

量子密码的基础知识

方

2020/9/16

Bell state

$$\begin{aligned} |\Psi^-\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B) = \frac{1}{\sqrt{2}} (|+\rangle_A |-\rangle_B + |-\rangle_A |+\rangle_B) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) = \frac{1}{\sqrt{2}} (|+\rangle_A |+\rangle_B + |-\rangle_A |-\rangle_B) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B) = \frac{1}{\sqrt{2}} (|-\rangle_A |+\rangle_B - |+\rangle_A |-\rangle_B) \\ |\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B) = \frac{1}{\sqrt{2}} (|+\rangle_A |+\rangle_B - |-\rangle_A |-\rangle_B) \end{aligned}$$

费马小定理：设P是任意大于2的素数，q是任意与P互素的非零整数，则有 $q^{p-1} \equiv 1 \pmod{p}$.

If p is a prime number, for any integer a , $a^{p-1}(a-1)$ is an integer multiple of p , i.e. $a^p \equiv a \pmod{p}$. 费马小定理推论：p和q是两个互素且大于2的

整数，a是任意与pq互素的非零整数，则有 $a^{(q-1)(p-1)} \equiv 1 \pmod{n}$

科考夫原则：

1. 表述一：一个密码系统的设计不应当是保密的，其原理细节应当是公开的
2. 表述二：一个密码系统哪怕它的一切有关信息是公开的，只要其密钥是隐秘的，它就是安全的

安全性:

1. Computational security: 计算安全性: 适用最好的破译算法来破解该密码系统至少需要N次计算, 当N远大于窃听者所能调用的全部计算能力, 可称该密码系统对该窃听者是具有计算安全性的
2. provable security: 可证明安全性: 破解该系统等价于求解某一困难的数学问题
3. unconditional security: 无条件安全性: 即便给予窃听者无限的计算资源, 其利用某破译算法也不能破解该密码系统

针对密码系统的攻击:

1. 唯密文攻击: ciphertext only attack
2. 已知明文攻击: known plaintext attack (密文 + 明文-密文对)
3. 选择明文攻击: chosen plaintext attack (密文+指定一些明文得到相应的密文)
4. 选择密文攻击: chosen ciphertext attack (密文+指定一些密文得到相应的明文)

完善保密性: 如果一个密码系统满足: 对于任意的明文 $x \in \mathcal{P}$ 和密文 $y \in \mathcal{P}$ 均有给定密文 y , 明文 x 的先验概率和后验概率是相等的 $P(x|y) = P(x)$, $P(y|x) = P(y)$. (给定明文x, 任意密文y, 都至少存在一个密钥K, 是的x可被加密成y)

$$\begin{cases} \text{加密函数是一个单射函数} \implies |K| \gg |C| \\ \text{解密函数是一个单射函数} \implies |C| \gg |P| \end{cases} \implies |K| \gg |C| \gg |P| \quad (1)$$

从二进制数据来看, 加密的密钥长度应该不少于明文的长度

任何攻击条件下都具有无条件安全性的密码系统只有“一次一密”系统。

量子不可克隆三种等价表述

1. 不存在能完美克隆任意未知量子态的量子克隆机
2. 不存在能完美克隆两个非正交量子态的量子克隆机
3. 不可能从非正交量子态中获取编码信息同时不扰动量子态

投影测量:

$$\begin{cases} \hat{P}_i^\dagger \hat{P}_i = \hat{P}_i^2 = \hat{P}_i \\ \hat{P}_i \hat{P}_j = 0 \quad i \neq j \\ \text{定义可观测物理量} \quad \hat{A} = \sum_i i \hat{P}_i \end{cases}$$

广义测量: 整体量子系统通常是高纬度的复杂系统, 量子测量针对的仅仅是这个系统的某个子空间, 把这种局域的量子测量, 看作是对整体系统进行投影测量的一个部分。

经过投影测量后, 不同测量结果下的量子态不一定正交。

正算符取值测量 (POVM)对于算符集合 $\{\hat{M}_i\}$, 定义算子 $\hat{F}_i = \hat{M}_i^\dagger \hat{M}_i$. 则 \hat{F}_i 满足:

$$\begin{cases} \sum_i \hat{F}_i = \sum_i \hat{M}_i^\dagger M_i = \hat{I} \\ \langle \phi | \hat{F}_i | \phi \rangle = \langle \phi | \hat{M}_i^\dagger \hat{M}_i | \phi \rangle \geq 0 \end{cases}$$

