第十二届全国量子光学会议
2006年8月21日 · 江西南昌

基于连续变量纠缠的安全通信研究

报告人：何广强　曾贵华

上海交通大学电子工程系
区域光纤通信网与新型光通信系统国家重点实验室

gqhe@sjtu.edu.cn or laser_gqhe@hotmail.com

连续变量量子安全通信研究

1 连续变量量子信息简介

- 简介

  单模电磁场的一对正交共轭变量为：

$$X_1 = \frac{1}{2}(\hat{a} + \hat{a}^\dagger), X_2 = \frac{1}{2i}(\hat{a} - \hat{a}^\dagger). \tag{1}$$

  满足测不准原理

$$\Delta X_1 \Delta X_2 \geq \frac{1}{4} \tag{2}$$

  X_1和X_2不能同时被精确测量，利用X_1和X_2作为信号载波实现共轭编码，构成连续变量量子密码的物理基础。

- 优势

  ⋆ 容易制备相干态；

  ⋆ 零差或外差检测相对容易；

  ⋆ 容易调制相位和振幅；

  ⋆ 通信速率高。

2 基于连续变量EPR纠缠对的直接安全通信

2.1. 协议描述

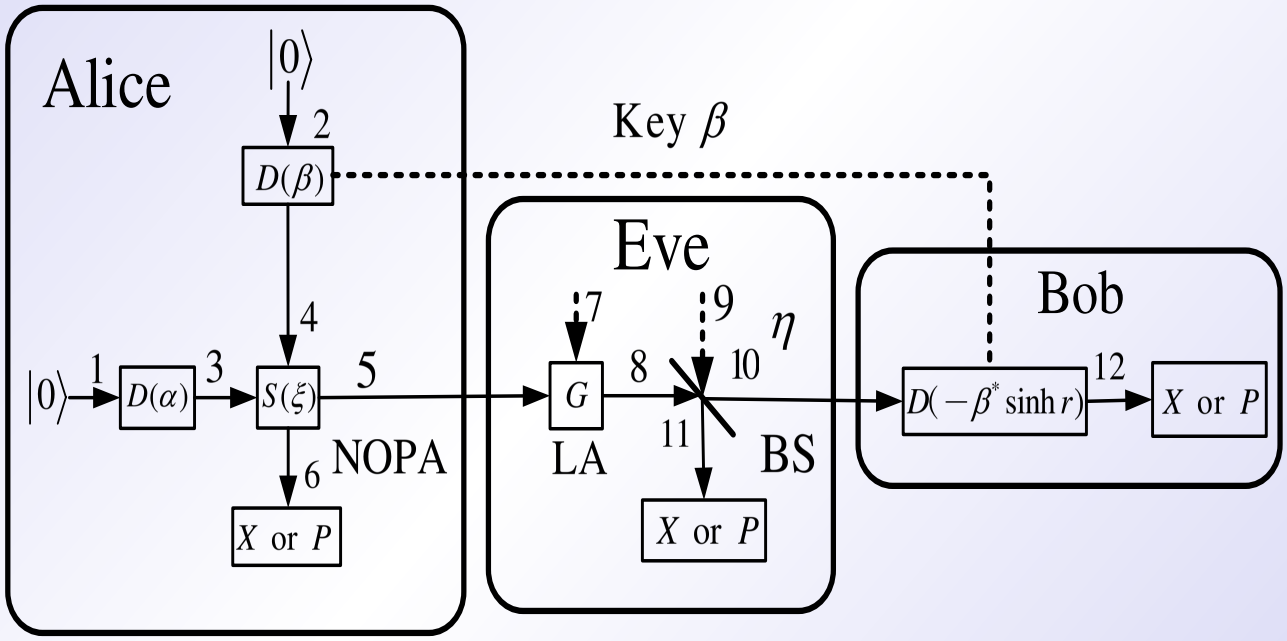

图1. 基于连续变量EPR关联对的量子安全通信方案框图

★ He-Guangqiang, Zhu-Jun, Zeng-Guihua, Physical Review A (2006) **73**, 012314

2.2. 引入纠缠参数F

2.2.1. 双模压缩变换

$$
\begin{aligned}
X_{out1} &= X_{in1}\cosh(r) + X_{in2}\sinh(r),\\
P_{out1} &= P_{in1}\cosh(r) - P_{in2}\sinh(r),\\
X_{out2} &= X_{in2}\cosh(r) + X_{in1}\sinh(r),\\
P_{out2} &= P_{in2}\cosh(r) - P_{in1}\sinh(r).
\end{aligned}
\tag{3}
$$

