Analysis of Reconciliation Protocol in Quantum Key Distribution

Xin-Xing Huo [1, 2], Li Yu [1, 2], Zhi-Xin Lu [1, 2], Bing-Can Liu [3]

1.School of Science，Beijing University Of Posts and Telecommunications，Beijing 100876，China

2.Key Laboratory of Information Photonics and Optical Communications (BUPT),Ministry of Education，Beijing 100876，China

3. Department of Fundamental Courses, Academy of Armored Force Engineering, Beijing 100072, China

e-mail xinxing188@sohu.com

Abstract: In this report, we derive an expression of the secret key rate in Post Selection with detection noise. We discuss the security condition as well as the security key rate of Reverse Reconciliation (RR) and Post Selection (PS) in a lossy and noisy channel. We show that with a little loss, the tolerance to noise of PS is better than that of RR. With the detection noise, it is more efficient to apply RR protocol.

Keywords: quantum key; continuous variable; noise; reverses reconciliation; post selection.

连续变量量子密钥协调协议分析

霍新星 [1,2]，于丽 [1,2]，逯志欣 [1,2]，刘炳灿 [3]

1、北京邮电大学理学院 北京 100876

2、北京邮电大学信息光子学与光通信教育部重点实验室 北京 100876

3、装甲兵工程学院基础部，北京 100072

E-mail xinxing188@sohu.com

【摘要】本文给出了在探测噪声下后向选择协议可以得到的密钥量的表达式，分析比较了在逆向协调和后向选择协调下，信道衰减及过噪声对量子密钥分配的影响，给出了各种噪声情况下这两种主要协议性能的优劣。研究表明：信道传输率较大时，后向选择协议性能优于逆向协调，且后向选择协议对过噪声的容忍度要好于逆向协调；在探测噪声下，逆向协调的性能受探测噪声的影响较小，优于后向选择协议。

【关键词】量子密钥；连续变量；噪声；逆向协调；后向选择

1 引言

连续变量量子密钥分配是当前量子信息领域研究热点之一。在相干态量子密钥分发提出的初期阶段，采用的协调方法是正向协调(Direct Reconciliation, DR)[1]，该协调方法下当信道衰减大于3dB时密钥将不再安全。为了突破了3dB衰减的限制，Grosshans等人提出了逆向协调协议(Reverse Reconciliation，RR)[2]，同时， Ralph等把另外一种可以突破3dB限制的“后向选择”（Post selection，PS）校验协议引入到连续变量校验协议中[3]。对于RR，它使用安全判据 $I_{BA} > I_{BE}$，当窃听者得到的信息量大于接收端得到的信息量时，系统密钥不再安全；而对于PS，当 $I_{AB} < \max(I_{AE}, I_{BE})$ 时，仍可以得到安全的密钥，它很好的解决了 $I_{BA} < I_{BE}$ 时无法得到安全密钥的问题，但是，Ralph等人最初提出的协议只考虑了忽略噪声的理想情况，而后来的Thomas Symul等人也只是研究了过噪声对后向选择协议的影响[4]。

本文对逆向协调和后向选择这两种可以突破 3dB限制的协议进行了研究；分析了在衰减信道中窃听者使用分束攻击时的情况，以及此种噪声影响下这两种协议的性能，并做了优劣比较。最后，引入了探测器的探测效率等效噪声和电子噪声，并分析了它们在这两种协调方式下对连续变量量子密钥分发的影响。

2 噪声对连续变量密钥分配的影响

在相干态的量子密钥分配方案中，系统噪声主要有四种：真空噪声、信道噪声、探测器的电子噪声和探测噪声[5]。真空噪声 N_0 是相干态固有噪声，表示真

资助项目：北京市教委共建项目（xk100130937）

空态的量子起伏，不会随外界的变化而变化。信道噪声包括信道衰减而引入的等效量子噪声和过噪声（调制过程不理想引入的噪声和光源的相位噪声）。信道噪声可以表示为 $\chi=(1-G)/G+\varepsilon$，其中 G 为信道传输率，$(1-G)/G$ 为信道衰减等效到输入端的等效量子噪声，ε 为过噪声，单位均为 N_0。电子噪声是由探测器电路产生，与探测电路的设计方案、光电二极管等器件选用有关，记作 N_{el}。

2.1 考虑信道衰减和信道过噪声

首先我们考虑信道存在衰减时两种协议的性能，对于使用逆向协调的连续变量密钥分配，其密钥量为[5]：

$$\begin{aligned}\Delta I_{RR} &= I_{BA}-I_{BE}\\ &=-(1/2)\log_2[G^2(1+\chi)(V^{-1}+\chi)]\end{aligned} \tag{1}$$

对于后向选择协调，发送端 A 发送方差为 V_A 的高斯信号 S_A，接收端 B 接收到信号 m_B，则[3,4]：

$$I_{AB}=1+P_e\log_2 P_e+(1-P_e)\log_2(1-P_e) \tag{2}$$

$$\begin{aligned}I_E=&\frac{1}{2}(1+\sqrt{1-f^2})\log_2(1+\sqrt{1-f^2})\cdot\\ &\frac{1}{2}(1-\sqrt{1-f^2})\log_2(1-\sqrt{1-f^2})\end{aligned} \tag{3}$$

