Problem Set 4 Solution

11.26

1 解答：(1) 在 Bob 进行正交测量后，Alice 与 Bob 公开通讯，Alice 告诉 Bob 测量为 $\perp$ 的结果在序列中的位置，建立秘钥。

(2) 由于态 $|0\rangle$ 与态 $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ 线性无关, 可以被克隆的充要条件为 $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ 半正定。其中

$X^{(1)}=\begin{pmatrix} 1 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 1 \end{pmatrix}$, $X^{(2)}=\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$

有 $Y^{(2)}=X^{(1)}-\sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}=\begin{pmatrix} 1-r_1 & \frac{1}{2}\sqrt{r_1\cdot r_2} \\ \frac{1}{2}\sqrt{r_1\cdot r_2} & 1-r_2 \end{pmatrix}$

可克隆条件为 $\det\left(Y^{(2)}\right)\geq 0$.

代入各组概率值可得 $\left(\frac{2-\sqrt{2}}{2},\frac{2-\sqrt{2}}{2}\right),(0.5,0.5)$ 满足条件，可以进行概率克隆。

(3) 以上最优的克隆方案的克隆概率为 (0.5,0.5). 故克隆失败并伪造信息错误的概率为 0.25. Alice 与 Bob 对比 N 组数据发现窃听者的概率为 $P=1-\left(\frac{3}{4}\right)^N$

由 $P\geq 0.99$ 可得 $N\geq 17$ (16 也算正确).

2 解答：

$$|\psi_{mn}\rangle=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}e^{2\pi jm/N}|j\rangle\otimes|(j+n)\bmod N\rangle$$

假设 $|\phi\rangle=\sum_{k=0}^{N-1}C_k|k\rangle$, 则

$$|\phi\rangle\otimes|\psi_{00}\rangle=\frac{1}{\sqrt{N}}\sum_{k,j}C_k|k\rangle\otimes|j\rangle\otimes|j\rangle$$

取 $U_{mn}^{\dagger}=\sum_{k}e^{-2\pi ilm/N}|(l+n)\mod N\rangle\langle l|$

有 $U_{mn}^{\dagger}|\phi\rangle=\sum_{kl}e^{-2\pi ilm/N}|(l+n)\mod N\rangle\langle l|k\rangle$

$$|\psi_{mn}\rangle\otimes U_{mn}^{\dagger}|\phi\rangle=\frac{1}{\sqrt{N}}\sum_{jk}e^{2\pi i(j-k)m/N}C_k|j\rangle\otimes|(j+n)\bmod N\rangle\otimes|(k+n)\bmod N\rangle$$

By $\sum_m e^{2\pi i(j-k)m/N} = N\delta_{jk}$,

$$\frac{1}{N}\sum_{mn} |\psi_{mn}\rangle \otimes U_{mn}^{\dagger} |\phi\rangle = \frac{1}{\sqrt{N}}\sum_{kn} C_k |k\rangle \otimes |(k+n) \bmod N\rangle \otimes |(k+n) \bmod N\rangle$$

and take $j = (k+n) \bmod N$, we have

$$\begin{aligned}&\tfrac{1}{N}\sum_{mn} |\psi_{mn}\rangle \otimes U_{mn}^{\dagger} |\phi\rangle = \tfrac{1}{\sqrt{N}}\sum_{jk} C_k |k\rangle \otimes |j\rangle \otimes |j\rangle \\ &= |\phi\rangle \otimes |\psi_{00}\rangle\end{aligned}$$

证毕.

3 解答：

(a) $|\psi^-\rangle\langle\psi^-|$ 对应概率为 $1-\lambda$, 保真度 $F=1$。$1-\lambda$ 对应概率为 λ, 此时 A 方只能随机发送信息给 B, 保真度 $F=\frac{1}{2}$。故 $\bar{F} = 1-\lambda+\frac{1}{2}\lambda = 1-\frac{1}{2}\lambda$。

已知经典极限为 $F_{cl} = \frac{2}{3}$, 故当 $\lambda < \frac{2}{3}$ 时将有 $\bar{F} > F_{cl}$.

(b)

$$\begin{aligned}&P = Tr_B Tr_A\left[\tfrac{1}{2}(I_A + \hat{n}\cdot\hat{\sigma}_A)\otimes\tfrac{1}{2}(I_B+\hat{m}\cdot\hat{\sigma}_B)\left(\tfrac{\lambda}{4}I_{AB} + (1-\lambda)|\psi^-\rangle\langle\psi^-|\right)\right] \\ &\ = \tfrac{\lambda}{16} Tr_B Tr_A\left[(I_A+\hat{n}\cdot\hat{\sigma}_A)\otimes(I_B+\hat{m}\cdot\hat{\sigma}_B) I_{AB}\right] \\ &\ + \tfrac{1-\lambda}{4} Tr_B Tr_A\left[(I_A+\hat{n}\cdot\hat{\sigma}_A)\otimes(I_A+\hat{m}\cdot\hat{\sigma}_B)|\psi^-\rangle\langle\psi^-|\right] \\ &= \tfrac{\lambda}{16} Tr_B Tr_A\left[I_A\otimes I_B\right] + \tfrac{1-\lambda}{4}\langle\psi^-|(I_A+\hat{n}\cdot\hat{\sigma}_A)(I_B+\hat{m}\cdot\hat{\sigma}_B)|\psi^-\rangle \\ &= \tfrac{1}{4} + \tfrac{1-\lambda}{4}\langle\psi^-|\hat{n}\cdot\hat{\sigma}_A\otimes\hat{m}\cdot\hat{\sigma}_B|\psi^-\rangle \\ &= \tfrac{1}{4} - \tfrac{1-\lambda}{4}\cos\theta\end{aligned}$$