量子信息导论 PHYS5251P 2021-2022 学年第一学期

第四次作业

截止日期：2021. 11. 24（周三）

姓名：陈 稼 霖
学号：SA21038052
成绩：__________

第 1 题 得分: _________. Alice 和 Bob 选择 B92 方案来建立量子秘钥序列. Alice 选择两种态: $|\psi_1\rangle = |0\rangle$, $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, 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秘钥;

(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秘钥建立过程进行攻击. 则以下的几组克隆概率中, 哪几组在理论上是可行的 (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.

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

(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 的概率). 如果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, 才能确保该秘钥的安全性达到 99% 以上?

解: (1) Bob 保留测得为 $|1\rangle$ 或 $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ 的结果, 而抛弃其他结果, 并将保留的结果在序列中的位置告诉 Alice, 从而建立秘钥. 具体来说, 分为以下 6 种情况:

Alice 发送的量子态	$\lvert\psi_1\rangle = \lvert 0\rangle$			$\lvert\psi_2\rangle = \frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle)$		
Bob 选择的测量基	$\{\lvert 0\rangle, \lvert 1\rangle\}$	$\{\frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle), \frac{1}{\sqrt{2}}(\lvert 0\rangle - \lvert 1\rangle)\}$		$\{\lvert 0\rangle, \lvert 1\rangle\}$		$\{\frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle), \frac{1}{\sqrt{2}}(\lvert 0\rangle - \lvert 1\rangle)\}$
Bob 的测量结果	$\lvert 0\rangle$	$\frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle)$	$\frac{1}{2}(\lvert 0\rangle - \lvert 1\rangle)$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\frac{1}{\sqrt{2}}(\lvert 0\rangle - \lvert 1\rangle)$
是否保留	否	否	是	否	是	否
生成的秘钥			0		1	

建立秘钥后, Alice 和 Bob 选择部分秘钥进行比较, 以检查是否有窃听.

(2) 定义

$$X^{(1)} = \begin{pmatrix} \langle\psi_1|\psi_1\rangle & \langle\psi_1|\psi_2\rangle \\ \langle\psi_2|\psi_1\rangle & \langle\psi_2|\psi_2\rangle \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 1 \end{pmatrix}, \tag{1}$$

$$X^{(2)} = \begin{pmatrix} (\langle\psi_1|\psi_1\rangle)^2 & (\langle\psi_1|\psi_2\rangle)^2 \\ (\langle\psi_2|\psi_1\rangle)^2 & (\langle\psi_2|\psi_2\rangle)^2 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}. \tag{2}$$

对克隆概率 (r_1, r_2),

$$\Gamma = \begin{pmatrix} r_1 & 0 \\ 0 & r_2 \end{pmatrix}, \tag{3}$$

$$X^{(1)} - \sqrt{\Gamma} X^{(2)} \sqrt{\Gamma} = \begin{pmatrix} 1 - r_1 & \frac{\sqrt{2} - \sqrt{r_1 r_2}}{2} \\ \frac{\sqrt{2} - \sqrt{r_1 r_2}}{2} & 1 - r_2 \end{pmatrix}. \tag{4}$$

若 $X^{(1)} - \sqrt{\Gamma} X^{(2)} \sqrt{\Gamma}$ 的顺序主子式的行列式均为正, 即

$$1 - r_1 > 0, \quad \left|X^{(1)} - \sqrt{\Gamma} X^{(2)} \sqrt{\Gamma}\right| = \begin{vmatrix} 1 - r_1 & \frac{\sqrt{2} - \sqrt{r_1 r_2}}{2} \\ \frac{\sqrt{2} - \sqrt{r_1 r_2}}{2} & 1 - r_2 \end{vmatrix} = (1 - r_1)(1 - r_2) - \left(\frac{\sqrt{2} - \sqrt{r_1 r_2}}{2}\right)^2 > 0, \tag{5}$$

则 $X^{(1)} - \sqrt{\Gamma} X^{(2)} \sqrt{\Gamma}$ 正定, 克隆概率 (r_1, r_2) 可行, 否则 $X^{(1)} - \sqrt{\Gamma} X^{(2)} \sqrt{\Gamma}$ 非正定, 克隆概率 (r_1, r_2) 不可行.

