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 $x = (0101100011101010)$and $e = (1010101110010101)$ The string x is encoded into a string of Qbits using the Z basis $\{|0\rangle, |1\rangle\}$ if $e_i = 0$ and the X basis $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ if $e_i = 1$. Bob decodes using the Z or X basis according to a randomly generated string $d = (1010100110101010)$ For the moment nothing is revealed publicly.

a) Write down the string of Qbits transmitted over the channel.

b) Suppose you are Bob and write down your measurement results.

c) Supposing that Eve does not interfere give the key that you generate by publicly discussing with Alice.

d) Suppose that Eve makes measurements of the type Z,X,Z,X,X,Z,Z,Z, X,Z,X,Z,Z,X,Z,X and sends her result to Bob. Describe the public discussion between Alice and Bob.

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) 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 ?