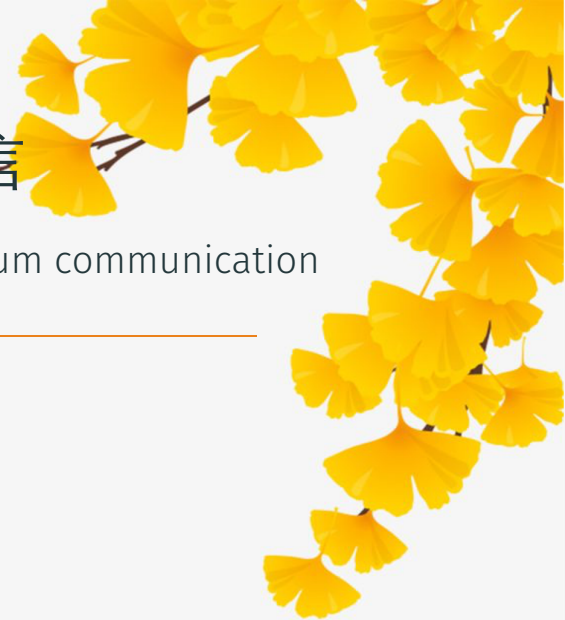
量子信息与量子通信

Quantum information and quantum communication

李小飞

光电科学与工程学院

2022 年 3 月 17 日

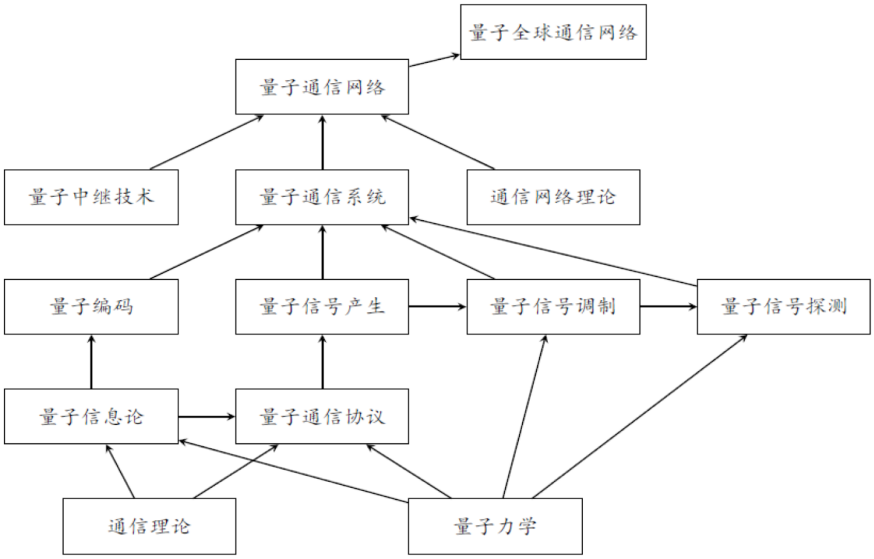


第 8: 量子通信 (1)

2. 量子密码分发

1. 量子通信基础

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!

1. 量子通信基础

2. 量子密码分发

量子不可克隆原理

量子不可删除原理

BB84 协议

B92 协议

1. 量子通信基础

2. 量子密码分发

量子不可克隆原理

量子不可删除原理

BB84 协议

B92 协议

- 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!

1. 量子通信基础

2. 量子密码分发

量子不可克隆原理

量子不可删除原理

BB84 协议

B92 协议

- 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

量子不可克隆原理

量子不可删除原理

BB84 协议

B92 协议

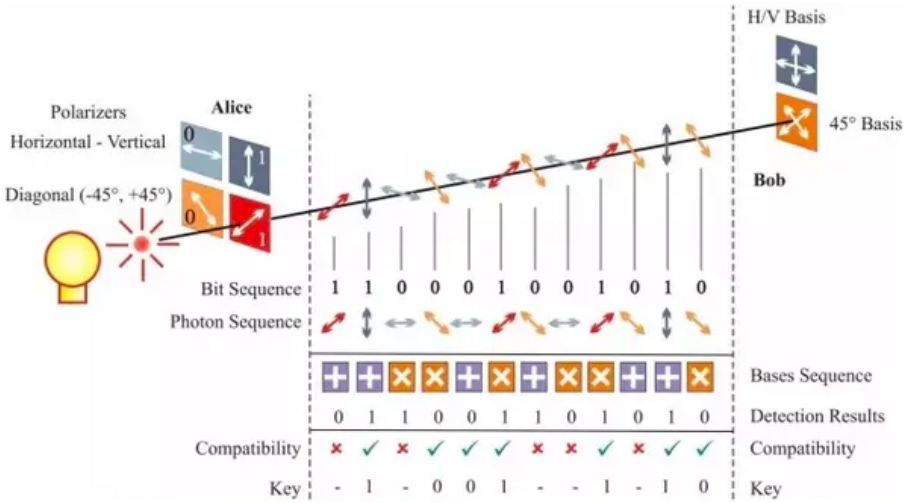
BB84 协议

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 a' 中的 1 代表 $|1\rangle, |-\rangle$