Neumark定理: 对于任意给定的POVM, 可以将所考虑的态空间拓展到一个较大空间, 并通过在这个较大的空间中进行某种投影测量, 来实现给定的POVM测量。

$$[\hat{x}_i, \hat{y}_j] = 0$$

$$[\hat{\rho}_i, \hat{\rho}_j] = 0$$

$$[\hat{x}_i, \hat{p}_j] = i\hbar\delta_{ij}$$

$$[\hat{L}_i, \hat{L}_j] = i\hbar\epsilon_{ijk}\hat{L}_k$$

$$[\hat{s}_i, \hat{s}_j] = i\hbar\epsilon_{ijk}\hat{s}_k$$

$$[\hat{s}_i, \hat{s}_j]_+ = \frac{\hbar^2}{2}\delta_{ij}$$

$$\hat{\sigma} = \frac{2}{\hbar}\hat{s}$$

$$\begin{aligned}
[\hat{\sigma}_i, \hat{\sigma}_j] &= 2i\epsilon_{ijk}\hat{\sigma}_k \\
[\hat{\sigma}_i, \hat{\sigma}_j]_+ &= 2\delta_{ij} \\
\hat{\sigma}_2^2 &= \hat{\sigma}_i\hat{\sigma}_i^\dagger = \hat{I} \\
[\hat{J}_i, \hat{J}_j] &= i\hbar\epsilon_{ijk}\hat{J}_k \\
[\hat{J}^2, \hat{J}_\pm] &= 0 \\
[\hat{J}^2, \hat{J}_i] &= 0 \\
[\hat{J}_z, \hat{J}_\pm] &= \pm\hbar\hat{J}_\pm \\
\begin{cases} [\hat{J}^2, \hat{J}_\pm] = 0 \\ [\hat{J}_z, \hat{J}_\pm] = \pm\hbar\hat{J}_\pm \end{cases} &\Rightarrow \begin{cases} \hat{J}^2(\hat{J}_\pm|\lambda, m\rangle) = \lambda\hbar^2\hat{J}_\pm|\lambda, m\rangle \\ \hat{J}_z(\hat{J}_\pm|\lambda, m\rangle) = (m \pm 1)\hbar\hat{J}_\pm|\lambda, m\rangle \end{cases} \\
\Rightarrow \hat{J}_\pm|\lambda, m\rangle &= \sqrt{(j \mp m)(j \pm m + 1)}|\lambda, m \pm 1\rangle
\end{aligned}$$

$$\begin{aligned}
\hat{a}^+ &= \sqrt{\frac{m\omega}{2\hbar}}(\hat{x} - \frac{1}{m\omega}i\hat{p}) \\
\hat{a} &= \sqrt{\frac{m\omega}{2\hbar}}(\hat{x} + \frac{1}{m\omega}i\hat{p}) \\
[\hat{a}, \hat{a}^+] &= 1
\end{aligned}$$

$$\begin{aligned}
[\hat{a}, \hat{H}] &= \hbar\omega\hat{a} \\
[\hat{a}^+, \hat{H}] &= -\hbar\omega\hat{a} \\
[\hat{a}^\dagger, \hat{a}, \hat{H}] &= 0 \\
\hat{a}^+|n\rangle &= \sqrt{n+1}|n+1\rangle \\
\hat{a}|n\rangle &= \sqrt{n}|n-1\rangle
\end{aligned}$$

真空中电磁波的传播

$$\begin{aligned}
\nabla \times \vec{H} &= \frac{\partial \vec{D}}{\partial t} & \nabla \times \vec{E} &= -\frac{\partial \vec{B}}{\partial t} \\
\nabla \cdot \vec{B} &= 0 & \nabla \cdot \vec{D} &= 0
\end{aligned}$$

介质中电磁波的传播

$$\begin{aligned}\nabla \times \vec{H} &= \frac{\partial \vec{D}}{\partial t} + \vec{J}_f & \nabla \times \vec{E} &= -\frac{\partial \vec{B}}{\partial t} \\ \nabla \cdot \vec{B} &= 0 & \nabla \cdot \vec{D} &= \rho_f\end{aligned}$$

$$\begin{aligned}\nabla \times \vec{H} &= \frac{\partial \vec{D}}{\partial t} & \nabla \times \vec{E} &= -\frac{\partial \vec{B}}{\partial t} \\ \nabla \cdot \vec{B} &= 0 & \nabla \cdot \vec{D} &= 0 \\ \vec{B} &= \mu_0 \vec{H} & \vec{D} &= \epsilon_0 \vec{E}\end{aligned}$$

