第二章 量子通信

§2.1 量子态的克隆

1. 量子态的不可克隆定理

定理：量子力学中不存在任何操作（包括幺正演化和测量）能够将一个完全未知的量子态复制。

证明：（反证法）设存在一个装置，克隆完全未知的量子态，特别地对于态 $|\varphi_0\rangle, |\varphi_1\rangle$

克隆操作：$|\varphi_0\rangle|Q_x\rangle \longrightarrow |\varphi_0\rangle|\varphi_0\rangle|\widetilde{Q}_{0x}\rangle$

$|\varphi_1\rangle|Q_x\rangle \longrightarrow |\varphi_1\rangle|\varphi_1\rangle|\widetilde{Q}_{1x}\rangle$

装置的初态都是一样的 $|Q_x\rangle$.

若 $|\varphi\rangle = c_0|\varphi_0\rangle + c_1|\varphi_1\rangle$

△ 克隆操作一定是个线性操作

$|\varphi\rangle|Q_x\rangle = c_0|\varphi_0\rangle|Q_x\rangle + c_1|\varphi_1\rangle|Q_x\rangle \xrightarrow{\text{Clone}} c_0|\varphi_0\rangle|\varphi_0\rangle|\widetilde{Q}_0\rangle_x + c_1|\varphi_1\rangle|\varphi_1\rangle|\widetilde{Q}_1\rangle_x$

我们要求输出态为 $|\varphi\rangle|\varphi\rangle$.

1) 如果 $|\widetilde{Q}_0\rangle_x$ 与 $|\widetilde{Q}_1\rangle_x$ 相等

则系统的态 $c_0|\varphi_0\rangle|\varphi_0\rangle + c_1|\varphi_1\rangle|\varphi_1\rangle \neq |\varphi\rangle|\varphi\rangle$

2) 如果 $|\widetilde{Q}_0\rangle_x$ 与 $|\widetilde{Q}_1\rangle_x$ 不相等，则系统的态一定是个混合态 $\neq |\varphi\rangle|\varphi\rangle$.

∴ 无论是哪一种情况，$|\varphi\rangle$ 都不能被克隆。

进一步的想法：以上所考虑的是普适的克隆，那么，如果 $|\varphi\rangle$ 不是完全未知的，$|\varphi\rangle$ 属于某个态集合会怎样？

2. 有限态集合中的不可克隆定理

定理：设 $|\varphi_i\rangle$ 随机地选自于有限态集合 $S = \{|\varphi_1\rangle, |\varphi_2\rangle, \cdots, |\varphi_n\rangle\}$，当且仅当态集合中的态相互正交时，$|\varphi_i\rangle$ 可以被幺正地克隆.

证明：(1) 充分性.

设 $|\varphi_1\rangle|\varphi_2\rangle\cdots|\varphi_n\rangle$ 为系统 A 的可能的正交量子态，$\dim H_A \geq n$，引进辅助系统 B，$\dim(H_B) = \dim(H_A)$

复制前 $|\varphi_i\rangle_A|\psi\rangle_B$. 复制后要求 $|\varphi_i\rangle_A|\varphi_i\rangle_B$

复制前 ${}_A\langle\varphi_i|{}_B\langle\psi|\psi\rangle_B|\varphi_j\rangle_A = \delta_{ij}$ 复制后 ${}_A\langle\varphi_i|{}_B\langle\varphi_i|\varphi_j\rangle_B|\varphi_j\rangle_A = \delta_{ij}$

根据前面的引理（对吗），存在幺正变换 U_{AB}，使得

$U_{AB}|\varphi_i\rangle_A|\psi\rangle_B = |\varphi_i\rangle_A|\varphi_i\rangle_B$ U_{AB} 不依赖于 $|\varphi_i\rangle$ 的选择

（引理：如 $|\varphi_1\rangle, |\varphi_2\rangle, \cdots |\varphi_n\rangle$ 和 $|\widetilde{e}_1\rangle, |\widetilde{e}_2\rangle, \cdots |\widetilde{e}_n\rangle$ 满足 $\langle\varphi_i|\varphi_j\rangle = \langle\widetilde{e}_i|\widetilde{e}_j\rangle$ $(i,j) = 1, 2, \cdots n$)

则存在一个幺正算符 U，使得 $U|\varphi_i\rangle = |\widetilde{e}_i\rangle$.）

(2). 必要性. S不是正交态的集合, 设$|\varphi_1\rangle$, $|\varphi_2\rangle$不正交.

设$|\varphi_1\rangle$, $|\varphi_2\rangle$被同一个幺正过程克隆

$U(|\varphi_1\rangle_A|\psi\rangle_B)\otimes|Q_{0x}\rangle \longrightarrow |\varphi_1\rangle_A\otimes|\varphi_1\rangle_B\otimes|\widetilde{Q_1}\rangle_x$

$U(|\varphi_2\rangle_A|\psi\rangle_B)\otimes|Q_{0x}\rangle \longrightarrow |\varphi_2\rangle_A\otimes|\varphi_2\rangle_B\otimes|\widetilde{Q_2}\rangle_x$.

