连续变量量子密钥分发多维数据协调算法

王云艳[1] 郭大波[1,2] 张彦煌[1] 王晓凯[1] 贺转玲[1]

([1] 山西大学物理电子工程学院，山西 太原 030006
[2] 山西大学量子光学与光量子器件国家重点实验室，山西 太原 030006)

摘要 数据协调是量子密钥分发的重要组成部分，特别是连续变量量子密钥分发远程化的关键环节。在 Leverrier 等关于多维协调安全性证明的基础上，给出了面向多维协调的低密度奇偶校验码(LDPC)错误校正算法，考查了该算法的最小收敛信噪比阈值，并估算出基于这种多维数据协调方案的量子密钥分发的最大密钥传输距离，经过协调效率的计算以及噪声分析估算出最大安全密钥量。算法仿真结果表明：Alice 和 Bob 之间的传输距离与分层错误校正协议(SEC)相比，从 30 km 增加到 47 km 左右，译码速度是 SEC 的 4 倍左右，密钥传输速率可以达到 8.61 kb/s。

关键词 量子光学；量子密钥分发；数据协调；多维协调；低密度奇偶校验码；稀疏矩阵

中图分类号 O431 **文献标识码** A **doi**：10.3788/AOS201434.0827002

Algorithm of Multidimensional Reconciliation for Continuous-Variable Quantum Key Distribution

Wang Yunyan[1] Guo Dabo[1,2] Zhang Yanhuang[1] Wang Xiaokai[1] He Zhuanling[1]

([1] *College of Physics and Electronic Engineering, Shanxi University, Taiyuan, Shanxi* 030006, *China*
[2] *State Key Laboratory of Quantum Optics and Quantum Optics Devices, Shanxi University, Taiyuan, Shanxi* 030006, *China*)

Abstract Data reconciliation is an important part of quantum key distribution, which is also the key step for the continuous-variable quantum key distribution (CVQKD). Based on Leverrier's prove about the security of CVQKD, a low density parity check code (LDPC) algorithm for multidimensional reconciliation is presented. The minimum convergence signal-to-noise ratio threshold of the algorithm is evaluated and the corresponding maximum key transmission distance of the CVQKD scheme is also estimated. By calculating the reconciliation efficiency and analyzing the noise, the maximum safe key capacity is further calculated. Simulation results indicate that the transmission distance between Alice and Bob increases from 30 km to 47 km, the decoding speed is 4 times of the sliced error correction (SEC) protocol, and the raw secret rate can reach 8.61 kb/s.

Key words quartum optics; quantum key distribution; reconciliation; multidimensional reconciliation; low density partity check code; sparse matrix

OCIS codes 270.5565; 270.5568; 270.5585

1 引 言

量子密钥分发(QKD)是信息安全领域的一个分支。20 世纪 80 年代，Bennet 等[1]根据量子信息的不可克隆性和测不准原理首先提出了量子密钥分发方案，被称为 BB84 协议。这种方案在理论上已证明具有无条件的绝对安全性[2]。这种以单光子为信号载波的 QKD 方案具有数据协调简单和传输距离相对较长等优点。经过 30 年的研究，该方案已经成熟，并开始商用化，国内外已建立了多个示范网络。但这种技术也日渐凸显出一些不足。在单光子

收稿日期：2014-03-10；**收到修改稿日期**：2014-04-02

基金项目：山西省基础研究项目(2014011007-2)、山西省回国留学人员科研资助项目(2014-012)、量子光学与光量子器件国家重点实验室开放基金(KF201003)

作者简介：王云艳(1987—)，女，硕士研究生，主要从事量子密钥分发方面的研究。E-mail：wangyunyan0923@126.com

导师简介：郭大波(1963—)，男，博士，副教授，主要从事量子密钥分发方面的研究。E-mail：dabo_guo@sxu.edu.cn (通信联系人)

的产生上，目前的技术还不能真正地俘获单光子，只能以衰减弱激光脉冲来模拟单光子源，只是这样产生的光源中两个光子以上的概率很小。理论上已证明，多个光子的存在会带来信息安全隐患。在单光子检测方面，尽管基于超导原理的单光子探测装置可以达到大于90%的探测效率，但探测装置需要制冷设备，装置复杂，造价昂贵，而且容易受到时间抖动[3]、大气湍流[4]和色散效应等多方面因素的影响，从而限制了其进一步的发展。

从1999年开始，学者们开始研究使用“强光”，即连续变量量子态，如相干态、压缩态、双模纠缠态和双模压缩态等为信号载波的密钥分发方案，并分别证明了各个方案的安全性[5-9]。相对而言，相干态光源因最容易获取而成为首选方案。连续变量的相干态方案具有成熟稳定的光源，可使用改进的零拍探测器[10]对量子态进行探测，不易受噪声的影响，因而具有较高的信道容量，较快的密钥传输速率，越来越多地受到国内外学者的关注。