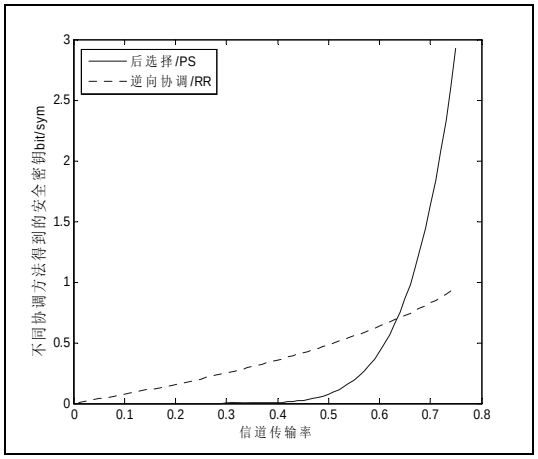

Figure1. curve of key rate generated with different Transmission

图 1. 不同协调方法下密钥量与信道传输率图

我们可以得到图 1 所示的结果，首先逆向协调和后向选择都可以很好地突破正向协调的 3dB 极限，而且通过计算可知，这两种协调方法得到的密钥量始终大于正向协调得到的密钥量。其次，在信道传输率小于 0.65 左右，后向选择得到的密钥量要小于逆向协调得到的密钥量，当信道传输率较大时，逆向协调获得的密钥量远不如后向选择，当信道传输率很高时，PS 可以得到的密钥量迅速增大，此时 PS 较 RR 有明显的优势。

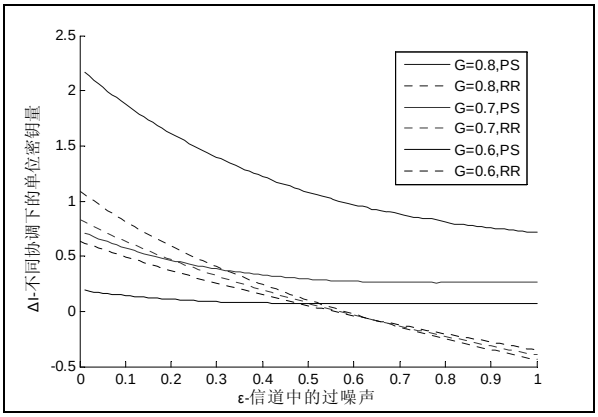

Figure 2. The security key rate with the effect of noise

图 2. 不同协调方法下密钥量与过噪声的关系

设信道传输率不变，分析信道过噪声对两种协议可以获取的密钥量的影响，我们分别考虑信道传输率为 0.6、0.7 和 0.8 这三种情况，如图 2 所示。对于逆向协调，只有当信道噪声小于 0.6 时，才能获取安全的密钥，当 $\varepsilon>0.6$ 时，密钥分发不再安全。对于后向选择，无论信道噪声有多大，总是存在安全的区域使得 $\Delta I>0$，在大噪声信道中，后向选择协调的性能要优于逆向协调。

2.2 考虑零拍探测的探测效率和电子噪声

我们引入零拍探测的探测效率 η 和探测器的电子噪声 N_{el}，并且令 $N_{el}=\alpha N_0$，我们考虑逆向协调的第一种假设“realistic assumption”[4]，则表达式(1)变为：

$$\Delta I_{RR}=\frac{1}{2}\log_2\left[\frac{1+G(\frac{1-\eta}{\eta}+\alpha)(\chi+V^{-1})}{G^2(1+\chi+\frac{1-\eta}{\eta G}+\frac{\alpha}{\eta G})(\chi+V^{-1})}\right] \tag{4}$$

在后向选择协调协议中，发射端 A 发送的是均值为 0 方差为 V_A 的高斯信号，接收端 B 接收到的也是高斯信号，我们假设对任一发射信号 S_A，接收端的接收信号为 m_B，则有

978-1-935068-01-3 © 2009 SciRes.

$$E(m_B) = E(\sqrt{\eta G} S_A) = \sqrt{\eta G} S_A \quad (5a)$$

$$D(m_B) = \eta(1+\varepsilon) + \alpha \quad (5b)$$

我们将探测的衰减等效为噪声$\frac{1-\eta}{\eta}$，则以上两式可重写为：

$$E'(m_B) = E(\sqrt{G} S_A) = \sqrt{G} S_A \quad (6a)$$

$$D'(m_B) = (1+\varepsilon) + \alpha + \frac{1-\eta}{\eta} \quad (6b)$$

令$\alpha + \frac{1-\eta}{\eta} = \beta$，我们统称之为探测器噪声，(5)式中相同。

令$(1+\varepsilon) + \alpha + \frac{1-\eta}{\eta} = \sigma^2$，可以得到 A 发送$S_A$，B 接收到$m_B$的概率为：

$$p(m_B \mid S_A) = \frac{\exp[-(m_B - \sqrt{G} S_A)^2 / 2\sigma^2]}{\sqrt{2\pi}\sigma} \quad (7)$$

$$P_e = \frac{1}{1 + e^{\frac{2\sqrt{G}|m_B S_A|}{\sigma^2}}} \quad (8)$$

将上式代入(2)式和(3)式，我们可以得到后向选择法的单位密钥量

$$R = \int_S ds \cdot [I_{AB} - I_E] \quad (9)$$

其中 S 表示后向选择法的安全区域，安全区域的分布服从

$$p(m_B, S_A) = \frac{1}{\sqrt{2\pi} d} e^{-\frac{S_A^2}{2d^2}} p(m_B \mid S_A) \quad (10)$$