两式求内积: 左边 $=\langle\varphi_1|\varphi_2\rangle$ 右边 $=(\langle\varphi_1|\varphi_2\rangle)^2\langle\widetilde{Q_1}|\widetilde{Q_2}\rangle$

求绝对值: $|\langle\varphi_1|\varphi_2\rangle| = |\langle\varphi_1|\varphi_2\rangle|^2|\langle\widetilde{Q_1}|\widetilde{Q_2}\rangle|$

$\because |\langle\widetilde{Q_1}|\widetilde{Q_2}\rangle|\le 1$

$\Longrightarrow |\langle\varphi_1|\varphi_2\rangle|^2 \ge |\langle\varphi_1|\varphi_2\rangle|$

又$\because$ $|\varphi_1\rangle$ $|\varphi_2\rangle$不正交. $\therefore \langle\varphi_1|\varphi_2\rangle\neq 0$.

$\Longrightarrow |\langle\varphi_1|\varphi_2\rangle|\ge 1$. $\therefore$只有$|\varphi_1\rangle$ $|\varphi_2\rangle$相同才能被克隆.

$\therefore$当两个态不相等, 且非正交, 则不能通过一个幺正过程来克隆.

3. 量子态的概率克隆

非正交态能否被幺正演化+测量来克隆?

$|\psi_i\rangle_A|\psi_0\rangle_B \xrightarrow{U} |\Phi\rangle_{AB}$ 仍为纯态

测量 $\begin{cases}\text{选择性. 末态仍为纯态}\\\text{非选择性 末态为混合态}\end{cases}$

$\therefore$只能用选择性测量来实现. U演化+选择性测量.

定理1: $|\psi_i\rangle$随机地选自于一个态集合 $S=\{|\psi_1\rangle,|\psi_2\rangle,\cdots,|\psi_n\rangle\}$, 当且仅当$|\psi_1\rangle,|\psi_2\rangle,\cdots|\psi_n\rangle$线性无关时, $|\psi_i\rangle$可以通过幺正-塌缩过程以大于0的概率克隆.

证明: (1) 必要性: 线性相关的量子态一定不能概率克隆.

对态而言, 幺正演化是线性的 $U(c_1|\psi_1\rangle+c_2|\psi_2\rangle) = c_1U|\psi_1\rangle+c_2U|\psi_2\rangle$

选择性测量也是一个线性过程: 投影算子P. $P(c_1|\psi_1\rangle+c_2|\psi_2\rangle) = c_1P|\psi_1\rangle+c_2P|\psi_2\rangle$

(注意, 要区分"线性性"是针对态来说。投影算符对P而言是线性的, 但不是对态矢)

反证法: 设 $|\psi_n\rangle=\sum_{i=1}^{n-1}c_i|\psi_i\rangle$

设$U+P$过程可以克隆$|\psi_1\rangle,|\psi_2\rangle,\cdots|\psi_{n-1}\rangle$.

$|\psi_i\rangle|Q_0\rangle_x \xrightarrow{U+P} |\psi_i\rangle|\psi_i\rangle|\widetilde{Q_i}\rangle_x$.

则 $|\psi_n\rangle|Q_0\rangle_x \xrightarrow{U+P} \sum_{i=1}^{n-1}c_i|\psi_i\rangle|\psi_i\rangle|\widetilde{Q_i}\rangle_x$.

要求输出态 $|\psi_n\rangle|\psi_n\rangle$。若任何一个 $|\tilde{Q}_i\rangle \neq |\tilde{Q}_j\rangle$，则 Trace 后为混合态，若 $|\tilde{Q}_i\rangle$ 都相等，则 $\sum_{i=1}^{n-1} c_i|\psi_i\rangle|\psi_i\rangle$ 为一纠缠态。∴ 线性相关的量子集合也不可以被概率克隆机。

(2) 充分性。(构造性证明)

引入一个探测空间 H_ϕ $\dim H_\phi \geq n+1$ $|p_0\rangle, |p_1\rangle, \cdots, |p_n\rangle$ 为 H_ϕ 中 $n+1$ 个正交态。

如存在幺变换：

$$U(|\varphi_i\rangle|\Sigma\rangle|p_0\rangle) = \sqrt{r_i}|\varphi_i\rangle|\varphi_i\rangle|p_0\rangle + \sum_{j=1}^{n} c_j|\Phi_{AB}^j\rangle|p_j\rangle$$

这里 $|\Phi_{AB}^j\rangle$ 为复合空间 A、B 中的归一化态。

当我们探测系统 H_ϕ 当输出为 $|p_0\rangle$ 时，克隆成功，其概率为 r_i。

现在要证明这样的 U 是存在的。

根据幺正演化存在性的定理（演化前后保持内积不变，即 U 存在的充要条件）

定义：$X^{(1)} = [\langle\varphi_i|\varphi_j\rangle]$ 矩阵。

$X^{(2)} = [\langle\varphi_i|\varphi_j\rangle^2]$ $C = [c_j^*]$

$\Gamma = \mathrm{diag}(r_1, r_2, \cdots r_n)$ 概率矩阵

$\sqrt{\Gamma} = \sqrt{\Gamma}^\dagger = \mathrm{diag}\{\sqrt{r_1}, \sqrt{r_2}, \cdots, \sqrt{r_n}\}$

所以，如上式的幺正变换成立的充要条件是：

$$X^{(1)} = \sqrt{\Gamma}X^{(2)}\sqrt{\Gamma} + CC^\dagger$$

引理：如果 n 个态 $|\varphi_1\rangle, |\varphi_2\rangle, \cdots |\varphi_n\rangle$ 是线性无关的，那么 $X^{(1)} > 0$。

