Excess Noise Analysis of Continuous Variable Quantum Key Distribution

Jian-Gui Lin [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

1. e-mail linjiangui83@126.com

Abstract: Excess noise will seriously affect the security of the quantum key in a reverse reconciliation coherent-state quantum key distribution system. Theoretical analysis of the excess noise in Alice's system, excess noise in channel and excess noise in Bob's homodyne detector are presented. And the bound of the excess noise in Alice, channel and Bob are also analyzed in the condition of ensuring the security of the quantum key. The results shows that the channel excess noise has the most serious impact to the security of the quantum key.

Keywords: quantum telecommunication; continuous variable quantum key distribution; theoretical analysis ; excess noise; reverse reconciliation

额外噪声对连续变量量子密钥安全性影响理论研究

林建桂 [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

1. E-mail linjiangui83@126.com

【摘要】在逆向协调的连续变量量子密钥分发系统中，额外噪声对密钥安全性有很大影响。本文从理论上分析了当窃听者采用个体攻击和集体攻击时，发送端额外噪声、信道额外噪声和探测器额外噪声对密钥安全性的影响，以及为保证量子密钥的安全性各部分额外噪声需满足的条件。分析得出密钥安全性对信道额外噪声最敏感，其次是发送端额外噪声，最后是探测器额外噪声。

【关键词】量子通信；连续变量量子密钥分发；理论分析；额外噪声；逆向协调

1 引言

连续变量量子密钥分发由于其光源实现简单、码率高等方面的优点，逐渐成为了量子通信领域的一个研究热点。在基于相干态的连续变量量子密钥分发系统中[1][2][3][4]，量子密钥分发过程包括两个阶段，第一阶段是量子通信阶段，发送方 Alice 将加载了经典信息的相干态通过量子信道传送至接收端，接收端 Bob 采用零拍探测器或外差探测器对所加载的信息进行检测。第二阶段是通过经典信道进行数据协调，获得安全密钥。常见的数据协调方式有直接协调和逆向协调两种方式[5][6]，逆向数据协调的好处是可在任意信道衰减下安全传输密钥，故长距离密钥分发常采用逆向数据协调。但逆向协调对额外噪声很敏感，因此在逆向协调的连续变量量子密钥分发系统中，必须严格控制额外噪声。

本文从理论上分析了逆向协调的相干态连续变量量子密钥分发系统中，当单独考虑系统发送端额外噪声、信道额外噪声以及探测器额外噪声时，它们对安全密钥率的影响以及为保证密钥安全性各部分额外噪声所需满足的条件，然后综合考虑三种噪声都存在时，为保证密钥的安全各部分噪声需满足的条件。

2 发送端额外噪声分析

2.1 发送方额外噪声对密钥安全性的影响

假设 Alice 端调制系统是绝对安全的，暂不考虑信道的额外噪声并认为探测器是理想的。记信道传输率为 G，发送方调制方差为 VN_0（$V = V_A + 1$，N_0 表

示量子噪声，文中取为 1），额外噪声方差为 ΔVN_0，这个噪声主要由调制误差及激光器相位噪声引起。

首先考虑逆向协调下 Eve 采用个体攻击的情况，此时 Alice 与 Bob 及 Bob 与 Eve 间互信息分别为 I_{AB} 和 I_{BE}，密钥安全性判据为：$\Delta I = I_{AB} - I_{BE} > 0$。当调制系统没有噪声时，安全密钥率为

$$\Delta I_1 = -\frac{1}{2}\log_2(\frac{G}{V}+1-G) \quad (1)$$

当存在调制系统额外噪声时，ΔI 可写为

$$\Delta I_2 = -\frac{1}{2}\log_2[\frac{G}{V+\Delta V}+1-G]-\frac{1}{2}\log_2[G\Delta V+1] \quad (2)$$

比较式(1)和式(2)可见，式(2)中第一项与式(1)形式相同，但由于额外噪声的存在其值略小于(1)式，式(2)中第二项是由于额外噪声的存在，安全密钥率的减小量。由式(2)可得对于给定的 V，ΔV 与 G 须满足一定条件才能得到安全密钥；在 V 任意大时，要保证 $\Delta I > 0$，ΔV 与 G 须满足[7]

$$\Delta V < 1/(1-G) \quad (3)$$

Eve 采用集体攻击时，逆向协调下密钥安全性判据为：$\Delta I = I_{AB} - \chi_{BE} > 0$，$\chi_{BE}$ 是 Eve 与 Bob 间的 Holevo 互信息。集体攻击下当 V 任意大时若发送端调制系统无噪声，安全密钥率的近似表达式为

$$\Delta I = \frac{1}{2}\log_2(\frac{1}{1-G}) \quad (4)$$

当发送方调制系统存在噪声（噪声功率 ΔV）时，安全密钥率为

$$\Delta I = \frac{1}{2}\log_2(\frac{1}{1-G})-\frac{1}{2}\log_2(1+G\Delta V) \quad (5)$$