真空中电磁波的传播，没有色散。介质的色散是指电容率和磁导率随着电磁波的频率而变的现象。

$$\begin{aligned}\nabla \times \vec{B} &= \mu_0 \epsilon_0 \frac{\partial \vec{E}}{\partial t} & \nabla \times \vec{E} &= -\frac{\partial \vec{B}}{\partial t} \\ \nabla \cdot \vec{B} &= 0 & \nabla \cdot \vec{E} &= 0\end{aligned}$$

$$\begin{aligned}\nabla \times (\nabla \times \vec{B}) &= \mu_0 \epsilon_0 \frac{\partial \nabla \times \vec{E}}{\partial t} & \nabla (\nabla \times \vec{E}) &= -\frac{\partial \nabla \times \vec{B}}{\partial t} \\ &= \mu_0 \epsilon_0 \left(-\frac{\partial^2 \vec{B}}{\partial t^2} \right) & &= \mu_0 \epsilon_0 \left(-\frac{\partial^2 \vec{E}}{\partial t^2} \right)\end{aligned}$$

$$\nabla \times (\nabla \times \vec{B}) = \nabla (\nabla \cdot \vec{B}) - \nabla^2 \vec{B}$$

时谐波：以单一频率 ω (k) 作振荡的电磁波。对于单一频率的电磁波有如下公式

$$\frac{\partial}{\partial t} \rightarrow -i\omega$$

$$\vec{B} = -\frac{i}{k} \sqrt{\mu\epsilon} \nabla \times \vec{E} = -\frac{i}{\omega} \nabla \times \vec{E}$$

$$\vec{E} = \frac{i}{k} \frac{1}{\sqrt{\mu\epsilon}} \nabla \times \vec{B} = \frac{i}{\omega\mu\epsilon} \nabla \times \vec{B}$$

$$k = \omega\sqrt{\epsilon\mu}$$

设沿x轴传播, $\vec{E}(\vec{x}) = \vec{E}_0 e^{ikx}$.

$$\vec{E}(\vec{x}, t) = \vec{E}_0 e^{i(kx - \omega t)} \quad \vec{B}(\vec{x}, t) = \vec{B}_0 e^{i(kx - \omega t)}$$

$$\vec{E}(\vec{x}, t) = \vec{E}_0 (\cos(kx - \omega t) + i \sin(kx - \omega t))$$

波动方程:

$$\nabla^2 \vec{E} - (\epsilon_0 \mu_0)^2 \frac{\partial^2 \vec{E}}{\partial t^2} = 0$$

假设电场的振动方向为x轴方向, $\vec{E} = E_x \vec{e}_x$

$$E_x = \sum_j A_j q_j(t) \cdot \sin(k_j z) \quad A_j = \sqrt{\frac{2\omega_j}{v\epsilon_0}} \quad k_j = j \frac{\pi}{L}$$

$$H_y(z, t) = \sum_j A_j \frac{q_j(t)\epsilon_0}{k_j} \cos(k_j z)$$

定义两个算符 $\hat{a}_j, \hat{a}_j^\dagger$

$$\hat{a}_j e^{-i\omega_j t} = \sqrt{\frac{1}{2\hbar\omega_j}} (\omega_j \hat{q}_j + i\hat{p}_j)$$

$$\hat{a}_j^\dagger e^{i\omega_j t} = \sqrt{\frac{1}{2\hbar\omega_j}} (\omega_j \hat{q}_j - i\hat{p}_j)$$

$$[\hat{a}_i, \hat{a}_j] = 0$$

$$[\hat{a}_i^\dagger, \hat{a}_j^\dagger] = 0$$

$$[\hat{a}_i, \hat{a}_j^\dagger] = i\hbar\delta_{ij}$$

由定义可以得到

$$E_x = \sum_j \epsilon_j (\hat{a}_j e^{-i\omega_j t} + \hat{a}_j^\dagger e^{i\omega_j t}) \sin(k_j z)$$

$$H_y(z, t) = -i\epsilon_0 \cdot c \sum_j \epsilon_j \dots$$

光子数算符: $\hat{n} = \hat{a}^\dagger \hat{a}$, 满足 $\hat{a}^\dagger \hat{a} |n\rangle = \hat{n} |n\rangle = n |n\rangle$.

