其中蓝色部分为变量。其余参数均为确定值。

Alice 发送强度为μ，ν，0的脉冲，概率分别为p_μ，p_ν，p_0， $p_\mu+p_\nu+p_0=1$。 Alice 和 Bob 选基概率相等，选 Z 基的概率为 0.5，Z 基下安全密钥长度为：

$$l_z \geq p_\mu * s_{Z,1}[1-H(e_1^X)] - n_{Z,\mu} f_{EC} H(E_\mu^Z)$$

其中，$H(x)=-x\log_2 x-(1-x)\log_2(1-x)$是二元香农熵函数。$s_{Z,1}$为强度为μ时单光子的总计数；$e_{Z,1}^p$表示 Z 基下单光子的相位误码；$\lambda_{EC}$表示纠错过程泄露的信息量。

$$s_{Z,1}=\frac{\mu^2 e^{-\mu}}{\mu\nu-\nu^2}\left(e^\nu \frac{\boldsymbol{n_{Z,\nu}}}{p_\nu}-e^\mu \frac{\nu^2}{\mu^2}\frac{\boldsymbol{n_{Z,\mu}}}{p_\mu}-\frac{\mu^2-\nu^2}{\mu^2}\frac{\boldsymbol{n_{Z,0}}}{p_0}\right)$$

Z 基下单光子的相位误码率$e_{Z,1}^p$需要由 X 基下单光子比特误码率$e_{X,1}^b$来估计。

X 基下

$$s_{X,1}=\frac{\mu^2 e^{-\mu}}{\mu\nu-\nu^2}\left(e^\nu \frac{\boldsymbol{n_{X,\nu}}}{p_\nu}-e^\mu \frac{\nu^2}{\mu^2}\frac{\boldsymbol{n_{X,\mu}}}{p_\mu}-\frac{\mu^2-\nu^2}{\mu^2}\frac{\boldsymbol{n_{X,0}}}{p_0}\right)$$

X 基下单光子比特错误数

$$e_1^X \leq \frac{1}{\nu * s_{X,1}}\left(e^\nu \frac{\boldsymbol{m_{X,\nu}}}{p_\nu}-\frac{\boldsymbol{m_{X,0}}}{p_0}\right)$$

假设$\boldsymbol{n_{Z,\mu}=n_{X,\mu}}$，那么有$e_1^X=e_1^Z=e_1$，$E_\mu^Z=E_\mu^X=E_\mu$

总密钥长度为

$$\begin{aligned} l = l_z + l_x &= p_\mu(s_{Z,1}+s_{X,1})[1-H(e_1^X)] - (n_{Z,\mu}+n_{X,\mu}) f_{EC} H(E_\mu^Z) \\ &= p_\mu \frac{\mu^2 e^{-\mu}}{\mu\nu-\nu^2}\left(e^\nu \frac{\boldsymbol{n_\nu}}{p_\nu}-e^\mu \frac{\nu^2}{\mu^2}\frac{\boldsymbol{n_\mu}}{p_\mu}-\frac{\mu^2-\nu^2}{\mu^2}\frac{\boldsymbol{n_0}}{p_0}\right)[1-H(e_1^X)] - n_\mu f_{EC} H(E_\mu^Z) \end{aligned}$$

结论：

最终密钥长度

$$l = p_\mu s_1[1-H(e_1)] - n_{leak}^\mu$$

$$s_1 = \frac{\mu^2 e^{-\mu}}{\mu\nu-\nu^2}\left(e^\nu \frac{\boldsymbol{n_\nu}}{p_\nu}-e^\mu \frac{\nu^2}{\mu^2}\frac{\boldsymbol{n_\mu}}{p_\mu}-\frac{\mu^2-\nu^2}{\mu^2}\frac{\boldsymbol{n_0}}{p_0}\right)$$

$$e_1 = \frac{1}{\nu * s_1}\left(e^\nu \frac{\boldsymbol{m_\nu}}{p_\nu}-\frac{\boldsymbol{m_0}}{p_0}\right)$$

更一般的形式

$$l = p_1^\mu s_1[1-H(e_1)] - n_{leak}^\mu$$

$$s_1 = \frac{\tau_1 \mu}{\mu\nu-\nu^2}\left(e^\nu \frac{\boldsymbol{n_\nu}}{p_\nu}-e^\mu \frac{\nu^2}{\mu^2}\frac{\boldsymbol{n_\mu}}{p_\mu}-\frac{\mu^2-\nu^2}{\mu^2}\frac{\boldsymbol{n_0}}{p_0}\right)$$

$$p_1^\mu = \frac{p_\mu e^{-\mu}\mu}{\tau_1}, \tau_1 = p_\mu e^{-\mu}\mu + p_\nu e^{-\nu}\nu$$

$$e_1 = \frac{\tau_1}{\nu * s_1}\left(e^\nu \frac{\boldsymbol{m_\nu}}{p_\nu}-\frac{\boldsymbol{m_0}}{p_0}\right)$$