量子光学学报 18(1)：23～26，2012
Acta Sinica Quantum Optica

文章编号：1007-6654(2012)01-0023-04 [2]

连续变量量子密钥分发的数据逆向协调

白增亮， 王旭阳， 杜鹏燕， 李永民†

（量子光学与光量子器件国家重点实验室，山西大学光电研究所，山西 太原 030006）

摘要：基于多级编码/多级译码(MLC/MSD)系统实现了连续变量量子密钥分发的逆向数据协调。讨论了高斯连续变量量化过程中使互信息量最大时最佳量化区间的选取，并且通过理论计算给出了信噪比为 4 dB 的情况下各级等价信道的最佳码率。协调方案中选择低密度奇偶校验码(LDPC)作为信道编码，结合边信息译码原理最终通过 LDPC 迭代译码算法实现了数据的逆向协调。

关键词：连续变量； 量子密钥分发； 逆向协调； 低密度奇偶校验码

中图分类号：O431 **文献标识码**：A

量子密钥分发(Quantum key distribution，QKD)是信息安全领域一个新的分支，量子不确定性原理和量子不可克隆原理等量子物理的基本原理保证了量子密钥分发对任意窃听行为的可检测性。

在 QKD 过程中，通信双方 Alice 和 Bob 得到互相关联的一组数据，在实际系统中，为了从存在各种噪声和窃听的裸码中提取出绝对安全的密钥序列，在 QKD 系统中引入数据协调和私密放大的概念[1]。所谓数据协调(reconciliation)，就是在接收方对量子态进行测量重新得到经典数据(裸码)后，利用公开经典信道对筛后数据进行纠错的全过程，数据协调的作用是通过纠错编码的方法，利用 Alice 和 Bob 共同拥有的关联数据序列得到一组完全一致的数据序列。

本论文在连续变量 QKD 的数据协调过程中采用逆向协调方案[2-5]。逆向协调系统采用 Multilevel Coding/Multistage Decoding (MLC/MSD)结构，并且结合性能良好的低密度奇偶校验码(LDPC)作为信道纠错码，最终实现了高效率的数据协调。

1 数据协调方案

在数据协调过程中，我们选用逆向数据协调方案，也就是说最终 Alice 要以 Bob 测量的数据为准达成一致，如图 1 所示。

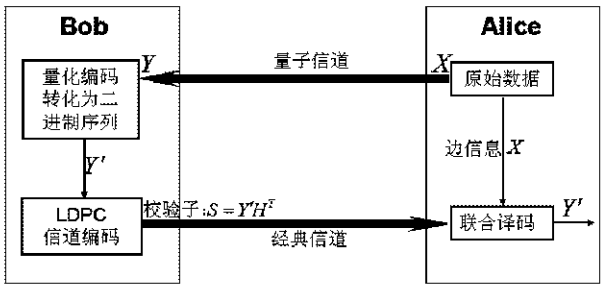

图 1 逆向数据协调方案

Fig. 1 Reverse-reconciliation protocol

Alice 通过高斯调制将原始的密钥数据 X 调制到相干态上，并经过量子信道发送给 Bob。由于量子信道以及实验元器件存在噪声和损耗，

[2] 收稿日期：2011-11-30

基金项目：国家自然科学基金(No. 11074156)；山西省高等学校优秀青年学术带头人支持计划；山西省回国留学人员科研资助项目

作者简介：白增亮(1984—)，男，山西原平人，硕士研究生，研究领域：量子通信。E-mail：200922609001@mail.sxu.cn

†通信作者：E-mail：yongmin@sxu.edu.cn

Bob 通过量子态的测量以及对基比对后得到了数据 Y，X 与 Y 是一组互相关联的、连续取值的高斯信号。然后 Bob 采用量化编码的方法将高斯连续信号转化为一组二进制序列 Y′。接着采用 LDPC 信道编码得到校验子 S 以后将其通过经典信道返回到 Alice。Alice 结合边信息译码原理[6]，采用迭代译码的方法，将自己原有的边信息 X 和得到的校验子 S 联合译码最终恢复出 Bob 的二进制序列 Y′。