传输距离是连续变量量子密钥分发(CVQKD)的首要问题，为此国内外学者做出了不懈的努力，2007年，Lodewyck等[11]在25 km单模光纤上演示了反向协调的高斯调制相干态的CVQKD协议[11]。2011年，上海交通大学实现了27.2 km光纤的高斯调制相干态CVQKD[12]。2013年，山西大学实现了30 km光纤四态分离调制CVQKD[13]。在高斯调制方面，研究者并没有放弃努力，Jouguet等[14]于2011～2012年在基于平衡零拍探测器的高斯调制相干态CVQKD方案的数据协调效率方面取得突破性进展，并于2013年实验上实现了80 km距离的密钥传输。

连续变量量子密钥分发的数据协调是从相关的连续量子变量中提取相同信息的过程，这一过程用到了传统通信技术。研究人员提出了基于分层错误校正协议(SEC)的逆向数据协调算法[15-18]，即对连续变量进行多电平的分层量化和编码，可在1个光脉冲上携带大于1 bit的信息。理想的最优量化是多个连续变量$\mathbb{R}^d$的矢量量化，但是在$d>1$时矢量量化复杂度大大增加。实际上只能选择$d=1$的标量最优量化，然后Bob端对多电平二进制编码后进行Slepian-Wolf(SW)式编码，形成的压缩码流通过经典授权信道送往Alice端，Alice端对多级码流进行循环迭代式的多级解码。最优基本构造码是低密度厚度奇偶校验(LDPC)码[19]，数据协调收敛最低信噪比(SNR，R_{SN})约为4 dB～5 dB，传输距离最多可达到30 km[11]。

数据协调是目前CVQKD远程化的瓶颈。当距离达到一定长度时，根据香农公式，每个脉冲的的信息量会远小于1bit，此时就不必按照SEC框架进行复杂的多级编译码过程，可直接根据每个脉冲的极性进行二值化处理，可称之为符号协调算法。

相干态的光脉冲服从中心值为0的正态分布，其特点是多数值分布在0附近，所以即便用符号协调算法也很难在信噪比较小时区分信息，数据协调过程得不到收敛，为此Lodewyck等[20]提出了多维协调方案，其核心思想是通过状态点的球面化过程，摆脱高斯随机变量数学期望值为0而不易进行符号甄别的问题，并通过旋转变换使各状态点之间的距离最大化，然而并没有给出协调过程的具体实现过程。

本文给出了一个面向多维协调的具体实现过程，以LDPC为构造码，用C语言实现了连续变量的球面化及旋转，实现了信号点之间距离的最大化，从而降低了协调收敛最小信噪比阈值，延长了通信距离，提高了密钥量。同时使用双向十字链表存贮稀疏矩阵方式存贮LDPC码的校验矩阵$\boldsymbol{H}$[21]，大大降低了空间及时间复杂度，可快速处理2×10^5连续变量的协调。

2 多维CVQKD数据协调方案

2.1 连续高斯向量的球面化

本文的远程协调过程不对连续变量进行量化处理，而是直接使用连续变量的符号进行二值化。多维数据协调的核心思想是利用多个高斯随机变量的平方和服从χ^2分布这一性质，从而摆脱多数状态点是接近于零的小数值点而难以正确二值化的困境。在进行译码之前，Alice和Bob首先把d个连续变量构成d维向量，双方可以直接按照顺序、也可以交织后组成d维向量，本文是按照顺序组合的。由于所讨论的是高斯调制的CVQKD，设Alice端发送的d维向量为$\boldsymbol{X}$，Bob端发送的d维向量为$\boldsymbol{Y}$，则有

$$\boldsymbol{Y}=\boldsymbol{X}+\boldsymbol{Z},\ \boldsymbol{X}\sim\boldsymbol{N}(0,\Sigma^2)^d,\ \boldsymbol{Z}\sim\boldsymbol{N}(0,\sigma^2)^d,\tag{1}$$

式中$\boldsymbol{N}(\cdot)$为正态分布，Σ^2为Alice端信号调制方差，σ^2为信道噪声方差。

图1为连续变量状态的球面化过程及旋转过程示意图。对于Alice端和Bob端的每组d维向量，Alice和Bob分别将$\boldsymbol{X}$和$\boldsymbol{Y}$归一化，完成如下欧氏空间$\mathbb{R}^d$到球面空间$\boldsymbol{S}^{d-1}$的映射：

$$\mathbb{R}^d \to \boldsymbol{S}^{d-1}: \boldsymbol{x} = \frac{\boldsymbol{X}}{\|\boldsymbol{X}\|}, \ \boldsymbol{y} = \frac{\boldsymbol{Y}}{\|\boldsymbol{Y}\|}, \tag{2}$$