- 对克隆概率 $\left(\frac{2-\sqrt{2}}{2}, \frac{2-\sqrt{2}}{2}\right)$,

$$1-r_1=\frac{\sqrt{2}}{2}>0, \quad \left|X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}\right|=(1-r_1)(1-r_2)-\left(\frac{\sqrt{2}-\sqrt{r_1r_2}}{2}\right)^2=\frac{6\sqrt{2}-7}{8}>0,$$

故 $X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}$ 正定, 克隆概率 $\left(\frac{2-\sqrt{2}}{2}, \frac{2-\sqrt{2}}{2}\right)$ 可行.

- 对克隆概率 $(1, 0.1)$,

$$1-r_1=0, \quad \left|X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}\right|=(1-r_1)(1-r_2)-\left(\frac{\sqrt{2}-\sqrt{r_1r_2}}{2}\right)^2=-\left(\frac{\sqrt{2}-\sqrt{0.1}}{2}\right)^2<0$$

故 $X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}$ 非正定, 克隆概率 $\left(\frac{2-\sqrt{2}}{2}, \frac{2-\sqrt{2}}{2}\right)$ 不可行.

- 对克隆概率 $(0.5, 0.5)$,

$$1-r_1=0.5>0, \quad \left|X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}\right|=(1-r_1)(1-r_2)-\left(\frac{\sqrt{2}-\sqrt{r_1r_2}}{2}\right)^2=\frac{4\sqrt{2}-5}{16}>0,$$

故 $X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}$ 正定, 克隆概率 $(0.5, 0.5)$ 可行.

- 对克隆概率 $(0.7, 0.7)$,

$$1-r_1=0.3>0, \quad \left|X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}\right|=(1-r_1)(1-r_2)-\left(\frac{\sqrt{2}-\sqrt{r_1r_2}}{2}\right)^2=0.3^2-\left(\frac{\sqrt{2}-0.7}{2}\right)^2<0,$$

故 $X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}$ 非正定, 克隆概率 $(0.7, 0.7)$ 不可行.

- 对克隆概率 $(0.9, 0.9)$,

$$1-r_1=0.1>0, \quad \left|X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}\right|=(1-r_1)(1-r_2)-\left(\frac{\sqrt{2}-\sqrt{r_1r_2}}{2}\right)^2=0.1^2-\left(\frac{\sqrt{2}-0.9}{2}\right)^2<0,$$

故 $X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}$ 非正定, 克隆概率 $(0.9, 0.9)$ 不可行.

(3) 以上几组方案中, 最优的克隆概率为 $(0.5, 0.5)$, 即无论 Alice 发送 $|\psi_1\rangle$ 和 $|\psi_2\rangle$ 中的任何一种, 窃听者 Eve 均有 0.5 的概率克隆成功, 有 $1-0.5=0.5$ 的概率克隆失败. 若 Eve 克隆成功, 则该次窃听不会被发现; 若 Eve 克隆失败, 则 Eve 随机发送的 $|\psi_1\rangle$ 和 $|\psi_2\rangle$ 中的一种, 有 $\frac{1}{2}$ 的概率和 Alice 发送的态相同, 有 $\frac{1}{2}$ 的概率和 Alice 发送的态不同. 若 Eve 随机选择的态和 Alice 发送的态相同, 则窃听仍不会被发现; 若 Eve 随机发送的态和 Alice 发送的态不同, 则 Bob 收到后, 若能成功生成秘钥, 则该秘钥必然错误, 从而在与 Alice 的比对中发现窃听. 综上, 每位秘钥的对比都有 $\frac{3}{4}$ 的概率发现 Eve 的窃听, 要使秘钥的安全性达到 99% 以上, 即

$$P_d=1-\left(\frac{3}{4}\right)^n>0.99 \tag{6}$$

则至少 $n\geq 17$, 即至少需要公开对照 17 组数据, 均检验无误, 才能确保该秘钥的安全性达到 99% 以上.

