山西大学学报(自然科学版)40(2):281－285,2017
Journal of Shanxi University(Nat. Sci. Ed.)

DOI:10.13451/j.cnki.shanxi.univ(nat.sci.).2017.02.012

用于连续变量码率自适应的数据协调方案

白增亮,杨申申,李永民*

(山西大学 光电研究所 量子光学与光量子器件国家重点实验室,山西 太原 030006;
山西大学 极端光学协同创新中心,山西 太原 030006)

摘　要:量子密钥分发能够使得合法通信双方共享一组无条件安全的密钥。数据协调是量子密钥分发过程中非常重要的一个环节,能够对密钥分发过程中产生的错误进行纠错。低密度奇偶校验(LDPC)码是一种性能接近于Shannon极限的信道纠错码,适用于高效的数据协调。为了达到高的协调效率,需要根据信道的信噪比适当地选择最佳的LDPC码的码率。我们提出了一种适用于高斯调制连续变量量子密钥分发的码率可调的数据协调方案:当信道信噪比发生变化时,使用码率调整技术对数据协调过程中每一级LDPC码的码率进行适当地调整,从而确保数据协调的效率在一定信噪比变化范围内能够保持。

关键词:量子密钥分发;连续变量;数据协调;LDPC码;码率自适应

中图分类号:O431　　**文献标志码**:A　　**文章编号**:0253-2395(2017)02-0281-05

Rate-Adaptive Protocol for Continuous Variable Key Reconciliation

BAI Zengliang, YANG Shenshen, LI Yongmin*

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

Abstract: Quantum key distribution (QKD) enables two legal parities to share a secure key. Information reconciliation is an essential process in quantum key distribution. Low-density parity-check (LDPC) codes, which belong to the class of linear error correcting codes and perform at rates extremely close to the Shannon capacity, can achieve the key reconciliation with high efficiency. Considering a time-varying channel in practical continuous variable QKD system, we propose a rate-adaptive protocol for continuous variable key reconciliation, which can cover a broad range of signal-to-noise ratio and achieve higher reconciliation efficiency.

Key words: quantum key distribution; continuous variable; information reconciliation; LDPC code; rate-adaptive

0　引言

量子密钥分发[1-5]是量子信息领域最接近实用化的一个发展方向,已经成为各国学者的研究热点之一。基于量子物理的基本原理(量子不确定性原理和量子不可克隆定理),任何潜在的窃听者都会对量子态造成

* 收稿日期:2017-02-28;修回日期:2017-03-07
基金项目:国家自然科学基金(61378010;11504219);国家重点研发计划(2016YFA0301403);山西省高等学校创新人才支持计划资助的课题
作者简介:白增亮(1984－),男,博士研究生,主要从事量子通信方面的研究。E-mail:bzlwmj@foxmail.com
* 通信作者:李永民(LI Yongmin),E-mail:yongmin@sxu.edu.cn

扰动,量子密钥分发能够对任意的窃听行为进行检测。共享的密钥用于一次一密(one-time pad)加密方案,通信双方可以实现无条件的安全通信。由于其具有安全通信的优势,能够广泛用于国防、军事、商业等领域。近几年量子密钥分发在实验室已经取得快速的发展,逐步走向了工程化、产品化阶段。

量子密钥分发一般包括量子密钥传输和经典的数据后处理两个阶段。在第一个阶段,通信双方(Alice和Bob)将密钥信息通过量子信道传输获得裸码。离散变量量子密钥分发将密钥信息调制在单光子或者弱相干态上,使用单光子探测器对量子态进行测量。连续变量量子密钥分发将高斯随机数调制到相干态或者压缩态光场上,然后使用平衡零拍探测器对其进行测量。由于在量子传输过程中存在各种各样的噪声以及第三方的窃听,在数据后处理阶段需要对量子传输以后得到的裸码信息进行经典的数据处理,最终提取出无条件安全的密钥。数据后处理主要包括数据协调与私密放大两个过程。数据协调是一个纠错过程,使用信道纠错的方法对裸码中不一致的信息进行纠错。然后经过私密放大,去除窃听者窃取的信息,从部分安全的信息中提取出安全密钥。