如 $X^{(1)} > 0$，则要求 $\forall$ $B = (b_1, b_2, \cdots b_n)^T$ $B \neq (0,0,0,\cdots 0)^T$

有 $B^\dagger X^{(1)} B > 0$。

现在 $B^\dagger X^{(1)} B = \sum_{ij} b_i^* X_{ij} b_j = \sum_{ij} b_i^* \langle\varphi_i|\varphi_j\rangle b_j = (\sum_i \langle\varphi_i| b_i^*)(\sum_j b_j|\varphi_j\rangle)$

∵ $|\varphi_1\rangle, \cdots |\varphi_n\rangle$ 线性无关。∴ $\sum_j b_j|\varphi_j\rangle \neq 0$。

∴ $B^\dagger X^{(1)} B > 0$。

∵ $X^{(1)} > 0$，只要我们选择足够小的 r_i，总可使得 $X^{(1)} - \sqrt{\Gamma}X^{(2)}\sqrt{\Gamma}$ 也是正定的。

$$X^{(1)} - \sqrt{\Gamma}X^{(2)}\sqrt{\Gamma} = V\,\mathrm{diag}\{m_1, m_2, \cdots, m_n\}V^\dagger$$

令 $C = V\,\mathrm{diag}\{\sqrt{m_1}, \sqrt{m_2}, \cdots, \sqrt{m_n}\}V^\dagger$

于是：$X^{(1)} = \sqrt{\Gamma}X^{(2)}\sqrt{\Gamma} + CC^\dagger$ 成立，进而可构造相应的 U。

定理2：态 $|\psi_1\rangle, |\psi_2\rangle, \cdots |\psi_n\rangle$ 的分别以概率 $r_1, r_2, \cdots r_n$ 精确克隆的充要条件是：

矩阵 $Y^{(2)} = X^{(2)} - \sqrt{\Gamma} X^{(2)} \sqrt{\Gamma}$ 半正定。

定理3：$|\psi_1\rangle, |\psi_2\rangle, \cdots |\psi_n\rangle$ 分别以 $r_1, r_2, \cdots r_n$ 精确克隆 m 份的充要条件是：

矩阵 $Y^{(m)} = X^{(1)} - \sqrt{\Gamma} X^{(m)} \sqrt{\Gamma}$ 半正定。

4. 量子态的认证：

输入 $|\psi_1\rangle, |\psi_2\rangle, \cdots |\psi_n\rangle$ n个之一，有n+1种测量结果

i) 测量结果为 $|i\rangle$, $\longrightarrow$ 确定为 $|\psi_i\rangle$ $i=1, 2, \cdots n$.

ii) 测量结果为 $|n+1\rangle$ $\longrightarrow$ 我们不知输入态为哪一个

∴ 量子态的认证是一种有n+1种结果的测量。

无穷次克隆与量子认证的等价性：

① $|\psi_i\rangle \longrightarrow |\psi_i\rangle^{\otimes\infty}$，则我们可以将 $|\psi_i\rangle$ 的信息完全把取出来

∵ 必要 $|\langle\psi_i|\psi_j\rangle| \neq 1 \Longrightarrow \langle\psi_i|^{\otimes\infty} |\psi_j\rangle^{\otimes\infty} = \delta_{ij}$ 于是，可以精确地认证 $|\psi_i\rangle$

② 一旦能够作精确认证，就可以做无穷次的克隆。

定理4：~~[redacted]~~

输入态 $|\psi_1\rangle, |\psi_2\rangle, \cdots |\psi_n\rangle$ 能分别以 $r_1, r_2, \cdots r_n$ 精确认证的充要条件是：矩阵 $X^{(1)} - \Gamma$ 半正定。

例子：两态 $|\psi_1\rangle, |\psi_2\rangle$，其出现概率为 $\{p_1, p_2\}$，对其做认证测量。求平均成功概率 $P_s = p_1 r_1 + p_2 r_2$ 的上限。

解：为能以 r_1, r_2 认证，要求 $X^{(1)} - \Gamma$ 半正定

$$X^{(1)} = \begin{bmatrix} 1 & X_{12} \\ X_{12}^* & 1 \end{bmatrix} \qquad X_{12} = \langle\psi_1|\psi_2\rangle \qquad X^{(1)} - \Gamma = \begin{pmatrix} 1-r_1 & X_{12} \\ X_{12}^* & 1-r_2 \end{pmatrix} \geq 0.$$

$$\Longrightarrow (1-r_1)(1-r_2) \geq |X_{12}|^2 .$$

$$\therefore \quad p_1 p_2 (1-r_1)(1-r_2) \geq p_1 p_2 |X_{12}|^2$$

又∵ $1 - p_1 r_1 - p_2 r_2 = p_1 + p_2 - p_1 r_1 - p_2 r_2 = p_1(1-r_1) + p_2(1-r_2) = 1 - P_s$

