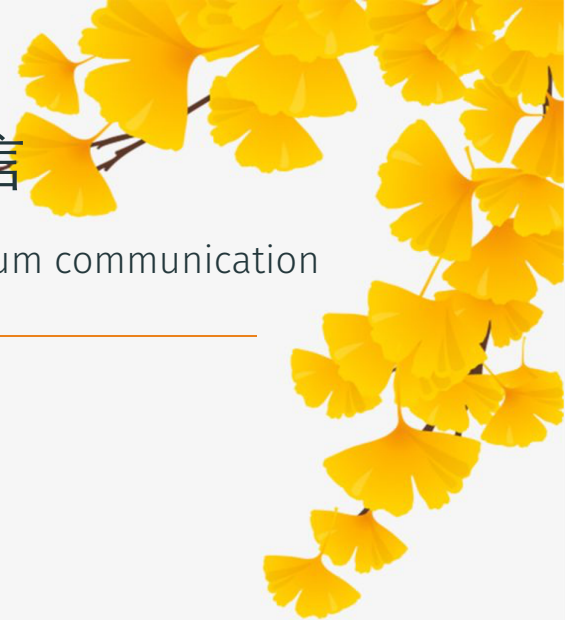
量子信息与量子通信

Quantum information and quantum communication

李小飞

光电科学与工程学院

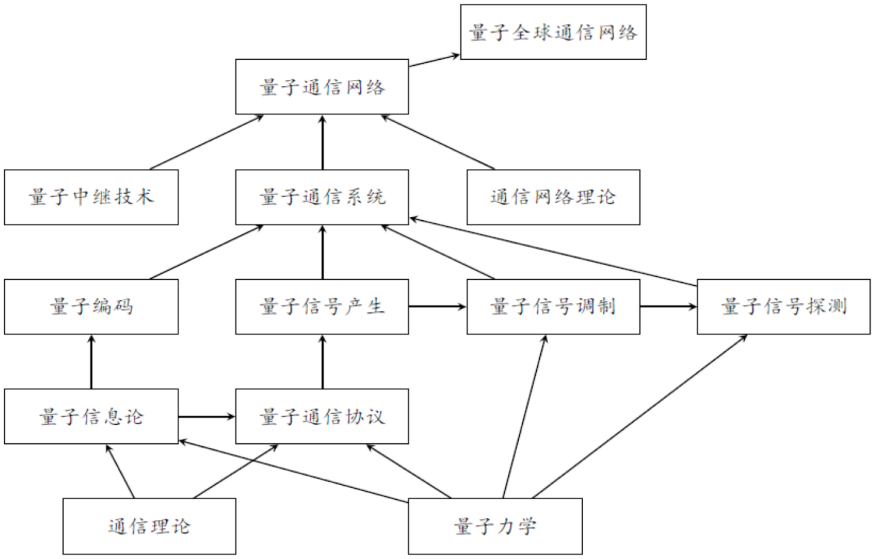
2022 年 3 月 11 日



第 8: 量子通信 (1)

Contents

量子通信网络


量子全球通信网络
量子通信网络
量子中继技术
量子通信系统
通信网络理论
量子编码
量子信号产生
量子信号调制
量子信号探测
量子信息论
量子通信协议
通信理论
量子力学

假设一个事件有 N 种可能的结果，对应的概率分布为 $\{p_k\}$, 则香农熵定义为:

$$H(x) = \sum_{k=1}^{N} p_k \log_2 \frac{1}{p_k} \text{ (bit)}$$

代表测得可获取信息量的平均值

对于 2 态事件，有:

$$\begin{aligned} H_2 &= p_0 \log_2 \frac{1}{p_0} + p_1 \log_2 \frac{1}{p_1} \\ &= p \log_2 \frac{1}{p} + (1-p) \log_2 \frac{1}{(1-p)} \\ &= 1; \quad \text{if} \quad p = \frac{1}{2} \end{aligned}$$

设体系第 n 个本征态出现的概率为 p_n，则密度矩阵和熵分别定义为：

$$\rho = \sum_{n=1} p_n |n\rangle\langle n|$$

$$S(\rho) = -\operatorname{tr}\left(\rho \log_2 \rho\right)$$

对于双粒子体系：有

$$S\left(\rho_{AB}\right) = -\operatorname{tr}\left(\rho_{AB} \log_2 \rho_{AB}\right)$$

$$S\left(\rho_A \otimes \rho_B\right) = S\left(\rho_A\right) + S\left(\rho_B\right)$$

$$S\left(\rho_A; \rho_B\right) = \left[S\left(\rho_A\right) + S\left(\rho_B\right)\right] - S\left(\rho_{AB}\right)$$

