作业一

1. （1）将|α⟩，|β⟩，|γ⟩三个矢量归一化，证明归一化后的矢量是三维希尔伯特空间的一组正交基。（2）该组基定义了一组投影测量，求量子态|ϕ⟩被其测量后，得到全部测量结果及其对应的概率。

$$|\alpha\rangle=\begin{bmatrix} i\sqrt{2} \\ 0 \\ \sqrt{3} \end{bmatrix} \quad |\beta\rangle=\begin{bmatrix} \sqrt{3} \\ 0 \\ i\sqrt{2} \end{bmatrix} \quad |\gamma\rangle=\begin{bmatrix} 0 \\ 3 \\ 0 \end{bmatrix} \quad |\phi\rangle=\begin{bmatrix} \frac{i}{2} \\ \frac{1}{2} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

2. 光子的偏振态如下|Ψ >所示，我们选取三组投影测量对其进行测量，分别是正负45度方向测量，左旋右旋测量和水平垂直方向测量；这些测量力学量对应矩阵如下。求每组测量后，态矢|Ψ >会被投影至的全部状态及其对应的几率。

$$|\Psi\rangle=\begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} \end{bmatrix} \quad \sigma_X=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \sigma_Y=\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \sigma_Z=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

作业一

3. （1）写出一组光子A和光子B的偏振状态组成的复合系统的基失。（2）请问下面四个态矢，是否互相正交？是不是该复合系统的一组基失？如果是，请问态矢$|0>_A|0>_B$被该组基失定义的投影测量所测量，得到各个结果的概率。

$$\begin{cases} \left|\varphi^{\pm}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B\right) \\ \left|\psi^{\pm}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B\right) \end{cases}$$

4. （1）一光子偏振态密度矩阵为$\rho = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$,则其被投影到正45度偏振态$|+\rangle$和负45度偏振态$|-\rangle$的概率分别为？（2）若光子的偏振态为纯态$|\psi\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$，写出其密度矩阵，它被投影到正45度偏振态$|+\rangle$和负45度偏振态$|-\rangle$的概率分别为？（3）写出一个纯态形式，其子系统的约化密度矩阵为ρ。

作业二

1. 六态协议如下：

➢Alice随机选取Pauli矩阵σ_X，σ_Y，σ_Z的本征态作为编码态承载密钥信息。当选中σ_Z基时，取其本征态$|0>$代表比特0，本征态$|1>$代表比特1；当选中σ_X基时，取其本征态$|+>$代表比特0，本征态$|->$代表比特1；当选中σ_Y基时，取其本征态$|+i>=(|0>+i|1>)/\sqrt{2}$代表比特0，本征态$|-i>=(|0>-i|1>)/\sqrt{2}$代表比特1；

➢Bob对收到的每个量子态依次随机采用σ_X，σ_Y，σ_Z测量，对于测量结果采用与Alice同样的规则记录密钥。

➢Bob和Alice互相通知对方所选取的基；双方保留基一致的密钥进行后处理。

在六态协议中，如果窃听者采用与如下截取重发攻击，将会导致Alice和Bob的密钥误码率为?

窃听者的截取重发攻击如下：窃听者对量子信道中每一个量子态随机执行σ_X，σ_Y，σ_Z基测量。测量结果为什么量子态就发送什么量子给Bob。

作业二

2. B92协议如下：

➢Alice制备N比特随机数作为自己的原始密钥，当随机数为0时，制备态$|0>$；随机数为1时，制备态$|+>$；后将N个量子态通过量子信道发送给Bob。

➢Bob对收到每个量子态依次随机采用σ_Z基测量或σ_X基测量。若他用σ_Z基测量，结果为态$|1>$时，他推断Alice制备的态为$|+>$，并记录密钥为1；当他用σ_X基测量，结果为态$|->$时，则推断Alice制备的态为$|0>$，并记录密钥为0；其他情况一律抛弃处理。

➢Bob通知Alice哪些密钥抛弃处理；双方对保留下的密钥进行后处理。

在B92协议中，如果窃听者采用与如下截取重发攻击，将会导致Alice和Bob的密钥误码率为?

窃听者的截取重发攻击如下：窃听者对量子信道中每一个量子态随机执行X基或Z基测量。测量结果是什么量子态就发送什么量子给Bob。

作业二

3. BB84，B92等量子密码协议能够在信道上安全的分发密钥。进而利用这些安全的密钥，执行一次一密算法才能实现需要的保密安全通信。那么是否可以绕过密钥分发和执行加密算法这两步，利用量子密码协议进行直接保密的安全通信，即直接利用量子态传送需要保密的明文消息？