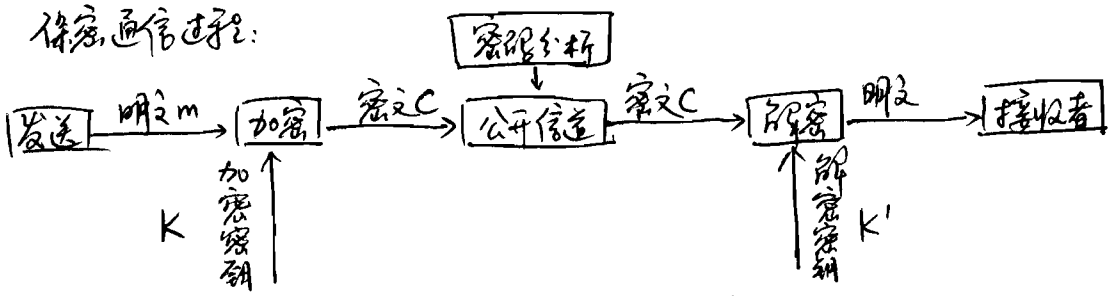
$$\left(\frac{1-P_s}{2}\right)^2 \geq p_1 p_2 (1-r_1)(1-r_2) \geq p_1 p_2 |X_{12}|^2$$

$$\Longrightarrow P_s \leq 1 - 2\sqrt{p_1 p_2}\,|\langle\psi_1|\psi_2\rangle|$$

§2.2. 量子密码方案

§2.2.1 保密通信的基本知识.

保密通信过程:



如 $K=K'$ 称为对称密钥体制; $K\neq K'$ 叫非对称密钥体制.

一般而言, 加密算法公开.

Shannon 的密码定理:

定理1: 在一个完全保密的体制中, 不同的密钥数不少于可能的明文数.

定理2: 若某一密钥体制的密钥数、密文数、明文数都相等, 则该体制完全保密的充要条件是:

①. 保每一明文加密为每一密文的密钥只有一个(一次一密体制) ②所有的密钥都以等概率出现.

例. Vernam 给出一次一密体制.

$$A\oplus C\oplus C=A$$

特点: ①. 绝对安全 ②密钥的需求量大. 问题: 怎样安全地传送密钥?

公钥体制: 加密算法公开, 加密密钥公开

解密密钥保密. $k'\neq k$.

一个基本的要求: 由 k 求 k', 涉及困难的算法.

k (某二进制数列长度为 n) $\longrightarrow k'$ 需要的计算规模 $O(e^n)$

§2.2.2. EPR QKD (Quantum Key Distribution) 1991 Ekert.

建立密钥的步骤

① Alice 制备 EPR 对序列, $|\Psi^-\rangle_{AB}\otimes|\Psi^-\rangle_{AB}\otimes|\Psi^-\rangle_{AB}$ 然后, 将B传送给 Bob.

② Alice, Bob 独立地、随机地测量 σ_x 或 σ_z, 依次测量所有的EPR对, 保留测量结果 (二进制序列),

③ Alice, Bob 公开通信. Alice 告诉 Bob 其测量的力学量 (σ_x or σ_z) 但保密测量结果。Bob 选择与 Alice 测量相同的情况 (并告知 Alice), 将测量结果保留下来, 形成密钥序列, 抛弃测量不同的结果。

④ 核验: Alice 和 Bob 随机地选择部分密码序列进行比较, 以确定是否有窃听者存在。

安全性分析: (假定: 不存在信道噪声; 不考虑测量误差; 设窃听者仅对比特序列进行窃听.

(排除联合窃听的情况)

建立EPR对时，Eve既要获得信息又要不能被发现。

$U_{BE}(|\psi_{AB}^-\rangle|e\rangle_E) \longrightarrow |r\rangle_{ABE}$.

※ E要与AB之间存在关联，同时又不能从A.B发现

※ A.B实施的测量为 $\sigma_x^A\sigma_x^B$ $\sigma_z^A\sigma_z^B$.

$\sigma_x^A\sigma_x^B|\psi^-\rangle_{AB} = -|\psi^-\rangle_{AB}$ ①

$\sigma_z^A\sigma_z^B|\psi^-\rangle_{AB} = -|\psi^-\rangle_{AB}$ ②

$|r\rangle_{ABE}$ 要满足以上条件.

$|r\rangle_{ABE}$ 可以做一般性展开：$|r\rangle_{ABE} = |00\rangle_{AB}|e_{00}\rangle_E + |01\rangle_{AB}|e_{01}\rangle_E + |10\rangle_{AB}|e_{10}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E$

为了满足条件①. $\sigma_x^A\sigma_x^B|\psi\rangle_{ABE} = -|r\rangle_{ABE}$

$\Longrightarrow |r\rangle_{ABE} = (|00\rangle - |11\rangle)|e_0\rangle + (|01\rangle - |10\rangle)|e_1\rangle$

为了满足条件② $\sigma_z^A\sigma_z^B|r\rangle_{ABE} = -|r\rangle_{ABE}$

$\Longrightarrow |r\rangle_{ABE} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)|e\rangle_E = |\psi^-\rangle_{AB}|e\rangle_E$

理想情况下，要满足①.②，则必须E与AB无纠缠。

§ 2.2.3 BB84 QKD

建立密钥的步骤：

① Alice从4态集合中$\{|\uparrow_z\rangle, |\downarrow_z\rangle, |\uparrow_x\rangle, |\downarrow_x\rangle\}$，随机、等概率地选择一个，发送给Bob.

② Bob对收到的态随机地测量 σ_x、σ_z（等概率各为$\frac{1}{2}$）.

正确的测量：σ_x（$|\uparrow_x\rangle$, $|\downarrow_x\rangle$） σ_z（$|\uparrow_z\rangle$, $|\downarrow_z\rangle$）测量结果唯一.