与离散变量相比,连续变量量子密钥分发在较短距离上能够实现较高的安全密钥速率,具有易于实现的商业化光学组件以及能够较好地兼容于现有的光通信网络。针对连续变量的数据协调,主要包括样条数据协调(slice reconciliation)[6-10]和多维协调(multidimensional reconciliation)[11-13]两种方案。样条数据协调主要适用于信噪比大于1的较短距离连续变量量子密钥分发。在信道纠错过程中,采用多级编码和多级译码(Multilevel coding and Multistage decoding)方案[7]。同时采用逆向协调方案(正向协调要求量子信道传输率必须大于0.5)[14]并结合边信息(side information)译码原理[15],通信双方只进行单次通信,从而最大限度地减小了信息的泄露,实现高效的数据协调。

低密度奇偶校验码,简称LDPC码,属于信道纠错码,具有接近香农极限的纠错性能,低的误码平台以及低的译码复杂度。将LDPC码用于数据协调中,能够实现高效的数据协调。在实际密钥分发过程中信道的信噪比并不是固定不变的,而是随着时间的变化,信噪比也发生着变化。LDPC码的码率自适应方案能够随着信噪比的变化而对码率进行适当的调整,从而能够在较大的信噪比变化范围内得到高的纠错效率。对于在离散变量量子密钥分发过程中,目前已经提出了几种码率可调整的自适应纠错方案[16-18],用于连续变量量子密钥分发的码率自适应方案还未有公开的报道。本文我们提出了连续变量的码率兼容的样条数据纠错方案,能够实现多级编码中每一级的码率根据信噪比的变化进行适当的调整,从而能够更有效地进行纠错编码,实现更高效的数据协调。

1 LDPC码率调整

LDPC码通常利用一个稀疏的校验矩阵或者Tanner图来表示。Tanner图中采用边将校验节点和变量节点相连。基于Tanner图中不同变量节点之间的信息传递,LDPC码采用后验概率信息的软判决译码,并通过迭代运算,从而实现高的纠错性能。删余(Puncturing)[19-20]和缩短(Shortening)[21]是两种码率调整技术,能够使LDPC码的码率分别增大和减小。使用这两种技术,我们可以对信噪比变化的信道实现LDPC码码率的自适应纠错编码。给定一个预先构造好的LDPC码$C(n,k)$,在n个码字中删除p个符号($p<n$)将$C(n,k)$码转化为一个$C(n-p,k)$码,被称为LDPC码的删余过程(如图1所示)。那么此时的码率被增大为

$$R=\frac{k}{n-p}=\frac{R_0}{1-\pi}, \tag{1}$$

其中$R_0=\frac{k}{n}$是原来的码率,$\pi=\frac{p}{n}$是删余符号占总码字的比例。删余技术是通过减少冗余信息而增大码率,而缩短技术是通过减少有用信息而减小码率。如图2所示为LDPC码的缩短方案,在编译码过程中,通过选定码字中的t个符号($t<n$)将$C(n,k)$码转化为$C(n-t,k-t)$码,从而码率被减小为

$$R=\frac{k-t}{n-t}=\frac{R_0-\sigma}{1-\sigma}, \tag{2}$$

其中$\sigma=\frac{t}{n}$是缩短符号占总码字的比例。如果将删余和缩短同时用于原始码$C(n,k)$,我们就可以根据信道的信噪比的变化,实时地调整LDPC码的码率。调整以后的码率为

$$R=\frac{k-t}{n-p-t}=\frac{R_0-\sigma}{1-\pi-\sigma}. \tag{3}$$

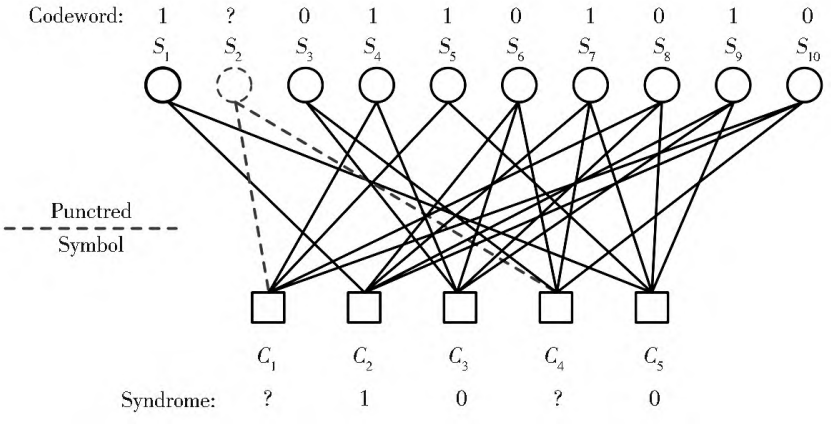

Fig. 1 Scheme of puncturing applied to a LDPC code represented by its Tanner graph. s_i: variable node, c_i: check node