2.2.2. 纠缠参数F

$$
F = \langle(\Delta(X_{out1} - k_1 X_{out2}))^2\rangle_{min}\langle(\Delta(P_{out1} + k_2 P_{out2}))^2\rangle_{min} \tag{4}
$$

当两模具有理想关联时，$F = 0$;当两模无关时，$F \longrightarrow +\infty$。纠缠参数$F$反映了EPR关联对的完善程度，因此可以判断窃听者对量子信道的破坏程度。

2.3. 安全性分析

2.3.1. 秘密信息速率(QKD)

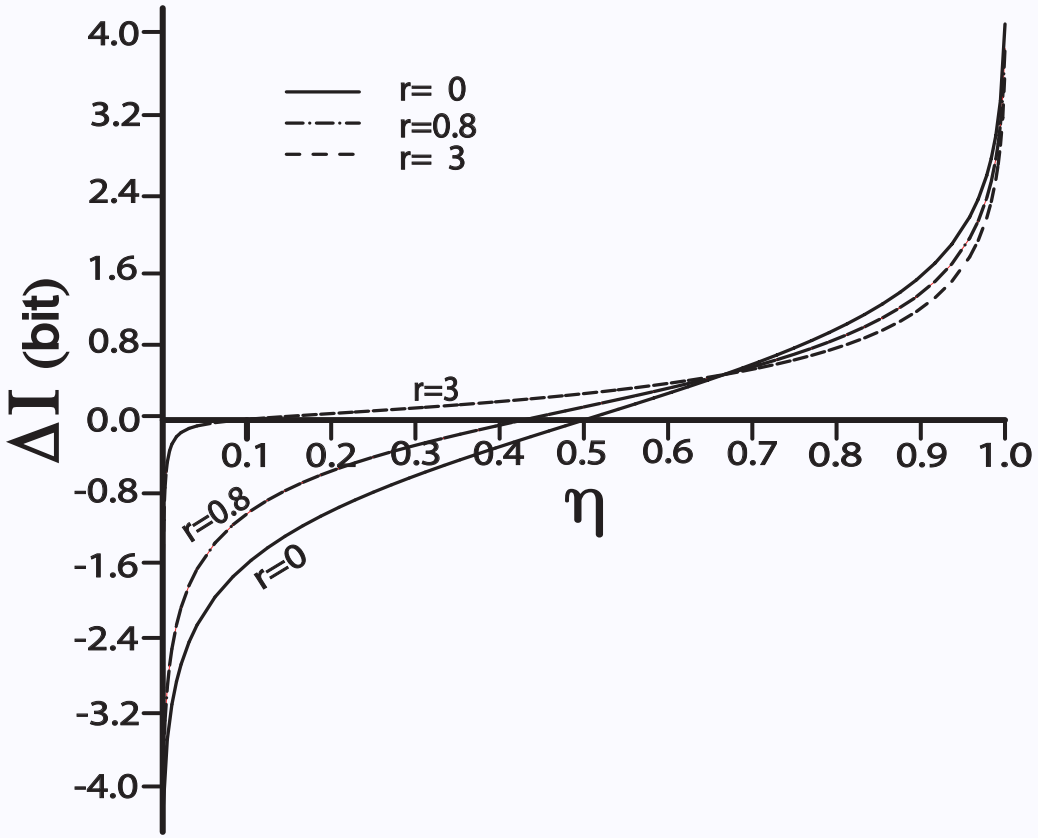

图2. ΔI与η之间的关系。$(\Sigma = 10, \sigma = 0, G = 1)$.

