Семинар по КВАНТОВОЙ КРИПТОГРАФИИ (I)

1 Три симметричных поляризационных базиса

Фотон распространяется в горизонтальном направлении. Выберем три поляризационных базиса

$$\langle\tilde{0}|\tilde{0}\rangle = \langle\tilde{1}|\tilde{1}\rangle = 1; \qquad \langle\tilde{0}|\tilde{1}\rangle = 0$$

с вертикальной и горизонтальной поляризациями:

$$|0\rangle = |\updownarrow\rangle = \binom{1}{0} \qquad |1\rangle = |\leftrightarrow\rangle = \binom{0}{1};$$

с поляризациями под углом 45° и −45° :

$$|0'\rangle = |\nearrow\rangle = \frac{1}{\sqrt{2}}\binom{1}{1} \qquad |1'\rangle = |\searrow\rangle = \frac{1}{\sqrt{2}}\binom{1}{-1};$$

с право- и лево- круговыми поляризациями:

$$|0''\rangle = |\nearrow\rangle = \frac{1}{\sqrt{2}}\binom{1}{i} \qquad |1''\rangle = |\searrow\rangle = \frac{1}{\sqrt{2}}\binom{1}{-i}.$$

Покажите, что если фотон находится в одном из базисных поляризационных состояний любого из этих базисов, то вероятность обнаружить фотон в состоянии любого из двух других базисов равна 1/2.

Заметим, что эти базисные состояния кубита, когда кубит - это спин $1/2$, *соответствуют состояниям спина с проекциями* $+\frac{1}{2}$ *и* $-\frac{1}{2}$ *на три ортогональных направления– оси* z, x *и* y.

2 Протокол с 6 состояниями

Подобно тому как в BB84 используется две пары ортогональных состояний. В этом протоколе используют три таких пара. Эффективноть передачи при этом составит только 33%, но зато повышается надежность против внедрения посторонных слушателей. Это достигается благодаря гораздо большей симметрии в пространстве состояний кубитов.

Постройте квантовый криптографический протокол с 6 состояниями. Определите ошибку, возникающую с появлением Евы в квантовом канале, если она производит измерение каждого фотона.

Ответ: возникающая ошибка 33%, *по сравнению с* 25% *в* BB84 *протоколе.*

3 Квантовое состояние пар $|\Psi-\rangle$ EPR -протокола

Идея этой вариация BB84 протокола состоит в замене квантового канала, по которому передаются кубиты от Алисы к Бобу, каналом, в котором от одного EPR-источника к Алисе и Бобу направляются фотоны из пары $|\Psi-\rangle$. Алиса и Боб, как в BB84, независимо и случайно используют два базиса, а затем согласуют свои результаты.

Запишем поляризационное состояние пары фотонов в состониии с полной нулевой полярицзацией (это максимально перепутанное состояние Бэлла $|\Psi-\rangle$ двух кубитов) в базисе с вертикальной и горизонтальной поляризациями:

$$|\Psi-\rangle_{12} = \frac{1}{\sqrt{2}}(|0>_1|1>_2 - |1>_1|0>_2) = \frac{1}{\sqrt{2}}\left(\binom{1}{0}_1\binom{0}{1}_2 - \binom{0}{1}_1\binom{1}{0}_2\right).$$

Произвольный поляризационный базис фотона можно записать в виде:

$$|\tilde{0}\rangle = \binom{\cos\theta}{\sin\theta e^{i\alpha}}, \qquad |\tilde{1}\rangle = \binom{-\sin\theta e^{-i\alpha}}{\cos\theta}.$$

Покажите, что состояние $|\Psi-\rangle_{12}$ во всех базисах имеет то же самое выражение:

$$|\Psi-\rangle_{12} = \frac{1}{\sqrt{2}}(|\tilde{0}>_1|\tilde{1}>_2 - |\tilde{1}>_1|\tilde{0}>_2).$$

Конечно, с точностью до фазы.

Литература:

1. N.Gisin, G.Ribordy, W.Tittel, H.Zbinden. Quantum Cryptography arXiv:quant-ph/0101098 **(2001)**.
2. S.J.Lomonaco. A Talk on Quantum Cryptography or How Alice Outwits Eve. arXiv:quant-ph/0102016 **(2001)**.