式中 $\|\boldsymbol{X}\| = \sqrt{\langle \boldsymbol{X}, \boldsymbol{X} \rangle}$，$\|\boldsymbol{Y}\| = \sqrt{\langle \boldsymbol{Y}, \boldsymbol{Y} \rangle}$。由此 d 维信号点就完成了球面化过程。图 1 中 Alice 所发出的两个连续变量 $X_1 > 0$ 和 $X_2 > 0$，所以实际状态点为实心点，还有三种可能的状态点。图 1(a)为状态点未球面化的情形，样条纠错方案(SEC)属于此种情形，图 1(b)为状态点球面化后的情形，符号纠错方案属于这种情形；图 1(c)为状态点球面化并旋转后的情形，本文的多维协调方案属于这种情形。

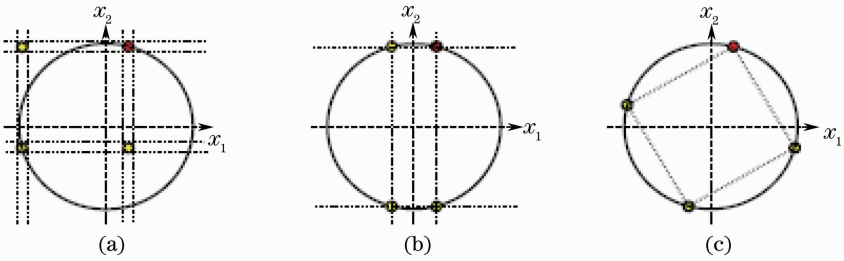

图 1 连续变量状态的球面化过程及旋转过程

Fig. 1 Spherizing and spinning processes of continuous variables

2.2 球面星座点的旋转及距离最大化

图 1(b)中信号点呈球面星座形式，但仍有某些星座点相距太近，难以甄别，可将第 2 象限和第 4 象限点作垂直旋转后可得到图 1(c)所示的多维协调方案，4 种状态的星座点之间的距离实现最大化。这种思想可扩展到 d 维，Alice 在单位球面 $\boldsymbol{S}^{d-1}$ 上随机选取 d 个最大距离星座点构成如下向量：

$$\boldsymbol{u} = \left\{\frac{-1}{\sqrt{d}}, \frac{1}{\sqrt{d}}\right\}^d. \tag{3}$$

也就是，首先选取随机二进制串，形式为 $(b_1, b_2, \cdots, b_d)$，然后进行如下操作：

$$\boldsymbol{u} = \left[\frac{(-1)^{b_1}}{\sqrt{d}}, \cdots, \frac{(-1)^{b_d}}{\sqrt{d}}\right], \tag{4}$$

计算旋转矩阵，使

$$\boldsymbol{M}(\boldsymbol{x}, \boldsymbol{u})\boldsymbol{x} = \boldsymbol{u}, \tag{5}$$

并将旋转矩阵 $\boldsymbol{M}(\boldsymbol{x}, \boldsymbol{u})$ 通过经典信道发送给 Bob 端。Bob 根据旋转矩阵和边信息进行类似球面旋转计算得到

$$\boldsymbol{v} = \boldsymbol{M}(\boldsymbol{x}, \boldsymbol{u})\boldsymbol{y}, \tag{6}$$