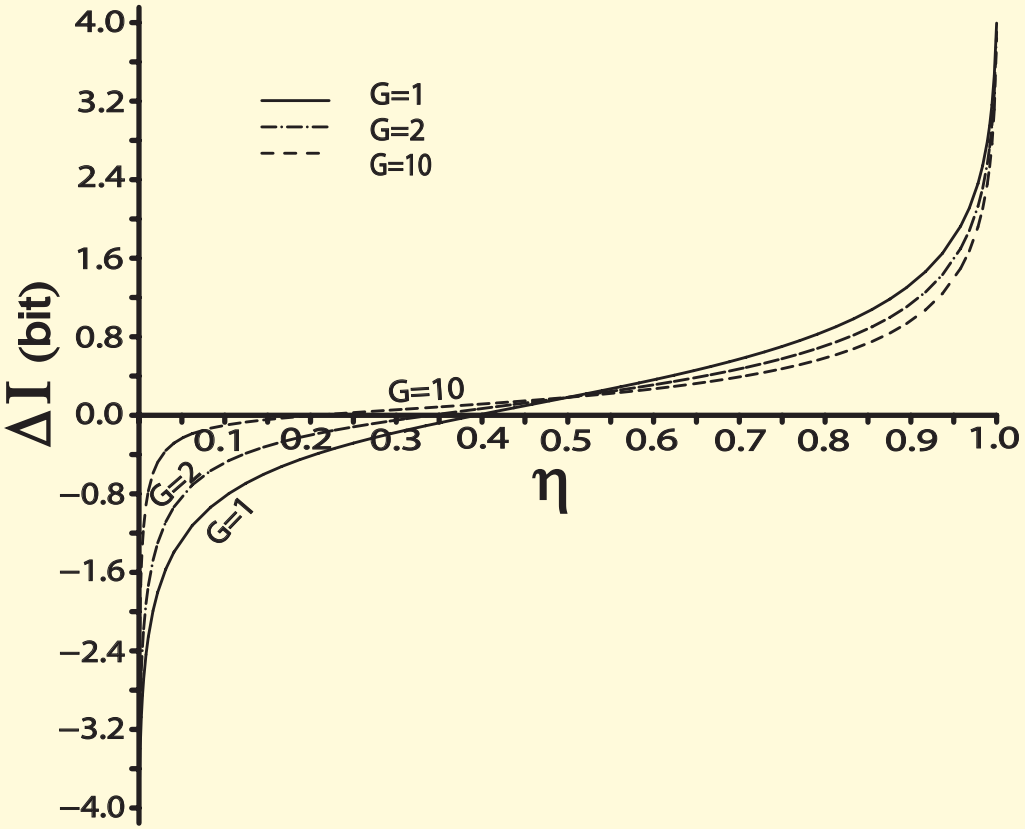

图3. ΔI与η之间的关系, $(\Sigma = 10, \sigma = 0, r = 1)$.

2.3.2. $I_{max}(\alpha,\epsilon)$(QE)