- 原文：I love you
- 密文：M PSZI CSY
- 加码函数：$f(x) = x + \alpha \bmod 26$
- 解码函数：$f^{-1}(y) = y - \alpha \bmod 26$
- 密钥：$\alpha = 4$
- 原文序列：abcdefghijklmnopqrstuvwxyz
- 密文序列：abcdefghijklmnopqrstuvwxyz

请问有多少个可能密钥？

- 原文字符串长度为 n

$$a_1 a_2 a_3 \dots a_n$$

- 信息发送者制备一个长度也为 n 的密钥串

$$b_1 b_2 b_3 \dots b_n$$

- 加密函数

$$c_i = a_i + b_i \bmod N$$

- 密文串

$$c_1 c_2 c_3 \dots c_n$$

- 解密函数

$$a_i = c_i - b_i \bmod N$$

- RSA 密码方案: R.L.Rivest，A.Shamir 和 L.Adelman 于 1978 年提出的
- 依据: “验证两个大素数容易，而将他们的乘积做因数分解则极其困难”
- 原文: X
- 密文: Y
- 加密: 使用公钥 (e, N) $Y = X^e \bmod N$
- 解密: 使用私钥 (d, N) $X = Y^d \bmod N$

制备： (e,d,N)

1. 秘密选择两个大素数 p, q
2. 计算出 $N = p \times q$
3. 计算出欧拉函数 $\Phi(N) = (p-1) \times (q-1)$
4. 选择一个较小的素数 e 做为公钥, 它与 $\Phi(N)$ 互质
5. 计算私钥 d, $ed \equiv 1 \mod \Phi(N)$

破解： 想从 e 得到 d, 必须知道 $\Phi(N)$； 想要得到 $\Phi(N)$， 必须知道 p, q; 想要得到 p, q， 必须做大数质因式分解 $N = p \times q$!

- 密使分发　　怕汉奸!
- 公开分发　　怕量子算法!

必须发展量子算法破解不了的量子密钥公开分发方案!

- 克隆 (cloning) 指在目标系统 (B) 中产生一个与源系统 (A) 相同的态，而不改变源系统的态。

例-1. 试证明未知量子态不可克隆:

证明: 设已知的本征态可以克隆

$$U_c |C\rangle |0\rangle_A |\varphi\rangle_B = |C_0\rangle |0\rangle_A |0\rangle_B$$

$$U_c |C\rangle |1\rangle_A |\varphi\rangle_B = |C_1\rangle |1\rangle_A |1\rangle_B$$

若 A 处于未知叠加态

$$|\Psi\rangle_A = \alpha |0\rangle + \beta |1\rangle$$

期望的克隆:

$$\begin{aligned} U_c|C\rangle|\psi\rangle_A|\varphi\rangle_B &= |C_\psi\rangle\,|\psi\rangle_A|\psi\rangle_B \\ &= |C_\psi\rangle\,(\alpha|0\rangle+\beta)|1\rangle)_A\,(\alpha|0\rangle+\beta|1\rangle)_B \\ &= |C_\psi\rangle\,(\alpha^2|0\rangle_A|0\rangle_B+\alpha\beta|0\rangle_A|1\rangle_B+\alpha\beta|1\rangle_A|0\rangle_B \\ &\quad +\beta^2|1\rangle_A|1\rangle_B) \end{aligned}$$

服从量子力学的过程:

$$\begin{aligned} U_c|C\rangle|\psi\rangle_A|\varphi\rangle_B &= U_c|C\rangle\,(\alpha|0\rangle+\beta|1\rangle)_A\,|\varphi\rangle_B \\ &= U_c|C\rangle\alpha|0\rangle_A|\varphi\rangle_B+U_c|C\rangle\beta|1\rangle_A|\varphi\rangle_B \\ &= \alpha^2\,|C_0\rangle\,|0\rangle_A|0\rangle_B+\beta^2\,|C_1\rangle\,|1\rangle_A|1\rangle_B \end{aligned}$$

两式相等的必要条件为 $\alpha\beta=0$, 即可克隆的 $|\Psi\rangle_A$ 态不可能是叠加态!

证毕!