比较式(4)和式(5)可见，式(5)中第二项是由于调制系统额外噪声的存在密钥的减少量。由式(5)可得为保证 $\Delta I > 0$，ΔV 与 G 须满足

$$\Delta V < 1/(1-G) \quad (6)$$

可见在 V 任意大时，为保证 $\Delta I > 0$，集体攻击和个体攻击下 ΔV 与 G 需满足的条件相同，都需满足式(6)所示的条件。

2.2 减小发送方额外噪声对密钥安全性影响

在调制误差不变的情况下，为了减小发送方额外噪声对密钥安全性的影响，可以采用在调制器输出端放置一衰减器的方法[7][8]。加衰减器后个体攻击下密钥率可表示为

$$\Delta I = -\frac{1}{2}\log_2(1-G+\frac{G}{T(V+\Delta V)})-\frac{1}{2}\log_2(1+GT\Delta V) \quad (7)$$

个体攻击下最优衰减器传输为

$$T = \frac{1}{V_A+\Delta V}(\sqrt{\frac{(1-G)\Delta V+V_A}{(1-G)\Delta V}}-1) \quad (8)$$

较式（7）和式（2），两式中第二项是由于额外噪声的存在使安全密钥率的减少量，由式（7）中第二项可见加入衰减器后，额外噪声 ΔV 对 ΔI 的影响减小，同时也可以看出衰减器也使（7）中第一项的值减小了。该方法的不足是减小发送方额外噪声对安全密钥率的影响的同时也减小了调制功率 V，从而使密钥率减小。

集体攻击下加入衰减器，在 V 任意大时密钥率为[6]

$$I = \frac{1}{2}\log_2(\frac{1}{1-G})-\frac{1}{2}\log_2(GT\Delta V+1) \quad (9)$$

比较式（9）和式（5），两式中第一项是发送方没有额外噪声时的安全密钥率，第二项是由于额外噪声的存在安全密钥率的减少量，由式（9）可以看出加入衰减器对第一项没有影响，只减小了额外噪声 ΔV 对 ΔI 的影响。

3 信道额外噪声分析

在连续变量量子密钥分发中，认为信道是完全由攻击者 Eve 控制的，信道额外噪声反映了攻击者对合法通信者的干扰。假设 Alice 端调制系统和 Bob 端探测器是理想的，只考虑信道的衰减和额外噪声。记信道传输率为 G，额外噪声为 ε_1。

个体攻击逆向协调下，当信道没有额外噪声时安全密钥率与式(1)相同，信道存在额外噪声时密钥率为

$$\Delta I_2 = -1/2\log_2(G\varepsilon_1+1)(1-G+G/V+G\varepsilon_1) \quad (10)$$

由式(10)可得，要使 $\Delta I > 0$，ε_1、G 须满足

$$\varepsilon_1 < 1/2G((G-G/V-2)+\sqrt{4+G^2(1/V-1)^2}) \quad (11)$$

由式(11)可得 ε_1 的上限值是信道传输率 G 的单调递增函数，其最大上限值出现在 G=1 处，在 V 任意大、$G\to 1$ 的极限条件下，ε_1 上限值约为 0.62，表明在个体攻击逆向协调下，要使 $\Delta I > 0$ 信道额外噪声不能大于 0.62 倍的量子噪声。

Eve 采用集体攻击时，逆向协调下密钥安全性判据为 $\Delta I = I_{AB} - \chi_{BE} > 0$，此时 ΔI 的解析表达式可见文献[2]。从其解析式可得出：当 V 任意大时，ε_1 的上限

978-1-935068-01-3 © 2009 SciRes.

随信道传输率 G 的增加而增加，当$G \to 1$时 ε_1 的上限值为 0.39。表明集体攻下逆向协调时，要得到安全的量子密钥，信道额外噪声不能大于 0.39 倍的量子噪声。

4 探测器额外噪声分析

假设探测器的额外噪声和衰减不受攻击者 Eve 控制，连续变量量子密钥分发系统的发送端和信道是理想，即发送端没有额外噪声，信道只有衰减没有额外噪声。记 Bob 端探测器传输率为 η，额外噪声 ε_2，等效探测器输入端噪声为 $\chi_2 = (1-\eta+\varepsilon_2)/\eta$。

个体攻击逆向协调下，当探测器没有额外噪声只有衰减时，安全密钥率为

$$\Delta I = \frac{1}{2}\log_2\left(\frac{\eta G + (1-G) + (1-\eta)G/V}{(1-G)+G/V}\right) \tag{12}$$

而当探测器存在额外噪声 ε_2 时的安全密钥率为

$$\Delta I = \frac{1}{2}\log_2\left(\frac{\eta G + (1+\varepsilon_2)(1-G) + (1-\eta+\varepsilon_2)G/V}{(1+\varepsilon_2)(1-G+G/V)}\right) \tag{13}$$