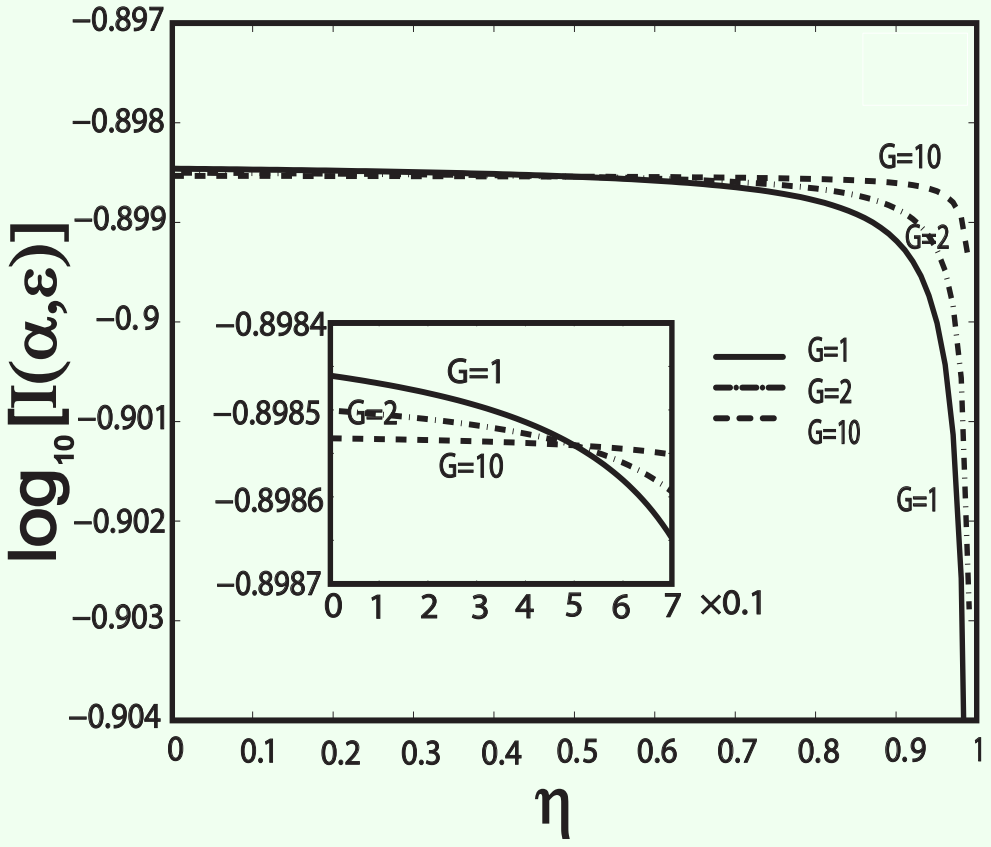

图4. $I(\alpha,\epsilon)$与η之间的关系，$\Sigma=10,\sigma=30$，$r=1$

2.3.3. 窃听检测

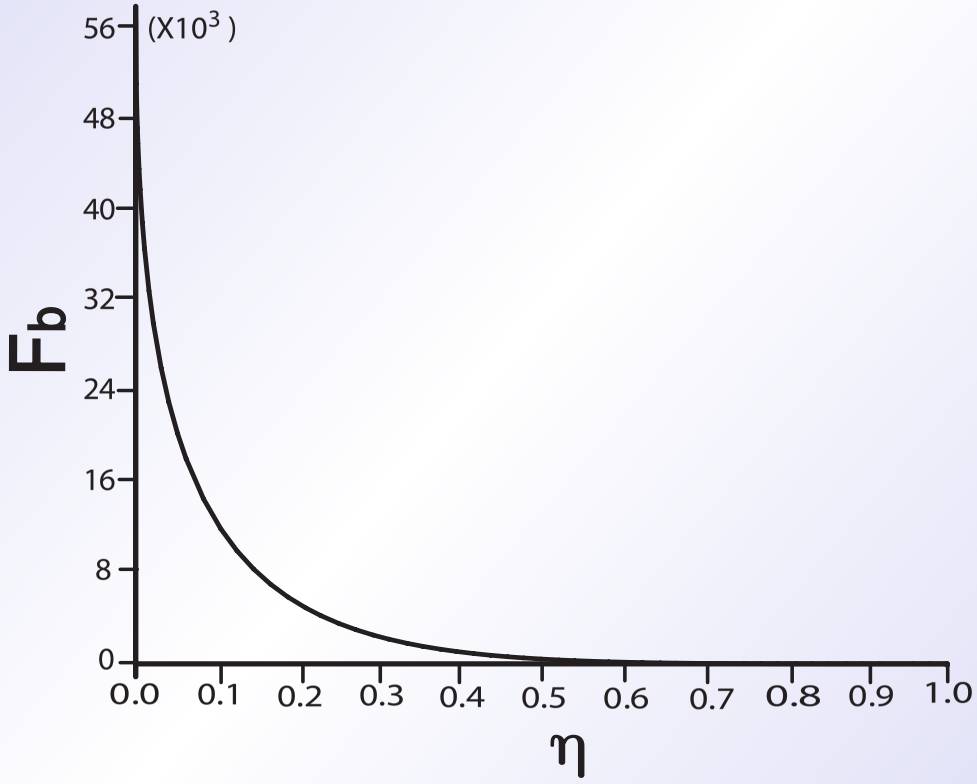

图5. 量子密钥分发过程中F_b与η之间的关系，$\Sigma = 10, \sigma = 0, G = 1, r = 1$。

2.3.4. ΔI与F_b之间的关系

