Exercises. October 12, 2007. Quantum information theory and computation

Exercise 1. BB84 protocol

In this exercise you are asked to apply all the steps of BB84 for a concrete example. Alice generates the classical strings $x = (01011000)$and $e = (10101011)$ Bob decodes using the Z or X basis according to a randomly generated string $d = (11011111)$ Suppose that Eve makes measurements of the type Z,X,Z,X,X,Z,Z,Z and sends her result to Bob. Describe a possible public discussion between Alice and Bob.

Exercise 3. B92 protocol

Analyze the security check for the B92 protocol under a (bit by bit) measurement attack of Eve.

Exercise 2. Bell states

It is important to be well acquainted with the strange properties of the four Bell states $|B_{xy}\rangle$ where $x, y = 00; 01; 10; 11$. They are usually written in the canonical basis of $\mathbf{C}^2 \otimes \mathbf{C}^2$.

a) Write down the states in the tensor product basis of linearly polarized states $|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ and $|\theta_\perp\rangle = \sin\theta|0\rangle - \cos\theta|1\rangle$.

b) Same question for the tensor product basis constructed out of circularly polarized states $|\tilde{\theta}\rangle = \cos\theta|0\rangle + i\sin\theta|1\rangle$ and $|\tilde{\theta}_\perp\rangle = \sin\theta|0\rangle + i\cos\theta|1\rangle$.

c) Show that no tensor product state can well-approximate a Bell state in the following sense (here $||\phi|| = ||\psi|| = 1$),

$$\min_{\phi,\psi} ||\phi \otimes \psi - B_{xy}||^2 = 2 - \sqrt{2} \tag{1}$$

c) Consider a perfect copy machine U_Z for the two states of the Z basis and another perfect copy machine U_X for the two states of the X basis. What are the state produced by U_Z when the X basis states are copied and what the states produced by U_X when the Z basis states are copied ?