Квантовый протокол обмена секретным ключом BB92

Алиса и Боб оставляют только те биты, для которых результаты Боба равны Y, именно эти биты соответствуют совпадению алфавитов. В приведенном примере только третий бит передает одинаковые буквы алфавита.

$$\begin{pmatrix} & 1 & 0 & 1 & 0 \\ & |\nearrow> & |\uparrow> & |\nearrow> & |\uparrow> \\ & 0 & 0 & 1 & 1 \\ & |\nwarrow> & |\nwarrow> & |\rightarrow> & |\rightarrow> \\ & N & N & Y & N \end{pmatrix}$$

Первый и четвертый биты Алисы и Боба имеют различные значения, так что в каждом из этих случаях результат Боба равен N. Во втором и третьем случаях значения битов совпадают, и с вероятностью 0.5 результат Боба будет равен Y. Конечно, нельзя предсказать заранее результат каждого измерения.

Чтобы закончить протокол Боб посылает свои результаты Y или N Алисе, не сообщая значений поляризации своих анализаторов. Это сообщение посылается по открытому каналу.

Таким образом, эффективность идеальной процедуры обмена, η_Q, равна 0.25.

Внедрение Евы приведет к ошибке в 25%, если она будет, например, измерять поляризации в базисе Алисы.