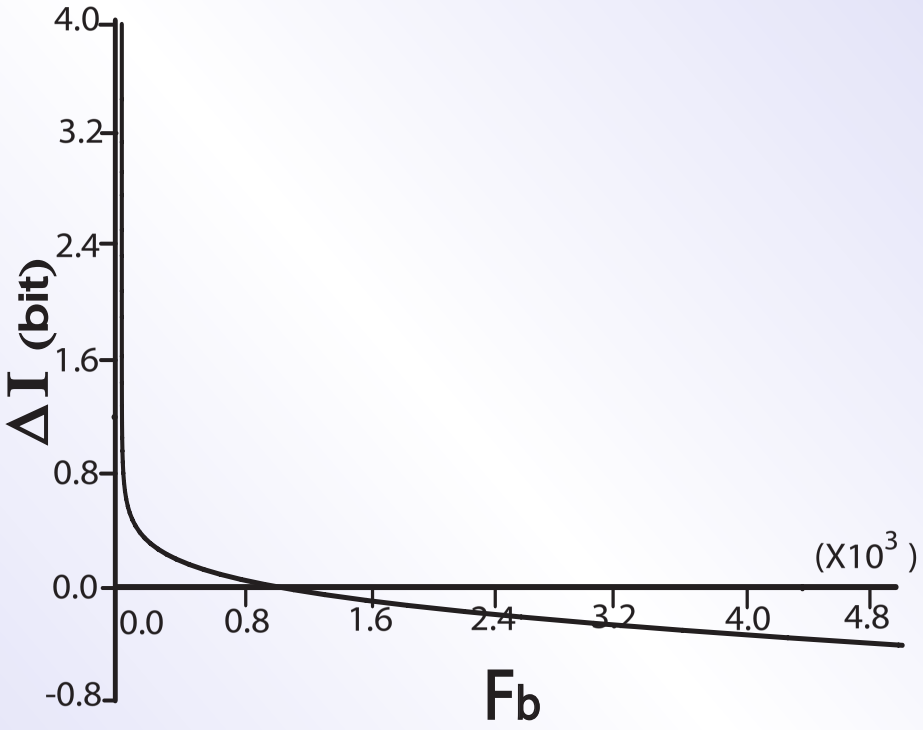

图6. 量子密钥分发过程中ΔI与F_b之间的关系，$\Sigma = 10, \sigma = 0, G = 1, r = 1$。

★ ΔI随着F_b的增大急剧减小。当F_b达到最小值时，ΔI达到最大值。例如当$\Sigma = 10, \sigma = 0, G = 1, r = 1, F_{bmin} = 3.248 \times 10^{-2} < \frac{1}{16}, \Delta I_{max} = 3.995$ 比特。