图 1 Tanner 图中 LDPC 码的删余方案,s_i:变量节点,c_i:校验节点

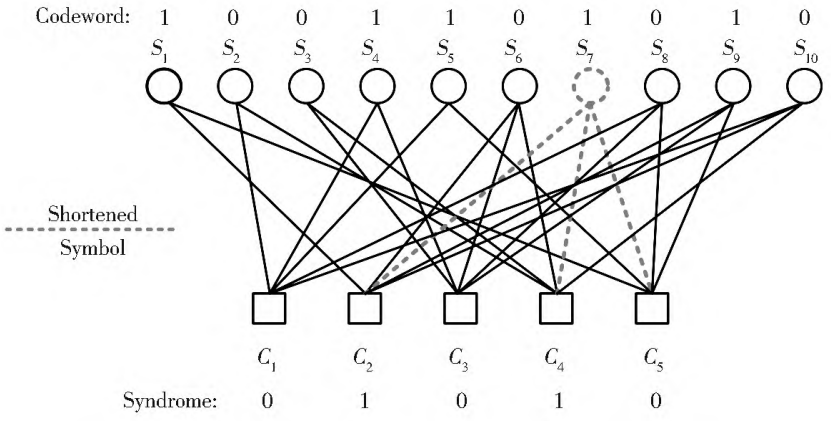

Fig. 2 Scheme of shortening applied to a LDPC code represented by its Tanner graph. s_i: variable node, c_i: check node

图 2 Tanner 图中 LDPC 码的缩短方案,s_i:变量节点,c_i:校验节点

2 码率自适应的样条数据协调方案设计

对于高斯调制相干态的连续变量量子密钥分发中,双方得到的裸码是一组相互关联的连续的高斯分布随机数。样条数据协调的过程中 Bob 首先需要对高斯分布的连续变量进行 2^m 区间量化,转化为 m 级二进制的随机序列,然后对每一级二进制序列分别编码(生成校验子)并发送给 Alice。Alice 结合自己原有的信息对每一级接收到的信息进行联合迭代译码,最终双方能够共享相同的二进制序列。在信道纠错过程中,LDPC 码只是针对某个信噪比而预先设计,无法满足信噪比连续变化的信道。我们在传统样条数据协调[10]的基础上引入了 LDPC 码率调整方案,可以使得预先设计的 LDPC 码适用于一定范围的信噪比区间。连续变量量子密钥分发码率自适应的样条数据协调过程如图 3 所示。

高斯随机数 X 和 Y 是 Alice 和 Bob 经过量子传输以后得到的一组相互关联的高斯随机数。双方通过信道参数估计可以计算得到量子信道的信噪比。根据信噪比选定初始的 LDPC 码,当信道信噪比发生较小的变化时,我们就可以使用 LDPC 码的删余和缩短技术对码率做适当的调整,具体步骤如下:

第一步:根据信噪比给每一级选定码长为 N 的初始 LDPC 码(校验矩阵为:H_i),初始码率为 R_i^0.

第二步:设定参数。信噪比发生改变后,根据当前信噪比,设定参数 d(删余符号和缩短符号的数量总和)以及每一级合适的目标码率 R_i。由于在多级译码过程中,每一级的译码与其他级并不是相互独立的,需要对多级之间进行联合译码,所以每一级中的参数 d 必须是相同的。缩短符号的数量 t_i 和删余符号的数量 p_i 分别可以根据以下式子计算得到:

$$t_i = \left\lceil \left(R_i^0 - \left(1 - \frac{d}{N}\right) \cdot R_i \right) \cdot N \right\rceil , \tag{4}$$