则

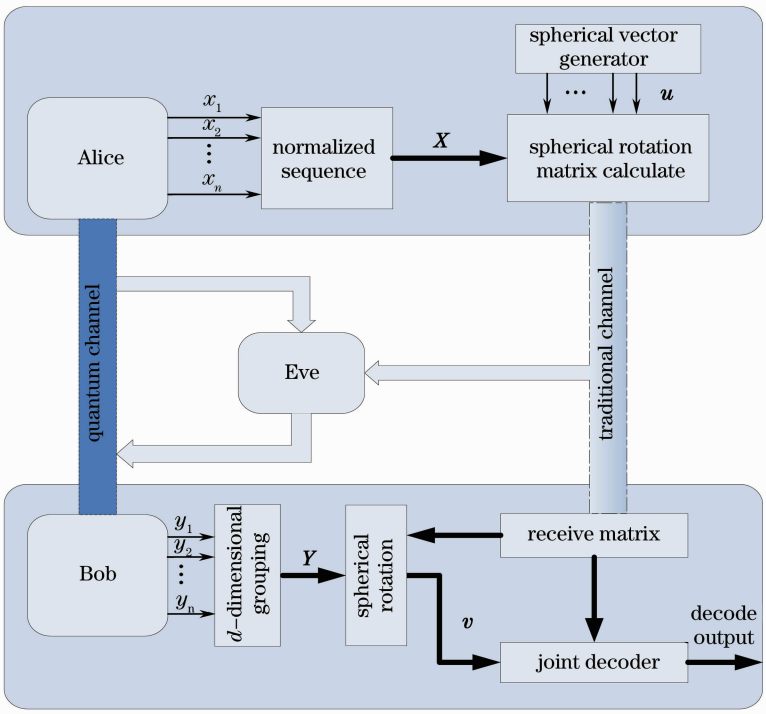

图 2 多维协调算法整体示意图

Fig. 2 Overall schematic chart of the multidimensional reconciliation algorithm

$$\boldsymbol{v}=\boldsymbol{u}+\boldsymbol{e}, \tag{7}$$

式中 $\boldsymbol{e}$ 为 $\boldsymbol{u}$ 的误差形式。

设计的多维协调算法的整体方案如图 2 所示。

通过上述旋转，搭建了将 $\boldsymbol{X}$ 变为 $\boldsymbol{u}$ 和将 $\boldsymbol{Y}$ 变为 $\boldsymbol{v}$ 的虚拟信道，即将连续变量高斯调制 CVQKD 的数据协调问题转换为离散数据协调的编解码问题，且避免了高斯分布大多数值接近于 0 而不易译码的缺点。之后就可以利用离散高斯调制的低收敛信噪比特性来延长 CVQKD 的通信距离。

2.3　旋转矩阵的计算

Leverrier 等[22]证明了当 $d=1,2,4,8$ 时旋转矩阵的存在性，并构造了一组 $d\times d$ 的正交矩阵 $(\boldsymbol{A}_1,\cdots,\boldsymbol{A}_d)$，其中 $\boldsymbol{A}_1$ 为单位矩阵，并满足 $i,j>1$ 时，

$$\{\boldsymbol{A}_i,\boldsymbol{A}_j\}=-2\delta_{i,j}\boldsymbol{I}_d, \tag{8}$$

式里 $\boldsymbol{I}_d$ 为单位矩阵，$\delta_{i,j}$ 为单位冲激函数，$\{\boldsymbol{A},\boldsymbol{B}\}$ 是反互易算子，满足 $\{\boldsymbol{A},\boldsymbol{B}\}=\boldsymbol{AB}+\boldsymbol{BA}$。由(8)式可知当 $i,j>1$ 且 $i\neq j$ 时，$\{\boldsymbol{A},\boldsymbol{B}\}=0$。

旋转矩阵 $\boldsymbol{M}(\boldsymbol{x},\boldsymbol{u})$ 的计算方法如下：

$$\boldsymbol{M}(\boldsymbol{x},\boldsymbol{u})=\sum_{i=1,\cdots,d}a_i(x,u)\boldsymbol{A}_i, \tag{9}$$

式中 $[a_1(x,u),\cdots,a_d(x,u)]$ 是 $\boldsymbol{u}$ 在正交基 $(\boldsymbol{A}_1x,\boldsymbol{A}_2x,\cdots,\boldsymbol{A}_dx)$ 上的坐标，$(\boldsymbol{A}_1,\cdots,\boldsymbol{A}_d)$ 已经确定，因此计算 $\boldsymbol{M}(\boldsymbol{x},\boldsymbol{u})$ 的过程就转化为计算 $[a_1(x,u),\cdots,a_d(x,u)]$。对于任意的 $x\in\boldsymbol{S}^{n-1}$，$[\boldsymbol{A}_1x,\cdots,\boldsymbol{A}_dx]$ 为可逆矩阵，则列向量 $[a_1(x,u),\cdots,a_d(x,u)]^{\mathrm{T}}$ 可以表示为

$$[a_1(x,u),\cdots,a_d(x,u)]^T=[\boldsymbol{A}_1x,\cdots,\boldsymbol{A}_ix]^{-1}\boldsymbol{u}. \tag{10}$$

3　多维协调的二进制 LDPC 译码过程

3.1　初始概率的计算

译码成功与否与初始概率有很大的关系，计算信道传递给变量节点的初始概率是 LDPC 译码的第一步，也是最关键的步骤。用 LDPC 码进行纠错译码时，每个二进制码符号就是一个比特，因此信道传递给变量节点的初始概率的计算就是求条件概率，即在向量 $\boldsymbol{v}$ 已知的情况下，求向量 $\boldsymbol{u}$ 中对应位的概率。本文中向量 $\boldsymbol{u}$ 中二进制串形式分别用 0 和 1 表示，旋转映射到球面相应的也就是分别计算 $-1/\sqrt{d}$ 或 $1/\sqrt{d}$ 的概率。要计算初始概率，林毅等[23]给出了计算 $\boldsymbol{u}$ 和 $\boldsymbol{v}$ 之间的关系。