错误的测量：σ_x（$|\uparrow_z\rangle$, $|\downarrow_z\rangle$） σ_z（$|\uparrow_x\rangle$, $|\downarrow_x\rangle$）测量结果不确定.

③ 公开通信，Bob告诉Alice他所选择的测量量，Alice通知Bob保存正确的测量结果，形成密钥序列.

④ 检验过程：Alice.Bob选择部分密钥序列进行比较.

安全性分析：

BB84方案相当于将A方的测量过程前移（相对于EPR）

EPR：$|\psi^-\rangle_{AB}$ → 发送B粒子 → Alice.Bob同时对σ_x.σ_z进行测量.

BB84：$|\psi^-\rangle_{AB}$ → Alice随机地对σ_x.σ_z测量A粒子 → 将B粒子发送给Bob

→ Bob随机选择σ_x.σ_z对B粒子进行测量。

BB84的安全性：

① 拦截式窃听：A → E测量，由测量结果制备一个态再发送给B.

由于4个态非正交，它们不可以以相等概率1次区分 ∴拦截式窃听是不可能的.

② 复制式窃听：$|\psi\rangle_B|e_0\rangle_E \longrightarrow |\psi\rangle_B|\psi\rangle_E$，线性无关的态集不能被克隆.

§2.2.4 BB84方案(两态方案)

步骤: ①. Alice随机地选择两个非正交态$|\psi_1\rangle, |\psi_2\rangle$任意给Bob;

② Bob随机地选择两组测量基$\{|\psi_1\rangle\langle\psi_1|, |\psi_1^\perp\rangle\langle\psi_1^\perp|\}$, $\{|\psi_2\rangle\langle\psi_2|, |\psi_2^\perp\rangle\langle\psi_2^\perp|\}$之一;

③ 公开通信, Bob通知Alice测量为上的结果在序列中的位置, 从而建立密钥;

④ 检验, 比较部分密钥序列, 以确定是否有窃听存在。

安全性分析: (1) 拦截式窃听. (非正交态不可以以概率1识别)

(2) 复制式窃听 $|\psi_1\rangle, |\psi_2\rangle$非正交, 不能完全克隆; 它们不能以概率1克隆.

§2.2.5 基于正交态的量子密码方案

1. 正交态不可克隆定理:

$\psi_0(A_2, A_1)$
$\psi_1(A_2, A_1)$ —先把A_1传给B→ B
↑
Eve

B收到A_1后, A_2才出去, 使Eve不能同时拥有A_1, A_2, Eve只能分步窃听, 不能做联合测量和联合变换。

定理: 设$\{\rho_i(A_1, A_2)\}$为复合系统A_1, A_2的相互正交的可能量子态的集合, 设窃听者只能依次接收到A_1, A_2(收到A_2之前, A_1要离开Eve), 则态集合不能被Eve精确克隆的条件是:

① 约化态$\rho_i(A_1) = Tr_{A_2}\rho_i(A_1, A_2)$之间非正交且非全同;

② 约化态$\rho_i(A_2) = Tr_{A_1}\rho_i(A_1, A_2)$非正交.

播送: $|\psi_i\rangle\langle\psi_i| \to \rho_i^{\otimes 2}$

克隆与播送的区别.

证明: 1). 非正交且非全同的混合态不可克隆.

设U是这样的变换 (设E, Σ为任意态) (这是因为幺正变换保持内积不变)

$$E \otimes \Sigma \otimes \rho_i \xrightarrow{U} (|\psi_i\rangle\langle\psi_i|_{E\Sigma}) \otimes \rho_i$$

$$Tr_E(|\psi_i\rangle\langle\psi_i|_{E\Sigma}) = \rho_i$$

由U变换的保迹性:

变换前后有: $Tr(E E\otimes\Sigma\Sigma)\, tr(\rho_0\rho_1) = Tr(\rho_0\rho_1)\, Tr(|\psi_0\rangle\langle\psi_0||\psi_1\rangle\langle\psi_1|)$

$\because Tr_E(|\psi_1\rangle\langle\psi_1|) \neq Tr_E(|\psi_0\rangle\langle\psi_0|) \Longrightarrow |\psi_0\rangle \neq |\psi_1\rangle$

$\therefore Tr(|\psi_0\rangle\langle\psi_0||\psi_1\rangle\langle\psi_1|) < 1$

$\Longrightarrow Tr\rho_0\rho_1 = 0$ $\therefore \rho_1, \rho_0$正交.

$\therefore$ 非正交且非全同的量子态不可以被确定性地克隆.

2). 一个混合态的集合, 可以被确定性地识别(概率为1), 当集合中的态都正交.

3). $\rho_i(A_1)$非正交, 不可识别, $\rho_i(A_2)$非正交, 亦不可识别.

如密码克隆，则存在窃听方式.

假如 $\rho_0(A_1)=\rho_1(A_1)$

窃听过程：① Eve收到 A_1 后，发送 B_1 粒子给Bob $\rho(B_1)=\rho_0(A_1)=\rho_1(A_1)$

② Eve收到 A_2 后，由于 $\rho_1(A_1,A_2)$ 全部被Eve所掌握；而 $\rho_0(A_1,A_2)$ 与 $\rho_1(A_1,A_2)$ 正交，Eve手里有对 A_1，A_2 做联合测量，从而很好地区别出态。

这时，Eve若再发送 B_2，使得 $\rho_1(B_1,B_2)=\rho_1(A_1,A_2)$，则窃听成功。

∴ Eve有必先制备态 $\rho_x(B_1,B_2)$

如 $U_{B_2}\rho_x(B_1,B_2)=\rho_1(A_1,A_2)$ 则成功.