$$p_i = d - t_i . \tag{5}$$

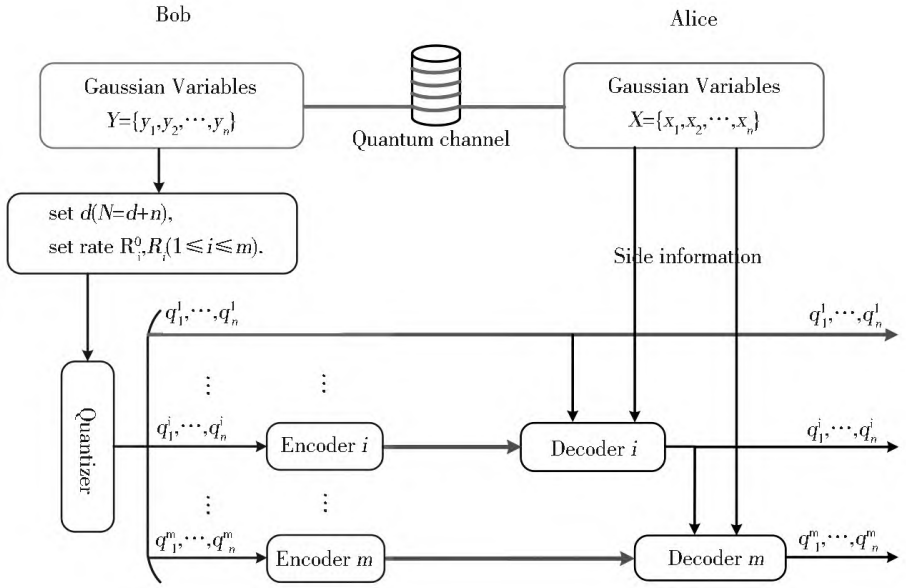

Fig. 3 Rate-compatible slice reconciliation scheme

图 3 码率自适应的样条数据协调方案

第三步:高斯随机数量化。 Bob **对长度为** $n=N-d$ **的高斯随机数序列进行** 2^m **个区间量化,转化为** m **个二进制序列:** $(q_1^1,q_2^1,\cdots,q_n^1),\cdots,(q_1^i,q_2^i,\cdots,q_n^i),\cdots,(q_1^m,q_2^m,\cdots,q_n^m)$.

第四步:分级编码。在每一级编码过程中,Bob **首先要通过随机数发生器产生两组长度为** p_i **和** t_i **的二进制随机数序列分别作为删余符号序列和缩短符号序列。产生的这两组序列与信息序列** $(q_1^i,q_2^i,\cdots,q_n^i)$ **进行随机组合,生成长度为** N **的码字** C_i**,然后生成校验子:** $S_i=H_i\cdot C'_i$. Bob **将删余符号所在码字中的位置,缩短符号序列及其位置以及校验子** S_i **一起发送给** Alice.

第五步:多级译码。 Alice **对从经典信道接收到的信息采用** belief propagation **译码算法进行迭代译码以及多级之间联合译码。在译码过程中,**Alice **首先将自己原有的高斯随机数作为边信息,结合接收到的信息,对** Bob **端的信息进行一个初始化估算。由于** Bob **仅仅将删余符号的位置发送给对方,所以** Alice **无法估算码字中删余符号的信息。**

通过以上编码和译码过程,我们就可以对初始 LDPC **码实现删余和缩短操作,方便灵活地改变数据协调过程中每一级码率,从而在信道信噪比变化的情况下实现高效的数据协调。**

3 结论

量子密钥分发由于在安全通信领域具有重要的应用价值,引起了各国研究人员的广泛研究与关注。数据协调是量子密钥分发中一个非常重要的环节,直接影响着通信双方的安全密钥速率和密钥分发距离。本文中我们在样条数据协调的基础上提出了一种基于 LDPC **码码率自适应的连续变量数据纠错方案,提高样条数据协调的码率兼容性,能够实现码率自适应的数据协调。该方案可以用于连续变量量子密钥分发系统中。对于该方案进一步的理论仿真,需要解决** LDPC **码删余过程中度分布的最优选择,长码长** LDPC **码的校验矩阵构造以及方案中参数** d **的选择确定等一系列问题,将是我们下一步的研究重点。**

参考文献:

[1] Bennett C H, Brassard G. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984[C]// Bangalore, IEEE, 1984.

[2] Ralph T C. Continuous Variable Quantum Cryptography[J]. *Phys Rev A*, 1999, **61**: 010303. DOI: 10. 1103/PhysRevA.

61. 010303.

[3] Gisin N, Ribordy G, Tittel W, *et al*. Quantum Cryptography[J]. *Rev Mod Phys*, 2002, **74**: 145-195. DOI: 10. 1103/RevModPhys. 74. 145.

[4] Braunstein S L, Van Loock P. Quantum Information with Continuous Variables[J]. *Rev Mod Phys*, 2005, 77: 513-577. DOI: 10. 1103/RevModPhys. 77. 513.