$\square$

第 2 题 得分: ________. 给出高维空间量子 teleportation 的数学证明.

证: 假设 Alice 处有一带传送的粒子, 标号为 1, 处于 N 维未知量子态

$$|\chi\rangle=\sum_{k=0}^{N-1}c_k|k\rangle, \tag{7}$$

Alice 和 Bob 共享一对处于 N 维最大纠缠态

$$|\psi_{00}\rangle=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle|j\rangle. \tag{8}$$

的粒子 2 和 3, 其中粒子 2 位于 Alice 处, 粒子 3 处于 Bob 处. 三个粒子的总量子态为

$$|\chi\rangle|\psi_{00}\rangle=\frac{1}{\sqrt{N}}\sum_{k,j=0}^{N-1}c_k|k\rangle|j\rangle|j\rangle. \tag{9}$$

取一组两粒子的纠缠态正交基

$$|\psi_{mn}\rangle=\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1}e^{i2\pi ln/N}|l\rangle|(l+m)\mod N\rangle, \tag{10}$$

和幺正变换

$$U_{mn}=\sum_{l=0}^{N-1}e^{i2\pi ln/N}|j\rangle\langle(l+m)\mod N|, \tag{11}$$

有

$$\begin{aligned}
U_{mn}^\dagger|\chi\rangle=&\sum_{l,k=0}^{N-1}c_ke^{-i2\pi ln/N}|(l+m)\mod N\rangle\langle l|k\rangle,\\
=&\sum_{l,k=0}^{N-1}c_ke^{-i2\pi ln/N}|(l+m)\mod N\rangle\delta_{lk}\\
=&\sum_{k=0}^{N-1}c_ke^{-i2\pi kn/N}|(k+m)\mod N\rangle, &(12)\\
|\psi_{mn}\rangle\otimes U_{mn}^\dagger|\chi\rangle=&\frac{1}{\sqrt{N}}\sum_{l,k=0}^{N-1}c_ke^{i2\pi(l-k)n/N}|l\rangle|(l+m)\mod N\rangle|(k+m)\mod N\rangle, &(13)\\
\frac{1}{\sqrt{N}}\sum_{m,n=0}^{N-1}|\psi_{mn}\rangle\otimes U_{mn}^\dagger|\chi\rangle=&\frac{1}{\sqrt{N}}\sum_{m,n,l,k=0}^{N-1}c_ke^{i2\pi(l-k)n/N}|l\rangle|(l+m)\mod N\rangle|(k+m)\mod N\rangle\\
&(\because\frac{1}{N}\sum_{n=0}^{N-1}e^{-i2\pi(k-l)n/N}=\delta_{lk})\\
=&\sum_{m,l,k=0}^{N-1}c_k\delta_{lk}|l\rangle|(l+m)\mod N\rangle|(k+m)\mod N\rangle\\
=&\sum_{m,k=0}^{N-1}c_k|k\rangle|(k+m)\mod N\rangle|(k+m)\mod N\rangle\\
&(\text{令 } j=(k+m)\mod N)\\
=&\sum_{k=0}^{N-1}c_k|k\rangle\otimes\sum_{j=0}^{N-1}|j\rangle|j\rangle\\
=&|\psi_{00}\rangle\otimes|\chi\rangle. &(14)
\end{aligned}$$

因此只需要 Alice 对粒子 1 和 2 以 $\{|\psi_{mn}\rangle\}$ 为基做正交测量, 并将测量结果以经典通讯方式告知 Bob, 然后 Bob 对粒子 3 做相应的幺正操作 U_{mn}, 就可以在粒子 3 上复现为原来待传粒子 1 的状态, 此即高维的 teleportation. □

第 3 题 得分: _________. 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 $\text{Prob}(\uparrow(\vec{n})\uparrow(\vec{m}))=\text{Tr}(E_A(\vec{n})E_A(\vec{m})\rho(\lambda))$
$E(\vec{n})$ 是 Alice 的比例投影到 $|\uparrow(\vec{n})\rangle$ 上的投影子.