   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。


H/V Basis
45° Basis
Bob
Alice
Polarizers
Horizontal - Vertical
Diagonal (-45°, +45°)
0
1
0
1
Bit Sequence
1 1 0 0 0 1 0 0 1 0 1 0
Photon Sequence
Bases Sequence
0 1 1 0 0 1 1 0 1 0 1 0
Detection Results
Compatibility
✗ ✓ ✗ ✓ ✓ ✓ ✗ ✗ ✓ ✗ ✓ ✓
Compatibility
Key
- 1 - 0 0 1 - - 1 - 1 0
Key

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。

(目前已走向实用!)

- 信息协调 (Information Reconciliation):

信息协调即密钥纠错 (Error Correction)，目的是保证 Alice 和 Bob 共同拥有的密钥的一致性。

由于可能被 C 窃听，得保证公布的信息越少越好。而信道噪声或第三方窃听而导致的无效的部分进行删除，

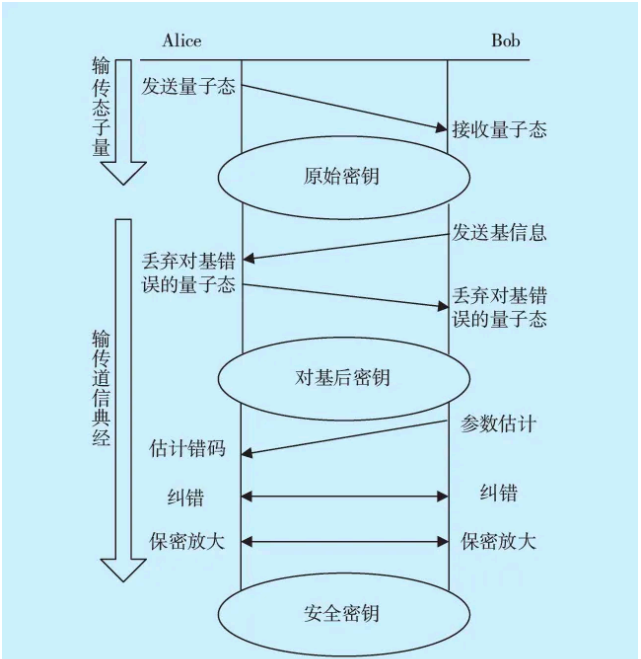
因此, 信息协调后的密钥将更短。

- 隐私增强 (Privacy Amplification):

使密钥得以增强的一种方式，。

(1) 公布的信息被窃听,(2) 信息协调被窃听, 窃听都知道的东西较多, 有被破解的风险. 比如排列组合!

隐私增强即利用 Alice 和 Bob 手中的现有密钥，再生成一个新的、更短的密钥，相当于二次加密, 增强破解难度.


Alice
Bob
输传态子量
发送量子态
接收量子态
原始密钥
发送基信息
丢弃对基错误的量子态
丢弃对基错误的量子态
输传道信典经
对基后密钥
参数估计
估计错码
纠错
纠错
保密放大
保密放大
安全密钥

1. 量子通信基础

2. 量子密码分发

量子不可克隆原理

量子不可删除原理

BB84 协议

B92 协议

BB84 协议要用四个偏振，1992 年，C. H. Bennett 提出用两个非正交偏振态也可进行密码分发!

原理:

(1) A 制备有二个偏振态

$$|0\rangle, |-\rangle \quad \rightarrow 0, 1$$

因此有:

$$\langle -|0\rangle = \frac{\langle 0|0\rangle - \langle 1|0\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}$$

(2) B 有两个检测器

$$P_{-} = 1 - |-\rangle\langle -|$$

$$P_0 = 1 - |0\rangle\langle 0|$$

(3) 若 A 发来的是 $|0\rangle$

$$\langle 0|P_{-}|0\rangle = 1\,\langle 0|0\rangle - \langle 0|-\rangle\,\langle -|0\rangle = 1 - \frac{1}{2} = \frac{1}{2}$$

若 A 发来的是 $|-\rangle$

$$\langle -|P_0|-\rangle = 1\,\langle -|-\rangle - \langle -|0\rangle\,\langle 0|-\rangle = 1 - \frac{1}{2} = \frac{1}{2}$$

即与 BB84 一样,0 和 1 态的光子各以 50% 的概率由 A 成功传送到 B! 因此可用于密码分发.

1991 年, Eckert A. 发布 E91 协议, 它是基于 EPR 纠缠对实现密码分发的试分析其工作原理, 并做出保密性分析

Thanks for your attention!

A & Q