$$\hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle \quad \hat{a} |n\rangle = \sqrt{n} |n-1\rangle$$

$$(\hat{a}^\dagger)^n |n\rangle = \sqrt{n!} |n\rangle$$

相干态：相干态光场可以看作是由于经典电流辐射产生的光场，定义为位移算符作用于真空而产生的光场态

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle \quad \hat{D}(\alpha) = \exp(\alpha\hat{a}^+ - \alpha^*\hat{a})$$

$$\hat{D}(\alpha)^\dagger \hat{D}(\alpha) = \hat{D}(\alpha)\hat{D}^\dagger(\alpha) = \hat{I}$$

$$\begin{aligned}\hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha) &= \hat{a} + \alpha \\ \hat{D}^\dagger(\alpha)\hat{a}^\dagger\hat{D}(\alpha) &= \hat{a}^\dagger + \alpha^* \\ \Leftarrow B - C - H \text{引理} : e^{-\alpha A}Be^{\alpha A} &= B - \alpha[A, B] + \frac{1}{2!}[A, [A, B]] + \dots\end{aligned}$$

$$\begin{aligned}\hat{a}|\alpha\rangle &= \alpha|\alpha\rangle \\ \Leftarrow \hat{a}|\alpha\rangle &= \hat{a}\hat{D}(\alpha)|0\rangle = (\hat{D}(\alpha)\hat{D}^\dagger(\alpha))\hat{a}\hat{D}(\alpha)|0\rangle \quad (\hat{a}|0\rangle = 0)\end{aligned}$$

相干态可以用Fock态展开：

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

相干态光子数分布：

$$\begin{aligned}p(n) &= |\langle n|\alpha\rangle|^2 \\ &= \frac{\langle n \rangle^n e^{-\langle n \rangle}}{n!}\end{aligned}$$

相干态具有最小不确定性，是一个最小测不准波包：

$$\Delta\hat{q} \cdot \Delta\hat{q} = \frac{\hbar}{2}$$

相干态 $|\alpha\rangle$ 构成了一组超完备基， $\frac{1}{\pi} \int |\alpha\rangle \langle \alpha| d^2\alpha = \hat{I}$. 且有 $|\langle \alpha|\alpha' \rangle|^2 = \exp(-|\alpha - \alpha'|^2) \neq 0$, 不正交.

$$\begin{cases}
\hat{x} = \frac{\hat{a} + \hat{a}^+}{2} \sqrt{\frac{2\hbar}{m\omega}} & \hat{p} = \frac{\hat{a} - \hat{a}^+}{2} \sqrt{\frac{2\hbar}{m\omega}} \\
|\alpha\rangle = \hat{D}(\alpha)|0\rangle & \Rightarrow \\
\hat{D}(\alpha) = \exp(\alpha\hat{a}^+ - \alpha^*\hat{a})
\end{cases}$$

$$\langle x \rangle = \int \langle \alpha | \hat{x} | \alpha \rangle d\alpha \quad \langle p \rangle = \int \langle \alpha | \hat{p} | \alpha \rangle d\alpha$$

$$\langle x \rangle = \int \langle 0 | \hat{D}^\dagger(\alpha) \hat{x} \hat{D}(\alpha) | 0 \rangle d\alpha = \frac{1}{2} \sqrt{\frac{2\hbar}{m\omega}} \int (\alpha + \alpha^*) d\alpha$$

$$\langle p \rangle = \frac{1}{2} \sqrt{\frac{2\hbar}{m\omega}} \int (\alpha - \alpha^*) d\alpha \quad \langle hx^2 \rangle =$$

$$\begin{aligned}
\langle \hat{x}^2 \rangle &= \frac{1}{2} \frac{\hbar}{m\omega} \int \langle 0 | \hat{D}^\dagger(\hat{a}^+ \hat{a}^+ + \hat{a}^+ \hat{a} + \hat{a} \hat{a}^+ + \hat{a} \hat{a}) \hat{D} | 0 \rangle d\alpha \\
&= \frac{1}{2} \frac{\hbar}{m\omega} \int (\langle 0 | \hat{D}^\dagger \hat{a}^+ \hat{a}^+ \hat{D} | 0 \rangle + \langle 0 | \hat{D}^\dagger \hat{a}^+ \hat{a} \hat{D} | 0 \rangle + \langle 0 | \hat{D}^\dagger \hat{a} \hat{a}^+ \hat{D} | 0 \rangle + \langle 0 | \hat{D}^\dagger \hat{a} \hat{a} \hat{D} | 0 \rangle) d\alpha
\end{aligned}$$