[5] Scarani V, Bechmann-Pasquinucci H, Cerf N J, *et al*. The Security of Practical Quantum Key Distribution[J]. *Rev Mod Phys*, 2009, **81**: 1301-1350. DOI: 10. 1103/RevModPhys. 81. 1301.

[6] Van Assche G, Cardinal J, Cerf N J. Reconciliation of a Quantum-distributed Gaussian Key[J]. *IEEE T Inform Theory*, 2004, **50**: 394-400. DOI: 10. 1109/TIT. 2003. 822618.

[7] Bloch M, Thangaraj A, McLaughlin S W, *et al*. Proceedings of Information Theory Workshop, Mar. 13－17, 2006[C]. Uruguay, IEEE, 2006. DOI: 10. 1109/ITW. 2006. 1633793.

[8] Lodewyck J, Bloch M, García-Patrón R, *et al*. Quantum Key Distribution Over 25 km with an All-fiber Continuous-variable System[J]. *Phys Rev A*, 2007, **76**: 042305. DOI: 10. 1103/PhysRevA. 76. 042305.

[9] Jouguet P, Elkouss D, Kunz-Jacques S. High-bit-rate Continuous-variable Quantum Key Distribution[J]. *Phys Rev A*, 2014, **90**: 042329. DOI: 10. 1103/PhysRevA. 90. 042329.

[10] Bai Z L, Wang X Y, Yang S S, *et al*. High-efficiency Gaussian Key Reconciliation in Continuous Variable Quantum Key Distribution[J]. *Sci China Phys Mech Astron*, 2016, **59**: 614201-614201. DOI: 10. 1007/s11433-015-5702-7.

[11] Leverrier A, Alléaume R, Boutros J, *et al*. Multidimensional Reconciliation for a Continuous-variable Quantum Key Distribution[J]. *Phys Rev A*, 2008, **77**: 042325. DOI: 10. 1103/PhysRevA. 77. 042325.

[12] Jouguet P, Kunz-Jacques S, Leverrier A. Long-distance Continuous-variable Quantum Key Distribution with a Gaussian Modulation[J]. *Phys Rev A*, 2011, **84**: 062317. DOI: 10. 1103/PhysRevA. 84. 062317.

[13] Jouguet P, Kunz-Jacques S, Leverrier A, *et al*. Experimental Demonstration of Long-distance Continuous-variable Quantum Key Distribution[J]. *Nat Photonics*, 2013, **7**: 378-381. DOI: 10. 1038/NPHOTON. 2013. 63.

[14] Grosshans F, Grangier P. Reverse Reconciliation Protocols for Quantum Cryptography with Continuous Variables[J/OL]. arXiv: quant-ph/0204127v1, Apr. 22, 2002.

[15] Liveris A D, Xiong Z X, Georghiades C N. Compression of Binary Sources with Side Information at the Decoder using LDPC Codes[J]. *IEEE Commun Lett*, 2002, **6**: 440-442. DOI: 10. 1109/LCOMM. 2002. 804244.

[16] Elkouss D, Martinez J, Lancho D, *et al*. Proceedings of IEEE Information Theory Workshop on Information Theory, Jan. 6-8, 2010[C]. Cairo, IEEE, 2010. DOI: 10. 1109/ITWKSPS. 2010. 5503195.

[17] Elkouss D, Martínez-Mateo J, Martin V. Proceedings of International Symposium On Information Theory & Its Applications, Oct. 17-20, 2010[C]// Taiwan, IEEE, 2010. DOI: 10. 1109/ISITA. 2010. 5650099.

[18] Martinez-Mateo J, Elkouss D, Martin V. Blind Reconciliation[J]. *Quantum Inf Comput*, 2012, **12**: 791-812.

[19] Pishro-Nik H, Fekri F. Proceedings of Information Theory Workshop, Oct. 24-29, 2004[C]// IEEE, 2005. DOI: 10. 1109/ITW. 2004. 1405302.

[20] Jeongseok H, Jaehong K, McLaughlin S W. Rate-compatible Puncturing of Low-density Parity-check Codes[J]. *IEEE T Inform Theory*, 2004, **50**: 2824-2836. DOI: 10. 1109/TIT. 2004. 836667.

[21] Tian T, Jones C R. Construction of Rate-Compatible LDPC Codes Utilizing Information Shortening and Parity Puncturing[J]. *EURASIP J Wirel Commun Netw*, 2005, **5**: 789-795. DOI: 10. 1155/WCN. 2005. 789.