量子信息导论第二章作业

1：Alice 和 Bob 选择 B92 方案来建立量子密钥序列。Alice 选择两种态：$|\psi_1\rangle=|0\rangle$，$|\psi_2\rangle=1/\sqrt{2}(|0\rangle+|1\rangle)$，分别以 1/2 的概率发送给 Bob，Bob 分别以 1/2 的几率选择基$\{|0\rangle,|1\rangle\}$和基$\{1/\sqrt{2}(|0\rangle+|1\rangle),1/\sqrt{2}(|0\rangle-|1\rangle)\}$对收到的态进行正交测量。

(1) 请论述 Alice 和 Bob 将遵从怎样的经典通信协议来建立密钥；

(2)假定存在一个窃听者，该窃听者试图以概率克隆的方式对该密钥建立过程进行攻击。则下列的几组克隆概率中，哪几组在理论上是可能的（括号中第一个数表示成功地克隆出$|\psi_1\rangle$的概率，第二个数表示成功地克隆出$|\psi_2\rangle$的概率）。并给出证明。

$\left(\frac{2-\sqrt{2}}{2},\frac{2-\sqrt{2}}{2}\right)$，（1，0.1），(0.5，0.5)，（0.7，0.7），（0.9，0.9）。

（3）窃听者如果克隆失败，他会随机发送$|\psi_1\rangle$或$|\psi_2\rangle$给 Bob（分别以 1/2 的几率）。如窃听者选择以上几组中最优的克隆方案进行攻击，则作为 Alice 和 Bob，他们至少要公开对照多少组数据，均检验无误，才能确保该密钥的安全性达到 99%以上？

2：给出高维空间量子 teleportation 的数学证明。

3：混合纠缠态 $\rho(\lambda)=(1-\lambda)|\psi^-\rangle\langle\psi^-|+\frac{\lambda}{4}I\otimes I$

a) 求标准 teleportation 的保真度，并且，当λ达到多少时，保真度将优于经典极限？（所谓经典极限是指：A 方随机选择一组测量基进行测量，并将测量结果通过经典信道通知 B，B 根据 A 的测量结果进行态制备。）

b) 计算 $\Pr ob(\uparrow(\vec{n})\uparrow(\vec{m}))=Tr\left(E_A(\vec{n})E_A(\vec{m})\rho(\lambda)\right)$

$E(\vec{n})$是 Alice 的比特投影到$|\uparrow(\vec{n})\rangle$上的投影子。