$$\begin{cases}
\langle 0 | \hat{D}^\dagger \hat{a}^+ \hat{a}^+ \hat{D} | 0 \rangle = \langle 0 | (\hat{a} \hat{D})^\dagger \hat{a}^+ \hat{D} | \alpha \rangle \\
\hat{a} \hat{D} | 0 \rangle = \hat{a} | \alpha \rangle = \alpha | \alpha \rangle
\end{cases} \Rightarrow \langle 0 | \hat{D}^\dagger \hat{a}^+ \hat{a}^+ \hat{D} | 0 \rangle = \alpha^* \alpha^* \langle \alpha | \alpha \rangle$$

其他三项有出现 $\hat{a}^+ | \alpha \rangle$ 不知道怎么处理，而且这个积分也不知道该怎么算。

两点分布: $P(x = k) = p^k(1-p)^{1-k}$, $k = 0, 1, 0 < p < 1$ $E(X) = p$,

$D(X) = p(1-p)$

伯努利分布: $P(x = k) = C_n^k p^k (1-p)^{n-k}$, $k = 0, 1, \dots, n$. $0 < p < 1$

$E(X) = np$, $D(X) = np(1-p)$. $X \sim B(n, p, k)$

泊松分布: $P(x = k) = \frac{\lambda^k}{k!} e^{-\lambda}$, $0 < p < 1$ $E(X) = \lambda$, $D(X) = p\lambda$

高斯分布: $P(x = k) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$, $0 < p < 1$ $E(X) = \mu$, $D(X) = \sigma^2$