- 删除是指如果目标系统 (B) 有源系统 (A) 的量子态副本，把 B"置零"而不改变 A 系统的状态

例-2. 试证明未知量子态不可删除:

证明: 设已知的本征态可以删除

$$U_c |C\rangle |0\rangle_A |0\rangle_B = |C_{00}\rangle |0\rangle_A |R\rangle_B$$

$$U_c |C\rangle |1\rangle_A |1\rangle_B = |C_{11}\rangle |0\rangle_A |R\rangle_B$$

$$U_c |C\rangle |0\rangle_A |1\rangle_B = |C_{01}\rangle |0\rangle_A |1\rangle_B$$

$$U_c |C\rangle |1\rangle_A |0\rangle_B = |C_{10}\rangle |0\rangle_A |0\rangle_B$$

对于叠加态，期望的删除:

$$\begin{aligned} U_c|C\rangle|\psi\rangle_A|\psi\rangle_B &= |C_\psi\rangle\,|\psi\rangle_A|R\rangle_B \\ &= |C_\psi\rangle(\alpha\,|0\rangle+\beta\,|1\rangle)_A|R\rangle_B \end{aligned}$$

服从量子力学的过程:

$$\begin{aligned} U_c|C\rangle|\psi\rangle_A|\psi\rangle_B =& U_c|C\rangle(\alpha|0\rangle+\beta|1\rangle)_A(|\alpha|0\rangle+\beta|1\rangle)_B \\ =& U_c|C\rangle\alpha^2|0\rangle_A|0\rangle_B + U_c|C\rangle\beta^2|1\rangle_A|1\rangle_B \\ &+ U_c|C\rangle\alpha\beta|0\rangle_A|1\rangle_B + U_c|C\rangle\alpha\beta|1\rangle_A|0\rangle_B \\ =& \alpha^2\,|C_{00}\rangle\,|0\rangle_A|R\rangle_B + \beta^2\,|C_{11}\rangle\,|1\rangle_A|R\rangle_B \\ &+ |C_{01}\rangle\,\alpha\beta|0\rangle_A|1\rangle_B + |C_{10}\rangle\,\alpha\beta|1\rangle_A|0\rangle_B \end{aligned}$$

两式根本无法相等，即可删除的 $|\Psi\rangle_A$ 态不可能是叠加态!

证毕!

1. 量子通信基础

2. 量子密码分发 Quantum key Distribution

BB84 量子密码分发协议

BB84 协议

1984 年，C. H. Bennett 和 G. Brassard 提出利用偏振光进行量子密钥分发的协议。把一次性密码原理和量子测量原理结合在一起，建立不可破解密码分发方案

1. Ailce 由随机数序列 a 决定选择纵横基还是对角基。设 a 中的 0 代表纵横基$|0\rangle, |1\rangle$，1 代表对角基$|+\rangle, |-\rangle$
2. Ailce 再由随机数序列 a' 决定发射给 Bob 的光子的具体偏振。设 a' 中的 0 代表 $|0\rangle, |+\rangle$

   设有 $a = 0010$，$a' = 1001$：Ailce 发出的光子的偏振序列为 $|10 + 1\rangle$
3. Bob 得到偏振光子串后，由随机数序列 b 决定选择纵横基还是对角基，再由随机数序列 b' 决定用相应基里的那个基矢波片进行测量

   设有 $b = 0110$，$b' = 1100$：Bob 使用的偏振片序列为 $|1 - +0\rangle$
4. 双方公布第一序列（a=0010 and b=0110），发现第 1、3 位相同。
5. 双方就知道各自手里的 $a' = 1001$ 和 $b' = 1100$ 中的第 1、3 位相同。整理出来，为 10, 并以此做为私钥 d, 完成密钥分发。

保密性分析:

1. 设有窃听者 C，先得到 A 发给 B 的每一个光子。这阻断了 A、B 之间的通信，没有得到 d。
2. C 想知道光子的状态，若测量，因不知道具体的基，导致每个光子有 50% 概率状态改变。
3. C 因不知光子状态，不能进行克隆，强行克隆势必导致原光子状态改变。
4. C 只能窃听 Ailce 和 Bob 的通信，得到 a 和 b，但不是 a' 和 b'。
5. 派内鬼分别去 Ailce 和 Bob 的办公室，窃取 a' 和 b'，难度大于窃取 d。

例-试求 x=11 和 N=21 的阶 r:

解:(1) 取 $r = 1, 2, 3, \cdots$, 依次计算 11^r

(2) 依次计算 $\frac{11^r}{21}$ 的余数

(3) 第一个余数为 1 的 r=6，得解

左表表明，阶就是余子式（完全集）的自由度

r	x^r(x=11)	x^r mod 21
0	1	1
1	11	11
2	121	16
3	1331	8
4	14641	4
5	161051	2
6	1771561	1
7	19487171	11
8	214358881	16
9	2357947691	8
10	25937424601	4
11	2.85312E+11	2
12	3.13843E+12	1
13	3.45227E+13	11