2 信源量化编码

协调过程的效率可写成两部分效率的乘积：

$$\beta = \beta_{codes}\beta_q \tag{1}$$

其中乘积中的第一项表示信道编码中实际码率带来的协调效率，而第二项是由于量化编码对互信息量的损失带来的协调效率。理论上，量化必然会带来一定的信息损失，即 $I(X,Y') < I(X,Y) = I_{AB}$，但是可以使信息损失降低到允许的范围里[7]。现简要说明量化区间的选取：Alice 端随机变量 $X \sim N(0,\Sigma)$，Bob 端随机变量 Y 是在 X 的基础上叠加了方差为 σ^2 高斯噪声 N，所以 $Y \sim N(0,\sqrt{\Sigma^2+\sigma^2})$。Bob 随机变量 Y 量化为离散变量 Y'，那么双方的互信息量 $I(X,Y') = H(X) + H(Y') - H(X,Y')$，其中

$$H(X) = \frac{1}{2}\log 2\pi e\Sigma^2 \tag{2}$$

$$H(Y') = -\sum_a P_a \log P_a \tag{3}$$

$$P_a = \frac{1}{2}\left(erf\left(\frac{t_a}{\sqrt{2(\Sigma^2+\sigma^2)}}\right) - erf\left(\frac{t_{a-1}}{\sqrt{2(\Sigma^2+\sigma^2)}}\right)\right) \tag{4}$$

$$H(X,Y') = -\sum_a \int_{-\infty}^{+\infty} dx f_a(x)\log f_a(x) \tag{5}$$

$$f_a(x) = \int_{t_{a-1}}^{t_a} dy f_{X,Y}(x,y) \tag{6}$$

$$f_{X,Y}(x,y) = \frac{1}{2\pi\Sigma\sigma} e^{-\frac{x^2}{2\Sigma^2}} e^{-\frac{(x-y)^2}{2\sigma^2}} \tag{7}$$

其中 $t_1, \cdots t_{a-1}$ 表示量化区间值，并且 $t_0 = -\infty$，$t_a = \infty$。a 表示区间 $[t_{a-1}, t_a]$。

Bob 对高斯连续信号进行量化的过程中，对实数采用等间隔 16 进制量化，每一个量化区间对应一个 4 bit 码本，并采用自然码对其编码。以下给出了信噪比为 4 dB 时，最佳量化间隔为 0.315，量化区间见表 1。

表 1 量化区间

Tab. 1 Quantized interval

[−inf,−2.205]	[−2.205,−1.89]	[−1.89,−1.575]	[−1.575,−1.26]
[−1.26,−0.945]	[−0.945,−0.63]	[−0.63,−0.315]	[−0.315,0]
[0,0.315]	[0.315,0.63]	[0.63,0.945]	[0.945,1.26]
[1.26,1.575]	[1.575,1.89]	[1.89,2.205]	[2.205,inf]

3 信道编码与译码

根据 Shannon 第二定理，对于有噪信道，只要信道编码采用足够长的码长，选择好的信道编码可以使得误码率达到任意小，且信道上信息的传输速率可以无限接近信道容量。LDPC 码是目前最逼近 Shannon 极限的信道纠错码，它是一种线性分组码，其校验矩阵只含有很少量非零元素。正是校验矩阵的这种稀疏性，保证了译码复杂度和最小码距都只随着码长呈现线性增加[8-10]。研究表明，与 Turbo 码相比，LDPC 码具有描述简单、译码复杂度低、可以并行实现等优点。基于 LDPC 码的协调方案理论上能够达到最佳性能[11]。鉴于连续变量量子密钥分发系统中量子信道噪声情况差、信噪比比较低而且要求通信速率很高这些特点，所以信道编码选择性能良好的 LDPC 码。

协调系统采用 Multilevel Coding/Multistage Decoding（MLC/MSD）结构，如图 2 所示[4]。MLC 是 H. Imai 于 1977 年首先提出来的思想[12]，也被称为“带宽有效性编码”。MLC 是基于信号星座点调制的一种信道编码技术，它在不增加信号带宽，又不降低有效数据传输速率的前提下，有效地提高了数据传输性能[13]。MLC 的优点就是：各级根据设计规则和实际考虑选择不