ΔI 随 ε_2 的增加而减小，当 $\varepsilon_2 \to \infty$ 时，$\Delta I \to 0$，但 ΔI 始终大于 0，这表明当探测器额外噪声很大时虽然密钥率会很小，但密钥是安全的。

集体攻击逆向协调下，当探测器没有额外噪声只有衰减时，在 $V \to \infty$ 时安全密钥率为

$$\Delta I = \frac{1}{2}\log_2\left(1+\frac{\eta G}{1-G}\right) \tag{14}$$

当探测器额外噪声为 ε_2 时，在 $V \to \infty$ 时安全密钥率为

$$\Delta I = \frac{1}{2}\log_2\left(1+\frac{\eta G}{(1+\varepsilon_2)(1-G)}\right) \tag{15}$$

由式（15）可见，存在探测器额外噪声时虽然安全密钥率会减小，但不论 ε_2 取何值，ΔI 始终是大于 0 的，即密钥是安全的。

比较在 $V \to \infty$ 时个体攻击和集体攻击下的安全密钥率，可以得出在此极限条件下，两种攻击方式安全密钥率的解析表达式是一样的，表明逆向协调下在没有信道额外噪声和发送端额外噪声时，不论攻击者采用何种攻击方式，对合法通信者的干扰能力相同。

5 连续变量量子密钥分发系统额外噪声分析

上文对连续变量量子密钥分发系统各部分噪声分别进行了讨论并给出了在个体攻击和集体攻击时，各部分噪声的上限。在实际系统中，上文所述各部分额外噪声都是存在的，故在此对系统的额外噪声进行整体分析。

如前所述，连续变量量子密钥分发系统的额外噪声包括发送端调制噪声和相位噪声、信道额外噪声以及探测器端额外噪声。记发送端额外噪声为 ΔV，信道额外噪声 ε_1，探测器端额外噪声 ε_2，信道传输率为 G，探测器传输率 η，总的等效输入端噪声为:

$$\chi = \Delta V + \frac{1-G}{G} + \varepsilon_1 + \frac{1-\eta+\varepsilon_2}{\eta G} \tag{16}$$

在连续变量量子密钥分发系统安全性的分析中，为简化分析通常假设探测器也完全受攻击者 Eve 的控制，即探测器端衰减和额外噪声都由 Eve 控制，但实际中探测器的衰减及额外噪声是不受攻击者控制的，下面在此实际情形下进行分析和讨论。

个体攻击逆向协调下，考虑整个系统中所有额外噪声，安全密钥率为

$$\Delta I = \frac{1}{2}\log_2\left(\frac{\eta/(1-G+G(1/(V+\Delta V)+\varepsilon_1))+1-\eta+\varepsilon_2}{1+\Delta V+\eta G\varepsilon_1+\varepsilon_2}\right) \tag{17}$$

在 $V \to \infty$ 时，为得到安全密钥，各部分额外噪声需满足

$$\frac{1}{\Delta V}\left(\frac{1-\varepsilon_1}{1-G+G\varepsilon_1}-\varepsilon_1\right) > \frac{1}{\eta G} \tag{18}$$

由式(17)(18)可见，在连续变量量子密钥分发系统中，影响密钥安全性的主要是信道额外噪声，其次是发送端额外噪声，探测器额外噪声对密钥安全性没有影响。在集体攻击的情形下也可做类似的分析[2]。

6 小结

对比逆向协调下连续变量量子密钥分发系统中各部分额外噪声对密钥安全性的影响，可以看出，密钥安全性对信道的额外噪声最敏感，其次是发送端的额外噪声，对探测器端额外噪声最不敏感。

References (参考文献)

[1] F. Grosshans, G. Van Assche, J. Wenger.Quantum key distribution using Gaussian-modulated coherent states[J]. Nature,2003, 421: 238-241.

[2] J.Lodewyck, M.Bloch. Quantum key distribution over 25km with an all-fiber continuous-variable system[J].Phys.Rev.A, 2007,76,042305.

[3] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri. Controlling excess noise in fiber-optics continuous-variable quantum key distribution[J]. Phys. Rev. A, 2005, 72, 050303 R.

[4] Bing Qi,Lei-Lei Huang. Experimental study on the Gaus-

sian-modulated coherent-state quantum key distribution over standard telecommunication fibers [J]. Phys.Rev.A , 2007,76,052323.

[5] J. Lodewyck, N.J,Cerf. Viritual Entanglement and Reconciliation Protocol for Quantum Cryptography with Continuous Variables.［EB/OL］.arXiv:quant-ph/0306141vl 20 Jun 2003.

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

[7] R.Filip. Continuous-variable quantum key distribution with noisy coherent states[J]. Phys.Rev.A , 2008,77,022310

[8] R.Filip.Security of conherent-state key distribution through an amplifying channel[J]. Phys.Rev.A , 2008,77,032347

978-1-935068-01-3 © 2009 SciRes.