这里计算一个 d 维向量的各个分量：

$$P_i(s)=P_{\mathrm{r}}[u_i=u(s)\mid v_i]=K\exp\left\{\frac{-[\|\boldsymbol{Y}\|v_j-\|\boldsymbol{X}\|u(s)]^2}{2\sigma^2}\right\}\Big/(2\pi\sigma^2)^{1/2}, \tag{11}$$

式中 P_i 表示概率计算，P_{r} 表示后验概率的计算，u_i 和 v_i 分别为向量 $\boldsymbol{u}$ 和 $\boldsymbol{v}$ 的第 i 个分量，$s\in\{0,1\}$，$u(s)=\dfrac{(-1)^s}{\sqrt{d}}$，$K$ 是归一化因子，使信道传递给变量节点的初始概率 $P_i(0)+P_i(1)=1$。

3.2　基于 LDPC 的解码过程

对数似然比置信传播(LLR BP)译码算法与置信传播(BP)算法的区别是 LLR BP 算法的概率消息用似然比表示，这样乘法运算过程就可以变为加法运算过程，可以大大地降低计算复杂度。下面结合上述多维协调算法简要介绍对数 LDPC 码似然比译码。

$r_{ji}(b)\left(b=\dfrac{1}{\sqrt{d}}\text{ 或}\dfrac{-1}{\sqrt{d}}\right)$ 是从校验节点 j 到变量节点 i 的外部信息概率，$q_{ij}(b)\left(b=\dfrac{1}{\sqrt{d}}\text{ 或}\dfrac{-1}{\sqrt{d}}\right)$ 是从变量节点 i 到校验节点 j 的信息概率，q_i 和 p_i 分别表示某一变量节点和校验节点，$R(j)$ 是与校验节点 j 相连的所有变量节点的集合，$C(i)$ 是与变量节点 i 相连的所有校验节点的集合，$C_i\backslash j$ 为除 j 外与变量节点 i 相连的校验节点的集合，$R_j\backslash i$ 为除 i 外与校验节点相连的变量节点的集合[24]。

LLR-BP 算法的步骤如下(其中迭代次数用消息符号的上标表示)：

1)信道初始化

$$L^{(0)}(q_{ij})=\mathrm{lb}\frac{P_i(0)}{P_i(1)}=\mathrm{lb}\frac{\left\{u_i=\dfrac{1}{\sqrt{d}}\mid v_i\right\}}{\left\{u_i=\dfrac{-1}{\sqrt{d}}\mid v_i\right\}}, \tag{12}$$

式中 $L^{(0)}$ 为信道传递给变量节点的初始概率似然比。

2) 迭代过程

① 校验节点的处理更新，

$$\tanh\left[\frac{1}{2}L^{(l)}(r_{ji})\right]=\prod_{i\in R_j\backslash i}\tanh[L^{(l-1)}(q_{ji})], \tag{13}$$

式中 $L^{(l)}$ 为经过 l 次迭代后校验节点传向变量结点的消息。

② 变量节点的处理更新，

$$L^{(l)}(q_{ji})=L(P_i)+\sum_{j\in C_i\backslash j}L^{(l)}(r_{ji}). \tag{14}$$

③判决处理，

$$L^{(l)}(q_i)=L(P_i)+\sum_{j\in C_i}L^{(l)}(r_{ji}),\tag{15}$$

$$\hat{C}_i=\begin{cases}1, & L^{(l)}(q_i)<0\\ 0, & L^{(l)}(q_i)>0\end{cases}.\tag{16}$$

3）迭代控制

在满足 $\boldsymbol{H}\hat{\boldsymbol{C}}^{\mathrm{T}}=0$（$\boldsymbol{H}$ 为校验矩阵，$\hat{\boldsymbol{C}}$ 为判决处理后解译的码字）或者达到最大迭代次数时，运算结束，译码输出，若不满足则返回步骤 1）。

4 噪声分析及安全密钥量估算

噪声分析和安全密钥量的计算是连续变量量子密钥分发系统的一个重要步骤。只有在密钥量足够大时，发送端 Alice 和接收端 Bob 才可以安全通信。相干攻击是目前量子攻击方法中最强的一种，其中集体攻击是相干攻击的代表。下面主要对集体攻击方法进行理论上的推理和估算。

信息论给出 Alice 和 Bob 能否安全通信是由 Alice 和 Bob 的互信息量 I_{AB} 和 Alice 或者 Bob 可能泄露给 Eve 的信息量 I_{AE} 或者 I_{BE} 之间的大小关系决定的，多维 CVQKD 数据协调方案是量子密钥分发数据协调的逆向协调，需要满足 $I_{\mathrm{AB}}>I_{\mathrm{BE}}$。下面整个系统的噪声功率都是以真空噪声功率 N_0 为单位进行的。