其中d是服从高斯分布的发射信号的标准差，同过合理的选择d的大小，我们可以使几乎所有的S_A的取值都落在安全区域，使得可获取的安全密钥量尽量大。

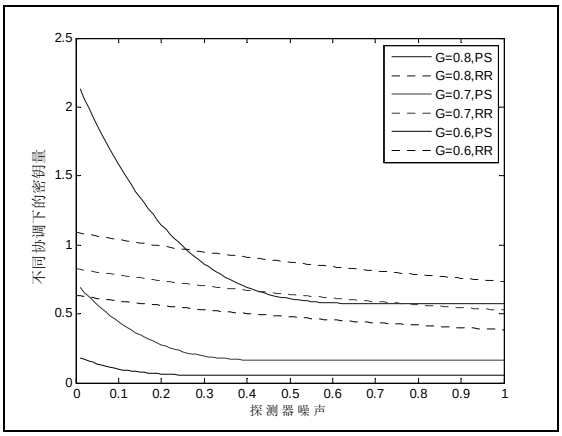

Figure 3. The security key rate with the effect of detection noise

图 3 不同协调协议下密钥量与探测器噪声的关系

目前零拍探测器的探测效率一般在 60%-80%[6]，总的探测噪声基本可以控制在 1 N_0 以内。文献 5 中的探测器探测效率满足$\frac{1-\eta}{\eta} = 0.27N_0$，电子噪声$N_{el} = 0.33N_0$，其总的探测噪声$\beta = 0.6N_0$；文献 6 中的探测效率为 53%,电子噪声控制在 0.025 N_0 左右，其总的探侧噪声约为 0.9 N_0。因此我们的分析只考虑了探测噪声在 1 N_0 以内的情况。

在我们的分析中，我们采用 G=0.8，0.7，0.6 此时 d 的最优值为约 3.2，2.6，2.2。如图 3 所示，后向选择协调获取的密钥量对探测起噪声非常敏感，其随着探测器噪声的增加迅速减小，当噪声增加到一定程度时，密钥量的减少趋缓；而逆向协调获取的密钥量受探测噪声的影响较小。在探测噪声较大时，后向选择协调的性能要劣于逆向协调，以 G=0.8 为例，当探测噪声大于 0.26 时，后向选择获取的密钥小于逆向协调。另外，在探测噪声存在的情况下，两种协议下的密钥分发都是安全的，即探测噪声只影响密钥量的大小。

3 结论

本文分析了逆向协调和后向选择下信道衰减及过噪声对密钥分发的影响，引入探测器的噪声并分析了其对密钥分配量的影响，比较了在各种噪声情况下两种协议的优劣。在低噪声高损耗信道中，RR 的性能要优于 PS；在大噪声信道中，PS 的性能要优于 RR；探测器噪声对两种主要的协调协议，尤其是后向选择下的密钥量影响较大，为了提高可获取的密钥量，进一步提高探测的探测效率、减小探测器的电子噪声是关键的因素之一。密钥分发过程中可以根据实际系统

的传输率、过噪声及探测器性能选择使用合适的协调协议，以期获得较大的密钥量。

References (参考文献)

[1] Grosshans F, Grangier P. Continuous Variable Quantum Cryptography Using Coherent States[J]. Phys.Rev.Lett, 2002,88:057902.

[2] Grosshans F, Grangier P. Reverse reconciliation protocols for quantum cryptography with continuous variables[OL]. arXiv:quant-ph/0204127, v1 22 Apr 2002

[3] Ch.Silberhorn, T.C.Ralph. Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit[J]. Phys.Rev.Lett, 2002,89:167901

[4] Symul T, Alton D J, Assad S M, et al. Experimental Demonstration of Post-Selection based Continuous Variable Quantum Key Distribution in the Presence of Gaussian Noise[J]. Phys.Rev.A, 2007,76:030303

[5] Grosshans F，Van Assche G，Wenger J，et al. Quantum key distribution using gaussian-modulated coherent states[J]. Nature, 2003,421:238～241

[6] Huang Lei-Lei, Qi Bing,, QianLi, et al. Continuous-Variables Quantum Key Distribution over Standard Telecom Fiber[OL]. http://arxiv.org/ftp/quant-ph/0611120 v1 10Nov2006

978-1-935068-01-3 © 2009 SciRes.