2.4. 小结

优点

1 该方案可同时实现量子密钥分发和量子加密，可以实现量子安全通信；

2 通信速率高，容易实验实现；

4 纠缠参数F能有效阻止光束分离攻击。

缺点

★ 对信道损耗比较敏感。

3 基于连续变量EPR纠缠对的确定性QKD

3.1. 协议描述

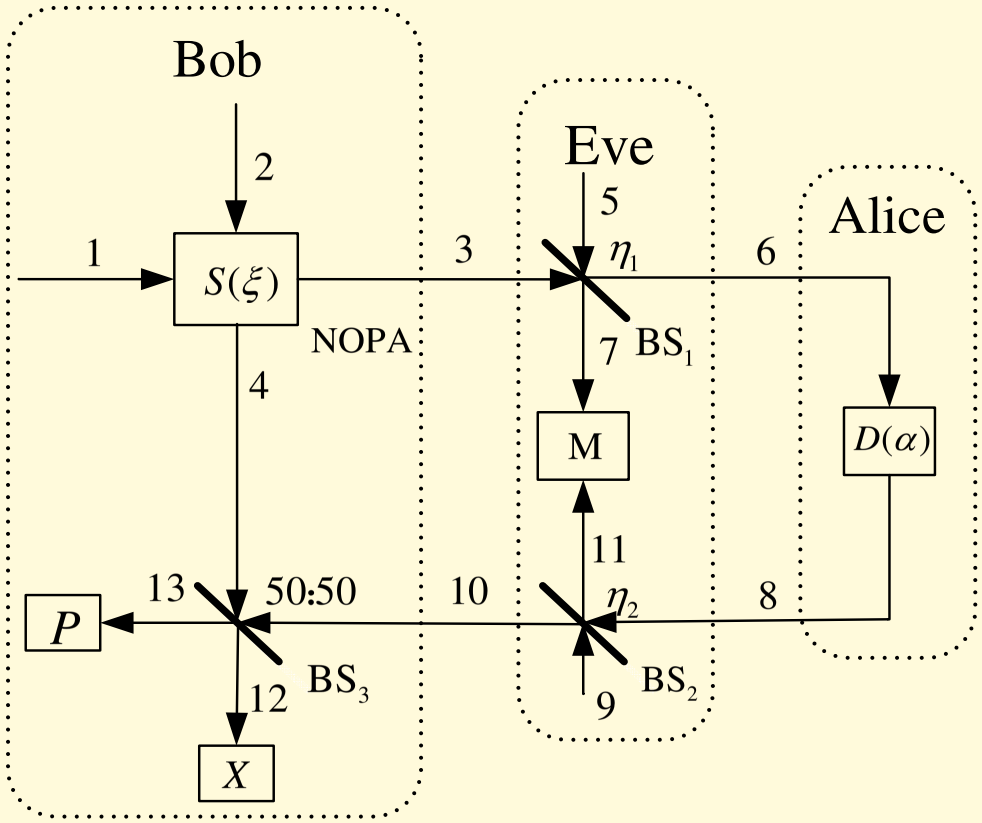

图7. 基于高斯调制连续变量EPR关联对的确定性量子密钥分发方案框图

3.2. 安全性分析

3.2.1. 秘密信息速率ΔI

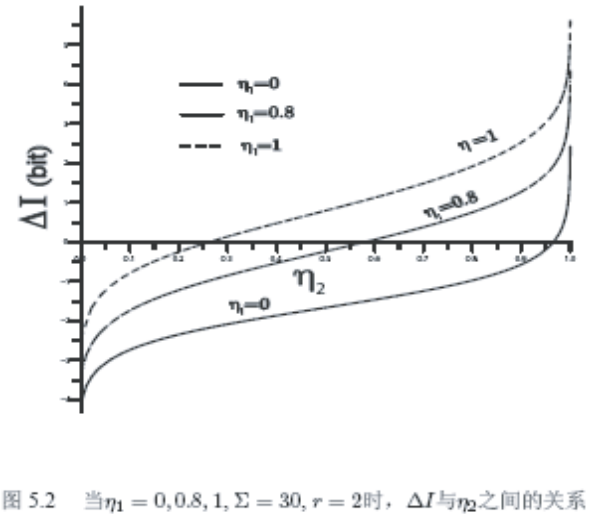

图 5.2 当$\eta_1 = 0, 0.8, 1, \Sigma = 30, r = 2$时，$\Delta I$与$\eta_2$之间的关系

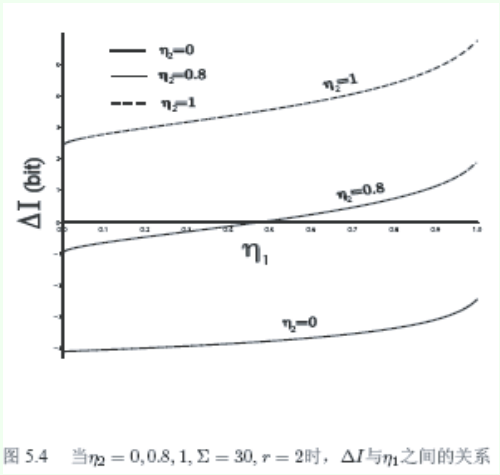