Alice 输出端的噪声由两部分构成，即

$$\chi_{\mathrm{tot}}=\chi_{\mathrm{line}}+\chi_{\mathrm{hom}}/T,\tag{17}$$

式中

$$\chi_{\mathrm{line}}=1/T-1+\varepsilon,\tag{18}$$

$$\chi_{\mathrm{hom}}=(1+\upsilon_{\mathrm{el}})/\eta-1.\tag{19}$$

其中，$T<1$ 为量子通道参量系数，ε 为传输过程中的额外噪声，η 为零拍探测器的探测效率，υ_{el} 为探测器系统引入的噪声。(18)式表示 Bob 端等效到 Alice 端的信道噪声，倘若不考虑 Alice 端的各种器件引入的衰减，Bob 端的输入噪声功率可表示为 $1+T\varepsilon$。(19)式表示 Bob 端仪器噪声等效到 Alice 端的噪声，Bob 端利用平衡零拍探测器对每个态的正交分量进行随机测量。

此时 Alice 和 Bob 的互信息可以用香农信道容量公式计算得

$$I_{\mathrm{AB}}=\frac{1}{2}\mathrm{lb}\frac{V_{\mathrm{B}}}{V_{\mathrm{B\backslash A}}}=\frac{1}{2}\mathrm{lb}\left(1+\frac{V_A}{1+\chi_{\mathrm{tot}}}\right)=\frac{1}{2}\mathrm{lb}\frac{V+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}},\tag{20}$$

式中主要考虑到 Bob 端的功率，V_{B} 为信号功率，V_{A} 为 Alice 端信号功率，$V=V_{\mathrm{A}}+1$，条件方差 $V_{\mathrm{B\backslash A}}$ 表示在 Alice 功率已知条件下 Bob 端的噪声功率。

本文只叙述集体攻击中的多维逆向协调过程。逆向协调时 Eve 能从 Bob 获取的信息量的上限 χ_{BE} 取决于 Holevo 限，即满足

$$\chi_{\mathrm{BE}}=S(\boldsymbol{\rho}_{\mathrm{E}})-\int\rho(\chi_{\mathrm{B}})S(\boldsymbol{\rho}_{\mathrm{E}}^{\chi_{\mathrm{B}}})\mathrm{d}\chi_{\mathrm{B}},\tag{21}$$

式中 $\boldsymbol{\rho}_{\mathrm{E}}$ 为 Eve 的密度矩阵，而 $\boldsymbol{\rho}_{\mathrm{E}}^{\chi_{\mathrm{B}}}$ 为 Eve 相对于 Bob 的条件密度矩阵，$\rho(\chi_{\mathrm{B}})$ 表示 Bob 端接收信号的概率分布[25]，S 为冯•诺伊曼熵。若 ρ 服从高斯分布，则冯•诺伊曼熵[26] $S(\rho_{\mathrm{E}})$ 亦可表示为

$$S(\rho_{\mathrm{E}})=\sum_i G\left(\frac{\lambda_i-1}{2}\right),\tag{22}$$

式中 $G(x)=(x+1)\mathrm{lb}(x+1)-x\mathrm{lb}\,x$，$\lambda_i$ 为高斯态协方差矩阵的特征值。通过解征值方程可得

$$\lambda_{1,2}^2=\frac{1}{2}(A\pm\sqrt{A^2-4B}),\tag{23}$$

式中 $A=V^2(1-2T)+2T+T^2(V+\chi_{\mathrm{line}})^2$，$B=T^2\cdot(V_{\chi_{\mathrm{line}}}+1)^2$。同样可以得到

$$\lambda_{3,4}^2=\frac{1}{2}(C\pm\sqrt{C^2-4D}),\tag{24}$$

式中 $C=[V\sqrt{B}+T(V+\chi_{\mathrm{line}})+A\chi_{\mathrm{hom}})/T(V+\chi_{\mathrm{tot}})$，$D=\sqrt{B}(V+\sqrt{B}\chi_{\mathrm{hom}})/T(V+\chi_{\mathrm{tot}})$。

通过(24)式可以得到

$$\chi_{\mathrm{BE}}=G\left(\frac{\lambda_1-1}{2}\right)+G\left(\frac{\lambda_2-1}{2}\right)-G\left(\frac{\lambda_3-1}{2}\right)-G\left(\frac{\lambda_4-1}{2}\right).\tag{25}$$

因此在集体攻击下采用逆向协调时，若已知协调效率 β，则 Alice 和 Bob 可以获得的安全密钥为

$$\Delta I=\beta I_{\mathrm{AB}}-\chi_{\mathrm{BE}}.\tag{26}$$

取 $V_{\mathrm{A}}=18.5$，$\varepsilon=0.01$，$T=0.151$，$\eta=0.606$，$\upsilon_{\mathrm{el}}=0.041$。

