\lambda}{2}$ Боб может ставить в двух направлениях: вертикально и под углом $67{,}5^{\circ}$. Если на вертикальную пластинку налетает фотон с поляризацией 0° или 90°, то поляризация не меняется. Если налетает фотон с диагональной поляризацией, то поляризация остается диагональной. Если пластинка расположена под углом $67{,}5^{\circ}$, то вертикальная и горизонтальная поляризация меняется на диагональную, а диагональная на вертикальную или горизонтальную. Расположены они следующим образом:

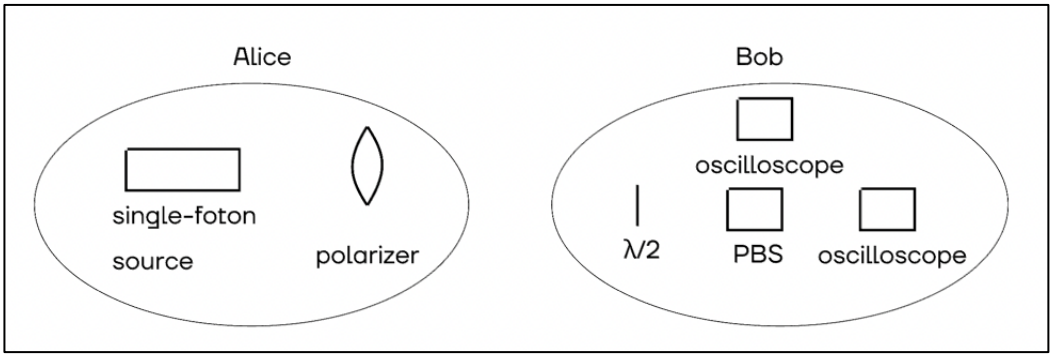

Схема из отправителя и получателя (рис. 3)

Вертикальным базисом будем называть совокупность вертикальной и горизонтальной поляризации. Диагональным базисом будем называть совокупность диагональных поляризаций. Если на бимсплиттер попадает фотон с диагонального поляризацией, то он либо отразится, либо пройдет дальше с одинаковой вероятностью $\frac{1}{2}$.

Разберем все варианты исходов при отправке одного фотона:

1) Если Алиса отправляет фотон из вертикального базиса, а пластинка $\frac{\lambda}{2}$ у Боба находится вертикально, то направление фотона после поляризационного светоделителя однозначно и Боб так же записывает биты, как и Алиса. Они у него совпадают.

2) Если Алиса отправляет фотон из диагонального базиса, а пластинка $\frac{\lambda}{2}$ у Боба находится под углом $67{,}5^{\circ}$ к горизонту, то направление фотона после поляризационного светоделителя однозначно и Боб так же записывает биты, как и Алиса. Они у него совпадают.

3) Если Алиса отправляет фотон из вертикального базиса, а пластинка $\frac{\lambda}{2}$ у Боба находится под углом $67{,}5^{\circ}$ к горизонту, то направление фотона после поляризационного светоделителя случайно.

И в обратном случае: если Алиса отправляет фотон из диагонального базиса, а пластинка $\lambda/2$ у Боба находится вертикально, то направление фотона после пластинки случайно. Следовательно, с равной вероятность $\frac{1}{2}$ даст сигнал один из приемников.

После передачи последовательности бит Алиса и Боб созваниваются по открытому каналу и рассказывают друг другу следующую информацию: какой базис использовала Алиса и как ставил пластинку Боб. Если их базисы в данном бите совпали, то такой бит они оставляют. Если базисы не совпали, то они удаляют бит.

В данном эксперименте часть бит теряется, но его можно продолжать до тех пор, пока не накопится нужная длина ключа. Ниже будет пример того, как происходит передача ключа.

Пример генерации ключа (таб. 1)

Базис Алисы	+	×	+	+	×	×	+	×	+
Поляризация	↑	↗	→	↑	↗	↘	→	↘	↑
Бит Алисы	1	1	0	1	1	0	0	0	1
Базис Боба	+	+	×	+	×	+	×	×	+
Результат	↑	↑ или →	↗ или ↘	↑	↗	↑ или →	↗ или ↘	↘	↑
Бит Боба	1	1 или 0	1 или 0	1	1	1 или 0	1 или 0	0	1
Итоговый ключ	1	-	-	1	1	-	-	0	1

Перехватчик

Теперь в нашей цепи присутствует перехватчик Ева. Ева может перехватывать фотоны и не отправлять дальше, но тогда Боб заметит ее

присутствие. Она пытается перехватить ключ, чтобы Боб и Алиса этого не заметили. Поэтому ее устройство дублирует Боба. Ева старается определить поляризацию и передает такой же фотон Бобу.

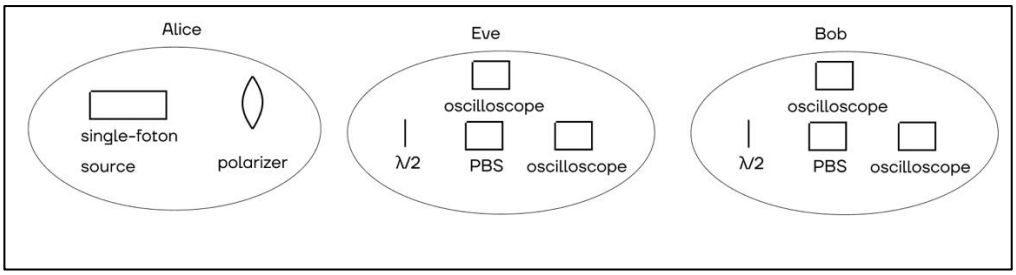

Схема с перехватчиком (рис. 4)

Разберем все возможные исходы:

1) Если у Алисы и Боба не совпали базисы, то не важно, что померила Ева, так как они не будут использовать этот бит.

2) Если у Алисы, Боба и Евы совпали базисы, то они никак не заметят прослушивание.

3) Если у Алисы и Боба базисы совпали, а у Евы нет, то Ева не сможет точно определить направление поляризации фотона, и на этом этапе Алиса и Боб могут заметить перехват, так как потом, созваниваясь по открытому каналу, они могут раскрыть часть битов, и если они не совпадут, то их прослушивала Ева.