例-试证明求阶问题与因式分解问题等价:

证明:设 N 可以作因子分解 $N = n_1 \times n_2$ 若阶 r 为偶数，有

$$x^r = 1(modN)$$

$$x^r - 1 = M \times N$$

$$(x^{r/2} - 1)(x^{r/2} + 1) = M \times N = M \times n_1 \times n_2$$

上式表明，求最大公约数

$$gcd(x^{r/2} - 1, N); \quad gcd(x^{r/2} + 1, N)$$

很可能就能得到因子 n_1 和 n_2
因此，因式分解问题就转化求阶问题，它们是等价的!

- 阶 r 就是余子式（完全集）的自由度。
- 量子傅里叶变换公式中，N 就是基矢数目

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{i\frac{2\pi}{N}jk}$$

- 量子力学表明这个数目就是体系的自由度，即上式可取 $N = r$

余子式 $\{|x^k \ mod \ N\rangle\}$ 构成完全集，任意态函数可在其上展开，比如本征态 S

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-i\frac{2\pi}{r}sk} |x^k \ mod \ N\rangle$$

对上式做傅里叶逆变换

$$\left|x^k \ mod \ N\right\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-i\frac{2\pi}{r}sk} \left|u_s\right\rangle$$

取 k=0，得到余子式 1 态在量子本征函数系 $\{|u_s\rangle\}$ 的展开式

$$\left|x^0 \ mod \ N\right\rangle = \sum_{s=0}^{r-1} \frac{1}{\sqrt{r}} \left|u_s\right\rangle = \sum_{s=0}^{r-1} a_s \left|u_s\right\rangle$$

其振幅 (展开系数)$a_s = \frac{1}{\sqrt{r}}$, 完全由阶 (r) 决定!

u_s 的本征值

试证明相位估计算子 U 的本征态 u_s 的本征值为 $\exp[i2\pi\varphi] = \exp[i2\pi\frac{s}{r}]$

即要证明其本征方程为:

$$U\left|u_s\right\rangle = \exp[i2\pi\frac{s}{r}]\left|u_s\right\rangle$$

证明: 相位估计算子 U 在余子式有如下作用效果

$$U\left|y\right\rangle = \left|xy \mod N\right\rangle$$

$$\left|u_s\right\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-i\frac{2\pi}{r}sk}\left|x^k \mod N\right\rangle$$

$$\begin{aligned} U\left|u_s\right\rangle &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-i\frac{2\pi}{r}sk}U\left|x^k \mod N\right\rangle \\ &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-i\frac{2\pi}{r}sk}\left|x^{k+1} \mod N\right\rangle \\ &= \frac{1}{\sqrt{r}}\sum_{k'=1}^{r} e^{-i\frac{2\pi}{r}s(k'-1)}\left|x^{k'} \mod N\right\rangle \end{aligned}$$

$$= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=1}^{r} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=1}^{r-1} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle + \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} e^{-i\frac{2\pi}{r}sr} \left| x^{r} \mod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=1}^{r-1} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle + \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} e^{-i2\pi s} \left| x^{0} \mod N \right\rangle$$

$$= \frac{1}{\sqrt{r}} e^{i\frac{2\pi}{r}s} \sum_{k'=0}^{r-1} e^{-i\frac{2\pi}{r}sk'} \left| x^{k'} \mod N \right\rangle$$

$$= \exp[i2\pi\frac{s}{r}] \left| u_s \right\rangle$$

证毕!

$$U\left|u_s\right\rangle = \exp[i2\pi\frac{s}{r}]\left|u_s\right\rangle = \exp[i2\pi\varphi]\left|u_s\right\rangle$$

因此

$$\varphi = \frac{s}{r}$$

φ 可通过傅里叶逆变换求得，则阶 r 可通过连分数算法求得

$$S_n = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}} \qquad \pi = \cfrac{1}{3 + \cfrac{1}{7 + \cfrac{1}{15 + \dots}}}$$

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \dots}}}}}$$

$\frac{1}{1}$ $\frac{3}{2}$ $\frac{7}{5}$ $\frac{17}{12}$

- 有理数的连分数表示是有限的
- 任一有理数的连分数表示是唯一的
- “简单”有理数的连分数表示是简短的

Thanks for your attention!

A & Q