5 数值仿真结果及分析

使用的硬件平台是 CPU 为 Inter Xeon E5620 2.4 GHz 和 32 G 内存的双核服务器，选择码率为 0.5，码长分别为 10^3、10^4、10^5 和 10^6，共 10 个分组进行统计，译码最大迭代次数为 100，实验数据统计如表 1 所示。

由表 1 可知在四维协调算法下，码长为 10^3、10^4、10^5、10^6 时，误码率收敛信噪比 R_{SN} 分别为 2.8 dB、1.9 dB、1.5 dB、1.5 dB。在八维协调算法下，R_{SN} 分别为 1.9 dB、1.4 dB、1.3 dB、1.2dB。随着码长的增加，译码性能增强，平均迭代次数（Ave_inter）增加，译码时间（Per_time）也随之增加。由表 1 可见，

八维协调算法译码性能高于四维协调算法。

实验结果验证了 LDPC 码随着码长的增加性能加强，但当码长增加到一定值时，其性能也会达到瓶颈。选择 10^5 数量级作了进一步研究。表 2 比较了在码长为 2×10^5 时不同码率的收敛情况。

表 1　四维及八维协调算法实验结果

Table 1　Experimental results of four and eight dimensional reconciliations

	Four dimensional reconciliation			Eight dimensional reconciliation		
Length	R_{SN}/dB	Ave_inter	Per_time/s	R_{SN}/dB	Ave_inter	Per_time/s
10^3	2.8	22.4	0.0880	1.9	37.4	0.0207
10^4	1.9	35.7	0.2778	1.4	39.1	0.2764
10^5	1.5	69.0	6.9455	1.3	43.1	4.3298
10^6	1.5	75.1	112.45	1.2	67.7	93.9985

表 2　码率不同时四维及八维协调算法实验结果

Table 2　Experimental results of four and eight dimensional reconciliations at different rates

	Four dimensional reconciliation				Eight dimensional reconciliation			
Rate	R_{SN}/dB	Ave_inter	Per_time/s	Speed /(kb/s)	R_{SN}/dB	Ave_inter	Per_time/s	Speed /(kb/s)
0.4	1.1	73.1	17.715	11.28	0.8	54.7	16.824	11.89
0.5	1.5	72.8	15.558	12.86	1.2	53.6	13.809	14.48
0.6	2.2	61.8	11.063	18.08	1.7	52.4	10.607	18.86
0.7	3.1	52.3	9.4540	21.16	2.3	51.4	10.344	19.33
0.8	4.3	47.3	8.2250	24.32	3.3	51.3	8.7771	22.79
0.9	6.3	38.4	6.1295	32.63	4.8	47.7	8.2322	24.29

由表 2 可以看到，在码长为 2×10^5 时，八维协调算法的 R_{SN} 比四维协调算法低，码率增大，收敛信噪比随之增大，Ave_inter 也降低，Per_time 也不断减少，译码速率加快，最大可以达到 32.63 kb/s。表 3 为不同码率时的密钥生产量。

表 3　码率不同时四维及八维协调算法密钥量实验结果

Table 3　Experimental results about rate bit of four and eight dimensional reconciliations at different rates

Rate	R_{SN}/dB	β/%	Rate bit /(kb/s)	Distance /km	R_{SN}/dB	β/%	Rate bit /(kb/s)	Distance /km
0.2	0.5	68.38	−55.99	47.5	0.4	82.40	−21.83	48
0.25	0.55	79.08	−29.92	47.25	0.5	85.48	−14.34	47.5
0.3	0.6	88.49	−7.00	47	0.55	94.89	8.61	47.25
0.35	0.7	91.44	0.19	46.5	0.7	91.44	0.19	47.5
0.4	1.1	74.74	−40.49	44.5	0.8	94.34	7.26	47

由表 3 可知，四维协调算法的协调效率明显地低于八维协调算法，四维协调算法只有在码率为 0.35时可以得到 0.19 kb/s 的安全密钥速率，八维协调算法在码率为 0.3 时协调效率可以达到 94.89%，可以提取到 8.61 kb/s 安全密钥，在 0.4 时协调效率达到94.34%，可以提取到 7.26 kb/s 的安全密钥。这些结果和文献[27]中的变化基本符合，且码率较小。

由此计算得到的安全距离可以达到 47 km 左右，并且只有在码率大于 90.0%才可以提取到密钥，密钥量为负值表明通信中存在问题，即 Eve 窃听的信息量大于 Alice 和 Bob 之间的互信息量，导致 Alice 和 Bob 无法安全通信。