同的码率[13-14]。MSD是H. Imai同时给出的针对MLC的一种准最佳译码方案[12]。

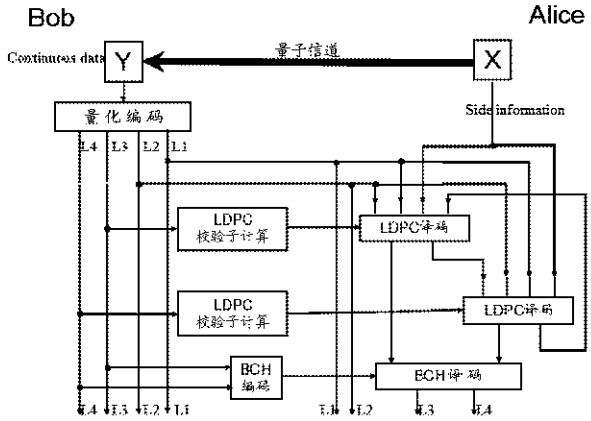

图2　基于LDPC码的多级编码原理

Fig. 2　Principle of MLC/MSD with LDPC codes

3.1　各级码率的选取

基于MLC方案的LDPC信道编码，其首先要构造理想的稀疏校验矩阵H，以及根据信道容量规则[13-14]选择各级的码率。根据互信息的链规则[15]可知：

$$I(X,Y') = I(X;L_1,L_2,L_3,L_4) = \sum_{i=1}^{4} I_{Li} \quad (8)$$

其中，

$$\begin{aligned} I_{Li} &= I(X;L_i \mid L_1,\cdots,L_{i-1}) \\ &= H(L_i \mid L_1,\cdots,L_{i-1}) - \\ &\quad H(L_i \mid X,L_1,\cdots,L_{i-1}). \end{aligned}$$

在编码调制过程中信号星座点集分割采用高斯信道中最佳集分割——自然分割法(Ungerboeck Partitioning)。根据已知的信道转移概率$f(y \mid x)$、量化区间以及信道容量公式，通过理论计算可得各级信息位所携带的密钥信息I_{Li}。当SNR=4 dB时，可以得到各级信息位所携带的密钥信息分别为：

$$I_{L1} = 0.003\ 6\ \text{bits/}symbol,$$

$$I_{L2} = 0.006\ 9\ \text{bits/}symbol,$$

$$I_{L3} = 0.273\ 9\ \text{bits/}symbol,$$

$$I_{L4} = 0.615\ 9\ \text{bits/}symbol,$$

据最佳码率计算公式：$R_{Li}^{opt} = 1 - (I_{Limf} - I_{Li})$，得各级信息位的最佳码率分别为：0.004/0.007/0.281/0.826。由于低的两位信息位最佳码率很小，如果直接公开传输而不进行编码，对协调系统的效率影响很小，并且这样处理后减少了系统的耗时，从而提高了密钥的传输速率。

3.2　LDPC迭代译码

在多级译码(MSD)过程中，采用LDPC码作为信道码，码长N为240000，校验矩阵H是LDPC码的核心，直接影响编码纠错的性能。我们采用Mackay构造法寻找比较理想的校验矩阵，结合边信息译码原理，各级采用对数似然比BP算法进行迭代译码。其中第一、二级通过经典信道不进行编码，直接公开发送；第三、四级之间互相迭代(即第三级的译码要以第四级的结果为条件，反之亦然)。通过分析迭代译码的收敛性，选择最佳的迭代译码次数，最终实现了编码纠错的过程。LDPC码稀疏矩阵的选取是非常重要的，它直接关系到协调系统性能的好坏。还可以选择其它的一些好的稀疏矩阵构造法，构造更理想的稀疏矩阵。由于LDPC编码纠错后有时候会有一些没有纠错的信息，为了达到更好的纠错性能，还可以在其后级联其它的信道编码，如BCH码，然而这同时会引入一些时间上的开销。

4　总结

本论文在全光纤连续变量量子密钥分发系统的基础上实现了逆向的数据协调。在量化过程中采用等间隔量化的方法，在编码过程中采用MLC的协调方案，通过选择合适的码率，结合边信息译码原理和各级迭代译码最终实现了数据逆向协调。

参考文献：

[1] BENNETT C H, BRASSARD G, ROBERT J M. Privacy Amplification by Public Discussion [J]. *SIAM Journal on computing*, 1988, **17**: 210-229.