图 5.4 当$\eta_2 = 0, 0.8, 1, \Sigma = 30, r = 2$时，$\Delta I$与$\eta_1$之间的关系

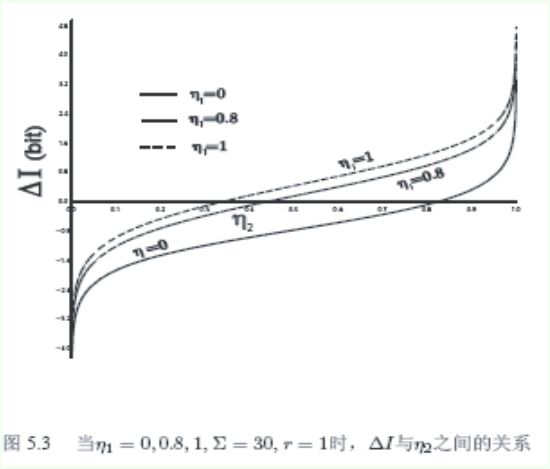

图 5.3 当$\eta_1 = 0, 0.8, 1, \Sigma = 30, r = 1$时，$\Delta I$与$\eta_2$之间的关系

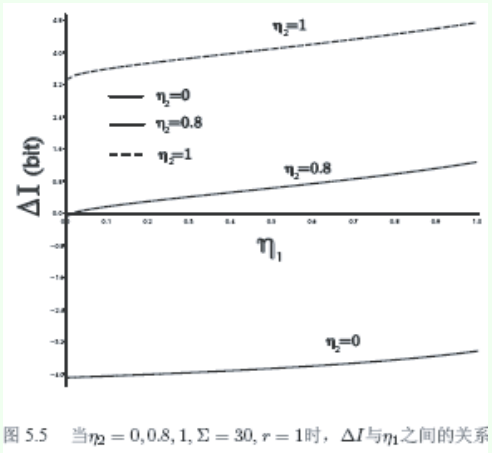

图 5.5 当$\eta_2 = 0, 0.8, 1, \Sigma = 30, r = 1$时，$\Delta I$与$\eta_1$之间的关系

图8. ΔI与η_1, η_2之间的关系

3.2.2. 窃听检测

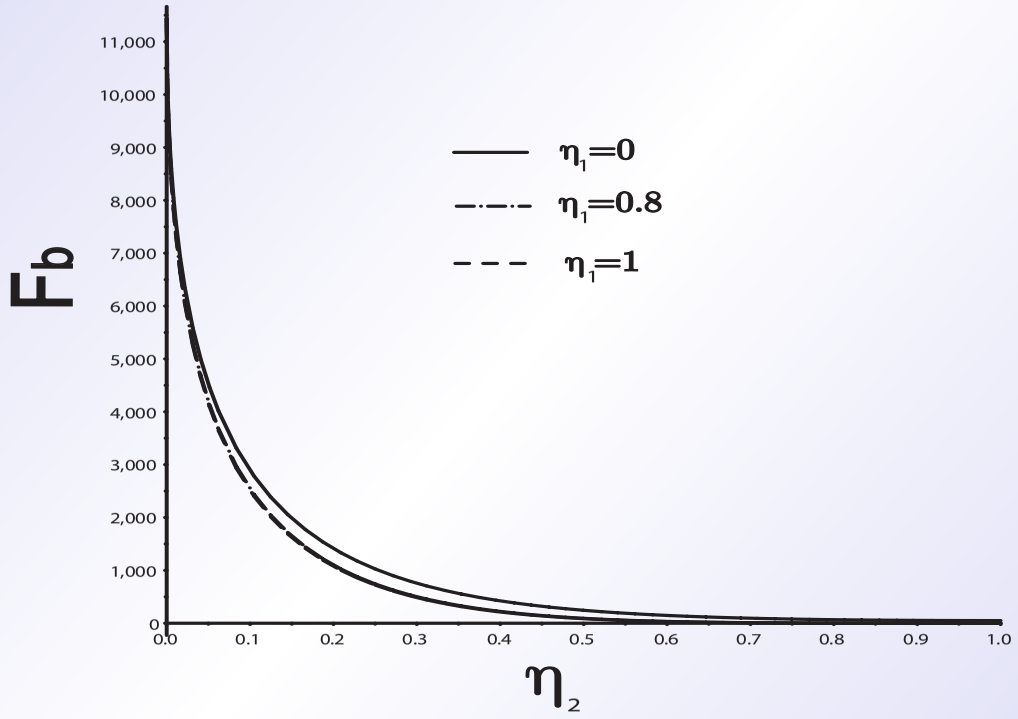

图9. 当$\eta_1 = 0, 0.8, 1, \Sigma = 10, r = 2$时，$F_b$与$\eta_2$之间的关系