已知 $Tr_{B_2}\rho_x(B_1,B_2)=Tr_{A_2}\rho_0(A_1,A_2)=Tr_{A_2}\rho_1(A_1,A_2)$

根据GHJW定理：不同纯化之间仅差一个扩展空间的么正变换。于是，该窃听策略是可行的。

2. 基于正交态的QKD.

(1) 三态方案 (PRL 75, 1239, 1995)

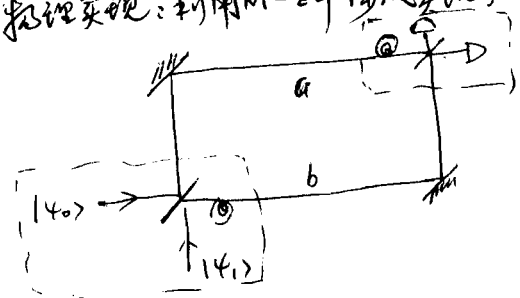
Alice发送的态有：$|\psi_0\rangle=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle-|1\rangle|0\rangle)$

$|\psi_1\rangle=\frac{1}{\sqrt{2}}(|0\rangle|1\rangle+|1\rangle|0\rangle)$

$|\psi_2\rangle=|0\rangle|0\rangle$

$\rho_0(A_1)=\rho_1(A_1)=\frac{1}{2}(|0\rangle\langle 0|+|1\rangle\langle 1|)$ $\rho_2(A_1)=|0\rangle\langle 0|$ 满足不可克隆的条件

物理实现：利用M-Z干涉仪实现编码过程.



Alice在邻近和t时刻，随机发送 $|\psi_0\rangle$，$|\psi_1\rangle$。中间如有在窃听者，由于引入了延迟，要求a进入Bob前系统后，b才离开Alice，延迟 $\tau>\frac{l}{c}$。(在特定时间段，Eve仅允许一定的操作)

(2) 二态方案 (1992 PRL. 69, 2883)

发送态 $|\psi_0\rangle=\cos\alpha|01\rangle+\sin\alpha|10\rangle$

$|\psi_1\rangle=\sin\alpha|01\rangle-\cos\alpha|10\rangle$ $\alpha\neq\frac{\pi}{4}k$

约化算符：$\rho_0(A_1)=\cos^2\alpha|0\rangle\langle 0|+\sin^2\alpha|1\rangle\langle 1|$ $\rho_1(A_1)=\sin^2\alpha|0\rangle\langle 0|+\cos^2\alpha|1\rangle\langle 1|$

(3) 三个直积态的方案 (PRL. 1998)

$|\psi_0\rangle=|00\rangle$ $|\psi_1\rangle=|10\rangle$ $|\psi_2\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|1\rangle$ → 把供保护.

$\rho_0(A_1)=|0\rangle\langle 0|$ $\rho_1(A_1)=|1\rangle\langle 1|$ $\rho_2(A_1)=\frac{1}{2}(|0\rangle+|1\rangle)(\langle 0|+\langle 1|)$

非正交态的量子密钥分享效率较低，存在冲突攻击的漏洞；正交态密钥分享解决了漏洞问题。但缺乏分辨仪器，效率未必提得很高。

§ 2.2.6. 关于QKD的安全性.

QKD的安全性所要进一步考虑的问题

①. 考虑信道噪声　②考虑联合窃听　③考虑窃听者的延迟测量.

※ Nielsen & Chuang 的关于安全的QKD的定义：

如果Alice和Bob选择任意的两个安全参数 $\varepsilon>0$ 和 $\ell>0$，对于任意的窃听策略，或者该协议中止，或者以 $m\,[1-O(2^{-\varepsilon})]$ 的概率成功，并且可以保证 Eve 同最终的密钥序列所获的信息量小于 $2^{-\ell}$。同时，密钥序列必须基本上也是随机的。那么，该QKD是安全的。

问题可以简化为：一个数据块中有t个错误，Alice可以编码她的量子比特成为到t位错的量子纠错码，Bob可以在解码过程中将这些中间干扰滤掉。 (QKD ⟷ 量子纠错)

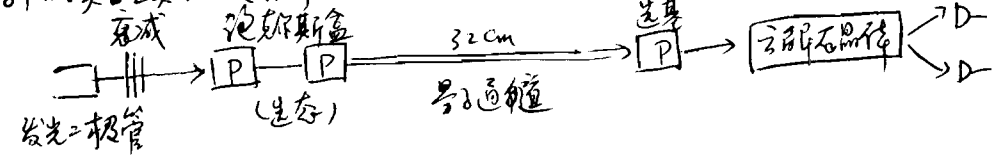
但这引来进一步的困难：需要量子计算机和量子存储器.

(目前的应用中：借助经典的保密放大技术：(从n个数据中提出m个数据，从而满足一定的安全限制).

进一步的考虑：① 可容忍的窃听上限是什么？

② 量子密钥的最终容量有多大？比特率问题.