[2] GROSSHANS F, ASSCHE G V, WENGER J, *et al*. Quantum Key Distribution Using Gaussian-modulated Coherent States [J]. *Nature*, 2003, **421**: 238-241.

[3] GROSSHANS F, GRANGIER P. Reverse Reconciliation Protocols for Quantum Cryptography with Continuous Variables [Z/OL]. arXiv:quant-ph/0204127v1 (Submitted on 22 Apr 2002).

[4] JÉRÔME LODEWYCK, MATTHIEU BLOCH, RAÙL GARCÍA－PATRÓN, *et al*. Quantum Key Distribution Over 25 km with an All-fiber Continuous-variable System [J]. *Physical Review A*, 2007, **76**: 042305.

[5] 逯志欣，于丽，李康，等. 基于逆向协调的连续变量量子密钥分发数据协调 [J]. 中国科学 G 辑，2009，**39**(11)：1606-1612.

[6] LIVERIS A D, XIONG Zi-xiang, GEORGHIADES C N. Compression of Binary Sources With Side Information at the Decoder Using LDPC Codes [J]. *IEEE Communications Letters*, 2002, **6**(10): 440-442.

[7] ASSCHE G V, CARDINAL J, CERF N J. Reconciliation of a Quantum-Distributed Gaussian Key [J]. *IEEE Trans Inform Theory*, 2004, **50**(2): 394-400.

[8] GALLAGER R G. Low-Density Parity-Check Codes [M]. Cambridge, MA: M. I. T. Press, 1963.

[9] MACKAY DAVID J C. Good Error-Correcting Codes Based on Very Sparse Matrices [J]. *IEEE Trans Inform Theory*, 1999, **45**(2): 399-431.

[10] MACKAY DAVID J C, NEAL R M. Near Shannon Limit Performance of Low Density Parity Check Codes [J]. *Electronics letters*, 1997, **33**(6): 457-458.

[11] SHANNON C E. A Mathematical Theory of Communication [J]. *Bell Syst Tech J*, 1948, **27**: 623-656.

[12] IMAI H, HIRAKAWA S. A New Multilevel Coding Method Using Error-Correcting Codes [J]. *IEEE Trans Inform Theory*, 1977, **IT-23**(3): 371-377.

[13] WACHSMANN UDO, FISCHER ROBERT F H, HUBER JOHANNES B. Multilevel Codes: Theoretical Concepts and Practical Design Rules [J]. *IEEE Trans Inform Theory*, 1999, **45**(5): 1361-1391.

[14] BORRAN J M, AAZHANG B. Multilevel Codes and Iterative Multistage Decoding: Rate Design Rules and Practical Considerations [J]. *IEEE Wireless Communications and Networking Conference*, 2000, **1**: 36-41.

[15] COVER T M, THOMAS J A. Elements of Information Theory [M]. New York: A John Wiley & Sons, 1991.

Reverse Reconciliation for Continuous Variable Quantum Key Distribution

BAI Zeng-liang, WANG Xu-yang, DU Peng-yan, LI Yong-min

(*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan* 030006, *China*)

Abstract: Based on the Multilevel Codes/Multistage Decoding system, we achieved the reverse reconciliation for continuous variable quantum key distribution. Firstly, we show how to select the optimal quantization interval by maximizing the mutual information between the communicating parties. Then the optimal rate of each equivalent channel is calculated at the SNR level of 4 dB. The low-density parity check (LDPC) code is chosen as the channel codes, and the reverse reconciliation utilize a side-information based LDPC iterative decoding algorithm.

Key words: continuous variable; quantum key distribution; reverse reconciliation; low density parity check code