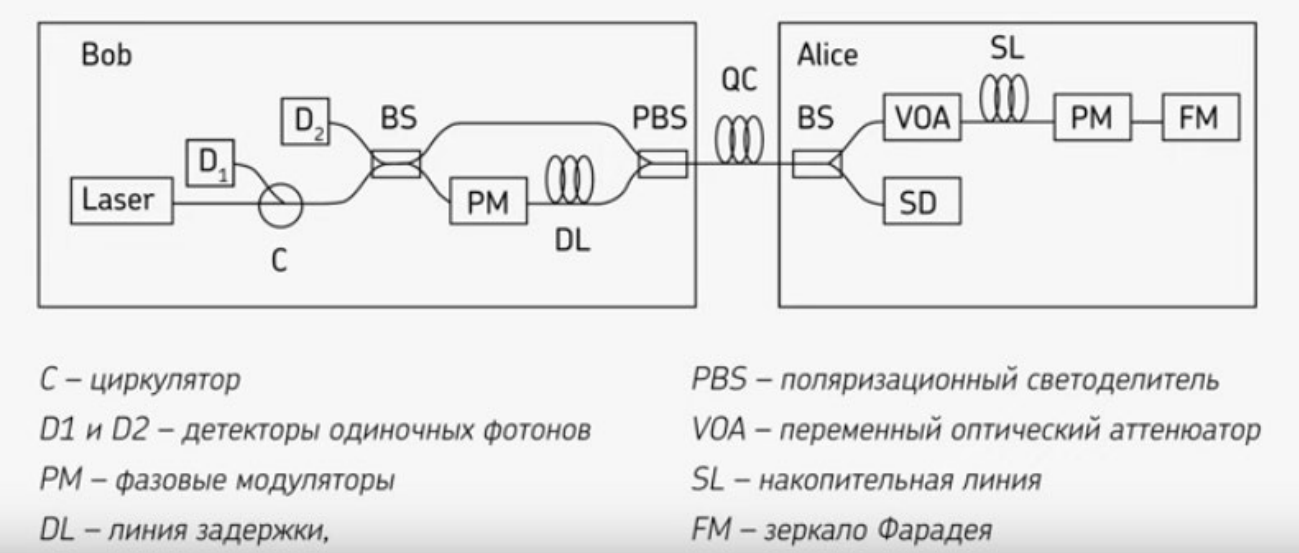
СХЕМА PLUG&PLAY

ВАДИМ РОДИМИН

СТАРШИЙ НАУЧНЫЙ СОТРУДНИК ГРУППЫ КВАНТОВЫХ КОММУНИКАЦИЙ РОССИЙСКОГО КВАНТОВОГО ЦЕНТРА

Хочется отметить, что протоколов квантового распределения ключа существует очень много. И для того, чтобы протокол работал, нужно собрать некую оптическую схему, где мы будем готовить квантовые состояния фотонов, передавать их и считывать.

Вариантов оптических схем тоже предостаточно, но я хочу остановиться на одной, не самой простой для понимания, но одной из наиболее простых для реализации. Она называется Plug&Play, или двухпроходная автокомпенсационная схема:



Алиса будет готовить квантовые состояния, но лазер находится в Бобе, который отсылает импульсы Алисе. Они приходят к ней, Алиса накладывает на них информацию и отсылает обратно.

Лазерные импульсы Боба сначала попадают на циркулятор (C), который «разруливает» проход импульсов, не требуя никакого питания. Дальше лазерный импульс попадает на светоделитель (PBS) и расходится по 2-ум плечам интерферометра. На втором плече находятся фазовый модулятор (PM) и линия задержки (DL). Часть света проходит по верхнему плечу интерферометра, а часть по нижнему. Из-за того, что интерферометр неравноплечий, один импульс обгоняет другой, и выходит уже пара импульсов, причем один помощнее, а другой послабее. Дальше эта пара импульсов отправляется к Алисе по квантовому каналу. Синхродетектор срабатывает и «говорит» Алисе, что к ней пришел импульс. Меньшая часть света отправляется в верхнее плечо после светоделителя, и в итоге она проходит в переменный оптический аттенюатор (VOA). Импульс дважды ослабляется, проходя через

него. Когда импульс проходит обратно, то он становится слабым однофотонным, а нам такие импульсы как раз нужны. Если импульсы будут мощные двухфотонные, то злоумышленник может расщепить их — один фотон отправить Бобу, а один оставить себе.

Дальше импульсы проходят через фазовый модулятор у Алисы, и Алиса может накладывать на один из импульсов фазу. Импульсы отражаются от зеркала Фарадея (FM) и идут обратно. Они приходят обратно, и тут получается вот что: на поляризационном светоделителе Боба эти импульсы расходятся по-другому. Тот импульс, который к Алисе шел по верхнему плечу, идет по нижнему плечу, и наоборот. Все импульсы были поляризованы. На поляризационный светоделитель Боба они зашли под перпендикулярным углом, поэтому они — ортогонально поляризованные. И к Алисе они пришли точно такими же.

Но поляризация в данном случае никакой информации не несет. Для чего тогда она нам нужна? Когда импульсы отражаются от зеркала Фарадея, то они меняют свою поляризацию на ортогональную. Потом они идут обратно и автоматически расходятся по разным путям. Таким образом, тот импульс, который сначала обогнал — теперь отстанет, и на конечном светоделителе Боба (BS) они сойдутся вместе и проинтерферируют. Но перед этим на один из них Боб наложит некоторый сдвиг по фазе. Фазовым модулятором он как раз и будет выбирать базис измерения. Если Боб приложит нулевое напряжение, то это будет один какой-то базис, допустим, прямой и т. д. После выбора базиса у нас есть два детектора, которые «кликают».

Эта схема и есть схема для реализации квантового распределения ключа с использованием протокола BB84.