BB84的实验实现（目前，BB84在设计时是安全的）(89年 Bennett)



$\langle n\rangle = 0.1$.　双光子的可能性 ~ 0.01

衡量标准：通信长度、比特率、错误率.

现在：光纤量子密钥 150~165 km (北京-天津 实际光纤中125km).

自由空间的量子密钥 23km. (2002 or 03?)

§ 2.3. 量子的态的纠缠及其相关问题.

量子密钥：通过量子通道，建立经典信息关联.

量子态的传送：通过EPR对 + 经典通信 (teleportation).

①. EPR纠缠只不能传递信息的.

$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$\rho_{\phi^+}^{(A)} = \rho_{\phi^+}^{(B)} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$

对A系做操作，最广泛的形式是选择一个测量：$\rho_{AB} = \sum_{ij} \frac{1}{2}|i\rangle\langle j|$

$\mathrm{Tr}_A \rho_{AB} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$　　$\mathrm{Tr}_A \sum_k F_k \$_A(\rho_{AB}) = \mathrm{Tr}_A \frac{1}{2}\sum_k F_k \sum_\mu A_\mu |i\rangle\langle j| A_\mu^\dagger \otimes |i\rangle\langle j|$

$= \frac{1}{2}\mathrm{Tr}_A \sum_{ij\mu} A_\mu |i\rangle\langle j| A_\mu^\dagger \otimes |i\rangle\langle j| = \frac{1}{2}\mathrm{Tr}\sum_{ij}|i\rangle\langle j| \otimes |i\rangle\langle j| = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$

即：B不论看到密度矩阵的任何变化.

② 经典通信不能完全传送量子态.

采用经典手段传量子态：Alice先对量子态进行测量，将测量结果传给Bob，Bob依靠测量结果制备一个态于来近似最初的态.

$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$.　Alice测量：$\{|\uparrow\rangle\langle\uparrow|, |\downarrow\rangle\langle\downarrow|\}$　$\rho_{out} = P_\uparrow|\uparrow\rangle\langle\uparrow| + P_\downarrow|\downarrow\rangle\langle\downarrow|$

其中 $P_\uparrow = |\langle\psi|\uparrow\rangle|^2$　$P_\downarrow = |\langle\psi|\downarrow\rangle|^2$

则 ρ_{out} 与 $|\psi\rangle$ 的保真度为：$\langle\psi|\rho_{out}|\psi\rangle = P_\uparrow^2 + P_\downarrow^2$.

$\overline{F} = \int(|\langle\psi|\uparrow\rangle|^4 + |\langle\psi|\downarrow\rangle|^4)d\psi = \frac{2}{3}$.

2.3.2. quantum teleportation

基本步骤：① A B双方建立EPR对 $|\phi^+\rangle_{23} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$;

② A输入粒子态$|\psi\rangle$完全未知，A方对1、2粒子做联合Bell基的测量;

③ A方将测量结果通知给B方(2-bit信息)

④ B方根据测量结果做一个相应的幺正变换(此幺正变换为4种可能的变换之一，它并不依赖于$|\psi\rangle$.

$|\psi\rangle_1|\phi\rangle_{23} = (a|0\rangle + b|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$= \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{b}{\sqrt{2}}|111\rangle$

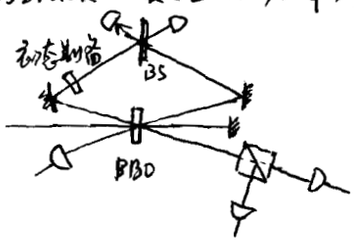
$= \frac{1}{2}\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)(a|0\rangle + b|1\rangle) + \frac{1}{2}\left(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)\right)(a|0\rangle - b|1\rangle)$

$+ \frac{1}{2}\left(\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\right)(a|1\rangle + b|0\rangle) + \frac{1}{2}\left(\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\right)(a|1\rangle - b|0\rangle)$

$= \frac{1}{2}|\phi^+\rangle_{12}|\psi\rangle_3 + \frac{1}{2}|\phi^-\rangle_{12}\sigma_z|\psi\rangle_3 + \frac{1}{2}|\psi^+\rangle_{12}\sigma_x|\psi\rangle_3 + \frac{1}{2}|\psi^-\rangle_{12}(-i\sigma_y)|\psi\rangle_3$

实验上的困难：① 产生EPR对. ② Bell基的测量. ③ 受控幺正变换

Innsbruck的实验(1997年).



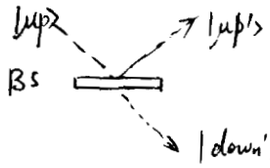
A：脉冲光源通过BBO晶体，通过自发参量下转换产生偏振纠缠.　(type II)

B：用分束器做出六个Bell基测量(只测量其中之一)

(加了滤波器，提高了相干时间 500fs. > 脉冲宽度 200fs)

C：没有幺正变换.