解: a) 混合纠缠态 $\rho(\lambda)$ 可视为有 $1-\lambda$ 的概率处于 $|\psi^-\rangle\langle\psi^-|$ 的纠缠态, 而有 λ 的概率处于可分混合态 $\frac{1}{4}I\times I$ (无纠缠). $|\psi^-\rangle\langle\psi^-|$ 可用于准确地传递待传态, 保真度为 1, 而 $\frac{1}{4}I\otimes I$ 无法用于传态, 相当于传了一个随机的量子态, 仅有 $\frac{1}{2}$ 的保真度, 故利用 $\rho(\lambda)$ 进行 teleportation, 保真度为

$$F=(1-\lambda)+\frac{\lambda}{2}=1-\frac{\lambda}{2}. \tag{15}$$

若 A 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, 则保真度 (经典极限) 为 $\frac{2}{3}$.

$$F=1-\frac{\lambda}{2}>\frac{2}{3}\Longrightarrow\lambda<\frac{2}{3},$$

故当 $\lambda<\frac{2}{3}$, 则保真度优于经典极限.

b) 设 $\vec{n}=(\sin\theta\cos\phi,\sin\theta\sin\phi,\sin\theta)$, 则

$$\begin{aligned}E_A(\vec{n})=&\left(\cos\frac{\theta}{2}|0\rangle+e^{i\phi}\sin\frac{\theta_1}{2}|1\rangle\right)\left(\cos\frac{\theta}{2}\langle0|+e^{-i\phi}\sin\frac{\theta}{2}\langle1|\right)=\begin{pmatrix}\cos^2\frac{\theta}{2} & e^{i\phi}\cos\frac{\theta}{2}\sin\frac{\theta}{2}\\ e^{-i\phi}\cos\frac{\theta}{2}\sin\frac{\theta}{2} & \sin^2\frac{\theta}{2}\end{pmatrix}\\ =&\frac{1}{2}\begin{pmatrix}1+\cos\theta & e^{i\phi}\sin\theta\\ e^{-i\phi}\sin\theta & 1-\cos\theta\end{pmatrix}=\frac{1}{2}(I+\vec{n}\cdot\vec{\sigma}),\end{aligned} \tag{16}$$

其中 $\vec{\sigma}=\begin{pmatrix}\sigma_1 & \sigma_2 & \sigma_3\end{pmatrix}^T$. 同理,

