Квантовые вычисления

Практическое занятие № 2. Квантовая криптография

Имеются два пользователя A и B, соединенные двумя открытыми каналами связи, из которых один – квантовый (по нему передаются кубиты), второй – классический (по нему передаются обычные сообщения). Опишем протокол, который позволяет пользователям сформировать *один* общий секретный бит информации, значение которого не может быть получено или как-то вычислено противником, имеющим доступ к используемым каналам связи. Данный протокол можно повторить необходимое число раз для получения требуемого количества секретных бит, которые могут быть использованы в качестве ключа в шифре Вернама (если ключ строится из полностью случайных бит, его длина равна длине сообщения, и он используется только один раз, то шифр Вернама получается совершенным, т.е. его невозможно взломать).

1. Пользователь A генерирует кубит, находящийся с равными вероятностями в одном из четырех состояний: $|0\rangle$, $|1\rangle$, $|0\rangle' = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ или $|1\rangle' = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, и отправляет его пользователю B по квантовому каналу связи.
2. Пользователь B с равными вероятностями выбирает один из двух измерителей: в базисе $|0\rangle$, $|1\rangle$ или в базисе $|0\rangle'$, $|1\rangle'$, и измеряет полученный кубит. Заметим, что если кубит совпадает с осью измерителя, то получается детерминированный результат (0 или 1). В противном случае результат измерения случаен.
3. Пользователь B сообщает A по классическому каналу, какой измеритель он использовал.
4. Пользователь A смотрит, соответствует ли этот измеритель тому кубиту, который он сгенерировал на первом шаге. Если да, то он говорит пользователю B «ОК». На этом протокол завершается. В противном случае он говорит «ПОВТОР» и протокол повторяется.

По завершении протокола общий секретный бит принимает значение 0, если на первом шаге генерировался $|0\rangle$ или $|0\rangle'$, и значение 1, если на первом шаге генерировался $|1\rangle$ или $|1\rangle'$.

Задание. Смоделировать квантовый протокол построения секретного ключа, визуально показав все его промежуточные этапы.