3.2.3. ΔI与F之间的关系

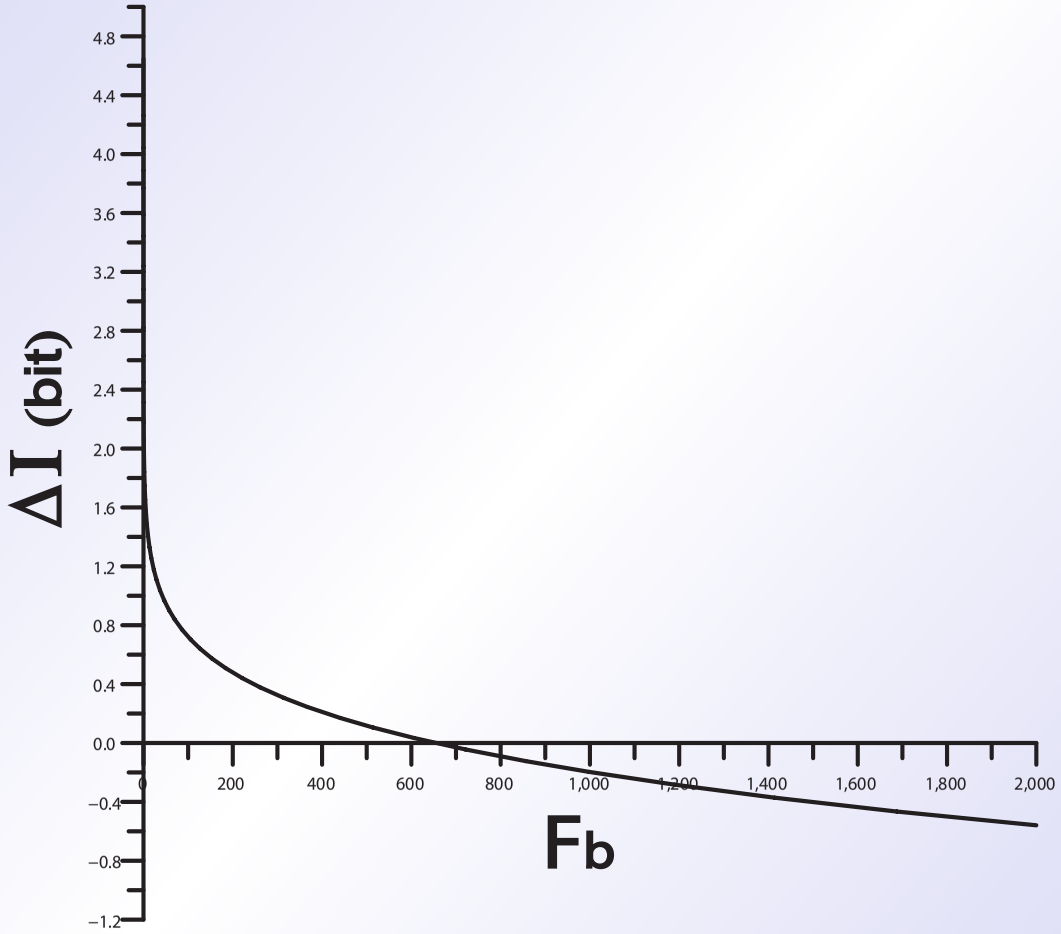

图10. 当$\eta_1 = 1, \Sigma = 10, r = 2$时，$\Delta I$与$F_b$之间的关系

3.3. 小结

优点

1 通信速率随着压缩参数的增大而提高；

2 通信速率高，容易实验实现；

3 不需要单独控制模式，容易实现；

4 纠缠参数F能有效阻止光束分离攻击。

缺点

1 对信道损耗比较敏感。

2 由于采用two-way传输，限制了传输距离。

谢谢!!

地址：上海市东川路 800 号交通大学电子工程系电信楼群 5 号楼 225 房间（200240）

Email: gqhe@sjtu.edu.cn or laser_gqhe@hotmail.com

电话：021－34204361（实验室）