$$E_A(\vec{m})=\frac{1}{2}(I+\vec{m}\cdot\vec{\sigma}). \tag{17}$$

$$\begin{aligned}\text{Prob}(\uparrow(\vec{n})\uparrow(\vec{m}))=&\text{Tr}(E_A(\vec{n})E_A(\vec{m})\rho(\lambda))=\text{Tr}\left(\frac{1}{2}(I+\vec{n}\cdot\vec{\sigma})\otimes\frac{1}{2}(I+\vec{m}\cdot\vec{\sigma})((1-\lambda)|\psi^-\rangle\langle\psi^-|+\frac{\lambda}{4}I\otimes I)\right)\\ =&\frac{1-\lambda}{4}\text{Tr}((I+\vec{n}\cdot\vec{\sigma})\otimes(I+\vec{m}\cdot\vec{\sigma})|\psi^-\rangle\langle\psi^-|)+\frac{\lambda}{16}\text{Tr}((I+\vec{n}\cdot\vec{\sigma})\otimes(I+\vec{m}\cdot\vec{\sigma})(I\otimes I))\\ =&\frac{1-\lambda}{4}\text{Tr}((I+\vec{n}\cdot\vec{\sigma})\otimes(I+\vec{m}\cdot\vec{\sigma})|\psi^-\rangle\langle\psi^-|)+\frac{\lambda}{16}\text{Tr}_A(I+\vec{n}\cdot\vec{\sigma})\,\text{Tr}_B(I+\vec{m}\cdot\vec{\sigma})\\ &(\because\text{Tr}\left(\frac{1}{2}(I+\vec{n}\cdot\vec{\sigma})=1\right))\\ =&\frac{1-\lambda}{4}\langle\psi^-|(I+\vec{n}\cdot\vec{\sigma})\otimes(I+\vec{m}\cdot\vec{\sigma})|\psi^-\rangle+\frac{\lambda}{4}\\ =&\frac{1-\lambda}{4}\langle\psi^-|I\otimes I|\psi^-\rangle+\frac{1-\lambda}{4}\langle\psi^-|\vec{n}\cdot\vec{\sigma}\otimes I|\psi^-\rangle+\frac{1-\lambda}{4}\langle\psi^-|I\otimes\vec{m}\cdot\vec{\sigma}|\psi^-\rangle\\ &+\frac{1-\lambda}{4}\langle\psi^-|\vec{n}\cdot\vec{\sigma}\otimes\vec{m}\cdot\vec{\sigma}|\psi^-\rangle+\frac{\lambda}{4}\\ =&\frac{1-\lambda}{4}\langle\psi^-|\vec{n}\cdot\vec{\sigma}\otimes I|\psi^-\rangle+\frac{1-\lambda}{4}\langle\psi^-|I\otimes\vec{m}\cdot\vec{\sigma}|\psi^-\rangle+\frac{1-\lambda}{4}\langle\psi^-|\vec{n}\cdot\vec{\sigma}\otimes\vec{m}\cdot\vec{\sigma}|\psi^-\rangle+\frac{1}{4}\end{aligned} \tag{18}$$

其中

$$\langle\psi^-|\vec{n}\cdot\vec{\sigma}\otimes I|\psi^-\rangle=\frac{1}{\sqrt{2}}(\langle01|-\langle10|)(\vec{n}\cdot\vec{\sigma}\otimes I)\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$$

$$
\begin{aligned}
&=\frac{1}{2}(\langle 01|-\langle 10|)((n_1\sigma_1+n_2\sigma_2+n_3\sigma_3)\otimes I)(|01\rangle-|10\rangle)\\
&=\frac{1}{2}(\langle 01|-\langle 10|)[n_1(|11\rangle-|00\rangle)+n_2(-i|11\rangle-i|00\rangle)+n_3(|01\rangle+|10\rangle)]\\
&=0,
\end{aligned}
\tag{19}
$$

同理,

$$
\langle\psi^-|I\otimes\vec{m}\cdot\vec{\sigma}\otimes I|\psi^-\rangle=0,
\tag{20}
$$

此外,

$$
\begin{aligned}
&\langle\psi^-|(\vec{n}\cdot\vec{\sigma}\otimes\vec{m}\cdot\vec{\sigma})|\psi^-\rangle\\
=&\frac{1}{\sqrt{2}}(\langle 01|-\langle 10|)[n_1m_1\sigma_1\otimes\sigma_1+n_1m_2\sigma_1\otimes\sigma_2+n_1m_3\sigma_1\otimes\sigma_3+n_2m_1\sigma_2\otimes\sigma_1+n_2m_2\sigma_2\otimes\sigma_2+n_2m_3\sigma_2\otimes\sigma_3\\
&+n_3m_1\sigma_3\otimes\sigma_1+n_3m_2\sigma_3\otimes\sigma_2+n_3m_3\sigma_3\otimes\sigma_3]\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)\\
=&n_1m_1+n_2m_2+n_3m_3=\cos\theta,
\end{aligned}
\tag{21}
$$

其中 θ 为 $\vec{n}$ 与 $\vec{m}$ 之间的夹角. 因此,

$$
\mathrm{Prob}(\uparrow(\vec{n})\uparrow(\vec{m}))=\frac{1-\lambda}{4}\cos\theta+\frac{1}{4}.
\tag{22}
$$

□