Homework Oct 17, 2013. Quantum information theory and computation

Problem 1. B92 protocol

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

Remark : you find this protocol explained in the notes of the course. There are two main differences with BB84. Two encoding states are used, whereas in BB84 four are used. Also, in B92 it is the random choice of basis that constitutes the key and Bob's detection that is publicly discussed. This second feature can be used to modify the BB84 key generation process: this is then called the SARG protocol (from the initials of the authors). The systems implemented by IdQuantique can be used in both ways, BB84 or SARG.

Problem 2. Production of Bell entangled states

a) Show that the four Bell states of two Qbits form an orthonormal basis of the two Qbit Hilbert space.

b) Take one of them and prove it is entangled.

c) Show that the circuit of figure 2 (or "unitary machine") produces Bell states from tensor product inputs $|x\rangle \otimes |y\rangle$.

d) Give a matrix 4×4 coordinate representation of the unitary matrix corresponding to this circuit in the basis $\{|0,0\rangle, |0,1\rangle, |1,0\rangle, |1,1\rangle\}$. You have to choose a coordinate representation of the basis vectors: choose the "canonical" one.

Problem 3. Fun and useful properties of Bell states

The four Bell states $|B_{xy}\rangle$ where $x, y = 00; 01; 10; 11$ 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) (Optional) 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 $|\tilde{\theta}_\perp\rangle = \sin\theta|0\rangle +$

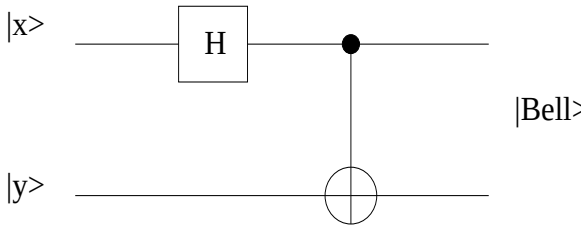

Figure 1: Machine for producing Bell states

$i \cos\theta|1\rangle$.

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

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

d) (Optional) 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 ?

Problem 4. Entanglement swapping

Suppose satellite S_1 distributes an entangled Bell pair between (distant) locations A and O on earth, and that satellite S_2 distributes another entangled pair between (distant) locations O and B. The polarization state of the four particles (photons) is

$$\frac{1}{\sqrt{2}}(|00\rangle_{AO} + |11\rangle_{AO}) \otimes \frac{1}{\sqrt{2}}(|00\rangle_{OB} + |11\rangle_{OB})$$

Note that there are two photons located at O. A physicist who sits at location O decides to make *a local measurement in the Bell basis at location O*.

a) List the relevant projectors of the measurement basis. *Hint*: your projectors should be 16 dimensional matrices (you are not asked to write the coordinate representation: use Dirac's notation !).

b) Give the four possible outcoming states of this measurement.

Remark : such ideas might be implemented for enhancing the distance of quantum communication protocols.