Figure 1: single photon detector

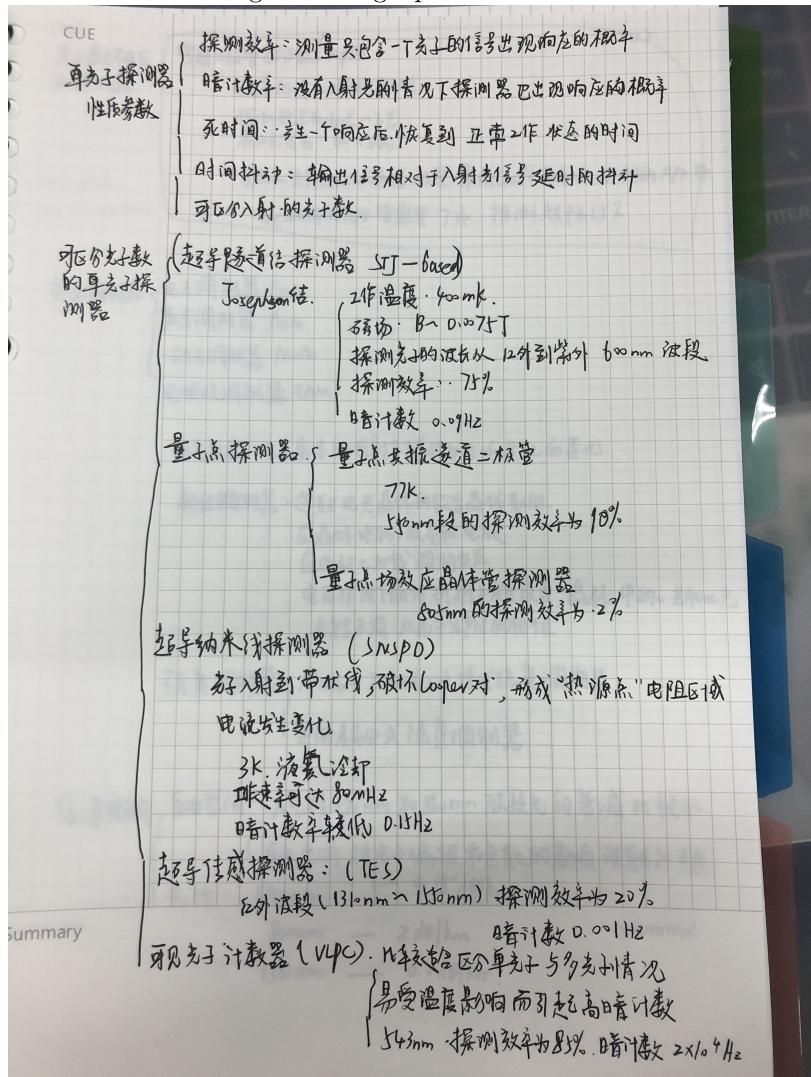


Figure 2: parameter down conversion

CUE	单光子源	300k	300-750nm	3nm	0.04	0.09
非线性单光子源	NV源	300k	600-800nm	nm	0.022	0.07
量子点 (InS)	300k	500-900nm	15nm	0.05	0.003	γ
单离子	≈ 0	原子谱线	5MHz	0.08	0.015	
单原子	≈ 0	原子谱线	10MHz	0.05	0.06	
发射效率 在控制指令下实际产生单光子的比例						
二阶相关函数 发射出的光场差接近单光子的程度						
单光子源：利用参量下转换方法得到一对偏振纠缠的单光子对						
参量下转换：一个光子在穿过多层时，会以很小的概率分裂为两个光子。 满足能量守恒和动量守恒						
一束强泵浦光与非线性晶体相互作用时，一个泵浦光子可以转换为一对低频光子 {信号光子，闲置光子}						
I类相位匹配：下转换的光子偏振方向一致，与泵浦光的偏振方向垂直，可以产生，时间，波长上的纠缠。						
II类相位匹配：下转换光子的偏振方向相互垂直，可以产生，时间，波长，偏振纠缠。						
可数源：激光场通常被描述为相干态，其光子数满足泊松分布。经过衰减后仍是泊松分布。 $p(n) = e^{-\mu} \frac{\mu^n}{n!}$						
summary						

Figure 3: modulator

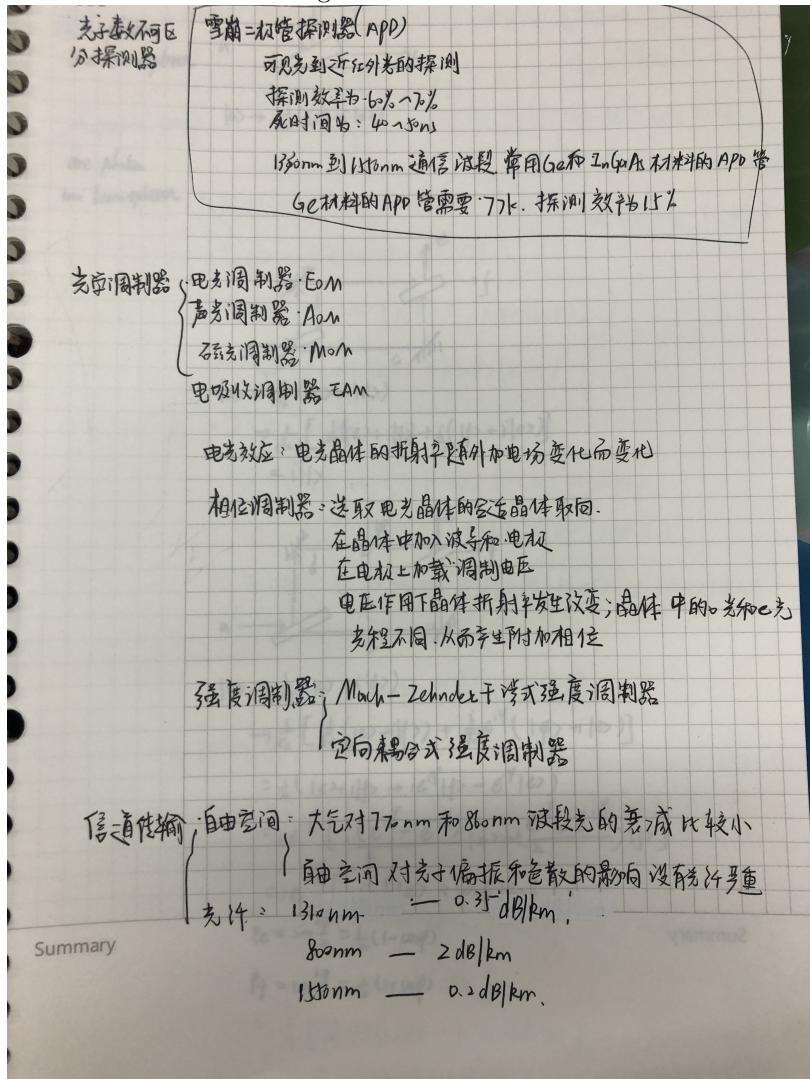


Figure 4: discrete source