关于双光子Bell态的识别：（通过BS）



$|up\rangle \xrightarrow{U_{BS}} \frac{1}{\sqrt{2}}(|up'\rangle + |down'\rangle)$

$|down\rangle \xrightarrow{U_{BS}} \frac{1}{\sqrt{2}}(|up'\rangle - |down'\rangle)$

双光子情形：

当两个波包在BS上相遇，我们可以将其视为全同波色子。

于是，两个波色子的波函数应满足交换对称性。在双光子情形，满足

该条件的有：$|\Psi^-\rangle|\Psi_A\rangle$，$|\Psi^+\rangle|\Psi_S\rangle$ $|\Psi^+\rangle|\Psi_S\rangle$，$|\Psi^-\rangle|\Psi_S\rangle$

$|\Psi_A\rangle = \frac{1}{\sqrt{2}}(|up\rangle|down\rangle - |down\rangle|up\rangle)$ $|\Psi_S\rangle = \frac{1}{\sqrt{2}}(|up\rangle|down\rangle + |down\rangle|up\rangle)$

$U_{BS}|\Psi_A\rangle = \frac{1}{\sqrt{2}}(|up'\rangle|down'\rangle - |down'\rangle|up'\rangle)$ $U_{BS}|\Psi_S\rangle = \frac{1}{\sqrt{2}}(|up'\rangle|up'\rangle - |down'\rangle|down'\rangle)$

于是，只要在BS的输出端，我们探测出一上一下分别有一个光子输出，我们就可以判定其偏振为$|\Psi^-\rangle$态。

如果在输出端，我们继续对偏振分辨，则可检验出$|\Psi^+\rangle$态；但$|\Psi^\pm\rangle$无法区分。

最近经证明，通过线性光学器件，无法区分4种偏振纠缠的Bell态。

Shih. YH 通过光学的办法（非线性）区分4个Bell态，但效率低。

2.3.3. Dense Coding 密集编码 Bennett. PRL 69, 2881 (1992)

一个量子比特至多可以传送一个比特的经典信息（Holove极限）。

Dense Coding：利用EPR对来1个量子比特传送多于1bit的信息。

步骤：① 先在A、B之间建立一个EPR对；

② A方对其拥有的1个做4种可能的变换之一（$I, \sigma_x, \sigma_z, -i\sigma_y$），由GHJW定理得对到4个Bell基的映射。

③ A方将其拥有的1传送给Bob，Bob对其拥有的1、2做一个联合Bell基的测量，若完全区分4个Bell基，Bob将获得2比特的信息。

Dense Coding 可以看作是teleportation的逆问题。

teleportation：2个经典比特 + 1 ebit $\xrightarrow{传}$ 1 qubit.

dense coding：1 qubit + 1 ebit $\xrightarrow{传}$ 2个经典比特。

2.3.4. 纠缠与teleportation和纠缠交换

$|\Phi^+_{23}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{23} + |11\rangle_{23})$

$W^+_{14} = |0\rangle_1|x_0\rangle_4 + |1\rangle_1|x_1\rangle_4$ （$|x_0\rangle, |x_1\rangle$ 明显非系数）

归一性条件为：$\langle x_0|x_0\rangle + \langle x_1|x_1\rangle = 1$

则: $|\Psi_{14}^+\rangle |\Psi_{23}^+\rangle$

$= \frac{1}{2}|\Psi^+\rangle_{12}(|\chi_0\rangle_4|0\rangle_3 + |\chi_1\rangle_4|1\rangle_3) + \frac{1}{2}|\Psi^+\rangle_{12}(|\chi_0\rangle_4|1\rangle_3 + |\chi_1\rangle_4|0\rangle_3) + \frac{1}{2}|\Psi^-\rangle_{12}(|\chi_0\rangle_4|1\rangle_3 - |\chi_1\rangle_4|0\rangle_3)$

$+ \frac{1}{2}|\Psi^-\rangle_{12}(|\chi_0\rangle_4|0\rangle_3 - |\chi_1\rangle_4|1\rangle_3)$

$= \frac{1}{2}|\Psi^+_{12}\rangle|\Psi_{34}\rangle + \frac{1}{2}|\Psi^+\rangle_{12}\sigma_3^x|\Psi_{34}\rangle + \frac{1}{2}|\Psi^-\rangle_{12}(-i\sigma_3^y)|\Psi_{34}\rangle + \frac{1}{2}|\Phi^-\rangle_{12}\sigma_3^z|\Psi_{34}\rangle$.

引申变换: 1/4 的 teleportation.

1.4 都处于 EPR 对. $\frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$ 2.3 处于 EPR 对 $\frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$

如测到到 $|\Psi^-\rangle_{12}$ 则 $|\Psi^-\rangle_{34}$.

2.3.5. 高维 Hilbert 空间的 teleportation

$N\times N$ 维空间的最大纠缠态.

$|\Psi_{00}\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle\otimes|j\rangle$.

$|\Psi_{mn}\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{i2\pi jm/N}|j\rangle\otimes|(j+n) \bmod N\rangle$

$\langle\Psi_{kl}|\Psi_{mn}\rangle = \delta_{nl}\sum_{j=0}^{N-1} e^{\frac{i2\pi}{N}j(m-k)} = \delta_{nl}\delta_{mk}$.

设 1 粒子. $|\phi_1\rangle = \sum_{k=0}^{N-1} C_k|k\rangle$

2.3 处于 $|\phi_{00}\rangle_{23} = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle_2\otimes|j\rangle_3$.

$|\phi\rangle_1\otimes|\Psi_{00}\rangle_{23} = \frac{1}{N}\sum_{mn}|\Psi_{mn}\rangle_{12}\otimes U_{mn}^+|\phi\rangle_3$

其中 $U_{mn} = \sum_k e^{i2\pi km/N}|k\rangle\langle(k+n) \bmod N|$ 为与 $|\phi\rangle$ 无关的幺正矩阵.