协调效率 β 的计算式[28]为

$$\beta=\frac{R}{I_{AB}},\tag{27}$$

式中 R 表示码率，$I_{AB}=\frac{1}{2}\mathrm{lb}(1+R_{SN})$。

6　结　论

对基于相干态高斯调制的 CVQKD 的多维数据协调进行了仿真，在对连续变量进行球面化及旋转操作后，利用 LDPC 进行编解码。采用所提出的四维和八维协调算法，可在很小的收敛信噪比时实现多维数据协调，通信距离达到 47 km 左右，比 SEC 扩展了约 20 km。在连续变量分组数为 2×10^5 时，速度是 SEC 的 4 倍左右。在码率很低时可以提取到安全密钥，性能得到很大的提高，接近于国际水平。

有待提高的是在码率较低时降低收敛信噪比以及提高协调效率，下一步将从密度进化的角度优化 $\boldsymbol{H}$ 矩阵度分布，进一步降低信噪比要求。

参 考 文 献

1 Charles H Bennet, Gilles Brassard. Quantum cryptography: publikey distribution and coin tossing [C]. Proceedings of International Conference on Computers, Systems & Signal Processing, 1984.

2 Ma Ruilin. Quantum Cryptography Communication [M]. Beijing: Science Press, 2006.
马瑞霖. 量子密码通信[M]. 北京:科学出版社, 2006.

3 Chen Shuai, Wang Jindong, Zhong Pingping, *et al*.. Influence of time jitter on quantum bit error rate of pahse-coding quantum key distribution system [J]. Acta Optica Sinica, 2011, 31(7): 0727001.
陈 帅，王金东，钟平平，等. 时间抖动对相位编码量子密钥分发系统量子误码率的影响[J]. 光学学报, 2011, 31(7): 0727001.

4 Zhao Guhao, Zhao Shanghong, Yao Zhoushi, *et al*.. Effect of the pulse broadening caused by atmosphere on staellite based quantum key distribution [J]. Acta Optica Sinica, 2012, 32(11): 1127001.
赵顾颢，赵尚弘，幺周石，等. 大气导致的脉冲展宽对星载量子密钥分发的影响[J]. 光学学报, 2012, 32(11): 1127001.

5 Timothy C Ralph. Continuous variable quantum cryptography [J]. arXiv: quant-ph// 9907073, 1999.

6 Mark Hillery. Quantum cryptography with squeezed states [J]. Phys Rev A, 2000, 61(2): 022309.

7 Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, *et al*.. Quantum key distribution using gaussian-modulated coherent states [J]. Nature, 2003, 421(6920): 238－241.

8 Frédéric Grosshans. Collective attacks and unconditional security in continuous variable quantum key distribution [J]. Phys Rev Lett, 2005, 94(2): 020504.

9 Gong Lihua, Song Hanchong, He Chaosheng, *et al*.. A continuous variable quantum deterministic key distribution based on two-mode squeezed states [J]. Physica Scripta, 2014, 89(3): 035101.

10 Wang Jinjing, Jia Xiaojun, Peng Kunchi. Improvement of balanced homodyne detector [J]. Acta Optica Sinica, 2012, 32(1): 0127001.
王金晶，贾晓军，彭堃墀. 平衡零拍探测器的改进[J]. 光学学报, 2012, 32(1): 0127001.

11 Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, *et al*.. Quantum key distribution over 25 km with an all-fiber continuous-variable system [J]. Phys Rev A, 2007, 76(4): 042305.

12 Wen Chao Dai, Yuan Lu, Jun Zhu, *et al*.. An integrated quantum secure communication system [J]. Science China Information Sciences, 2011, 54(12): 2578－2591.

13 Wang Xuyang, Bai Zengliang, Wang Shaofeng, *et al*.. Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise [J]. Chin Phys Lett, 2013, 30(1): 010305.

14 Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, *et al*.. Experimental demonstration of long-distance continuous-variable quantum key distribution [J]. Nature Photonics, 2013, 7: 378－381.

15 Gilles Van Assche, Jean Cardina, Nicolas J Cerf. Reconciliation of a quantum distributed Gaussian key [J]. IEEE Transactions on Information Theory, 2004, 50(2): 394－400.

16 Matthieu Bloch, Andrew Thangara, Steven W McLaughlin, *et al*.. LDPC-based Gaussian key reconciliation [C]. IEEE Information Theroy Workshop, 2006. ITW′06 Punta del Este, 2006. 116－120.

17 Guo Dabo, Zhang Ning, Liu Gang. Reconciliation of quantum Gaussian distributed key based on Turbo codes [J]. Acta Sinica Quantum Optica, 2013, 19(1): 32－38.
郭大波，张 宁，刘 纲. 基于Turbo码的量子高斯密钥分发的数据协调[J]. 量子光学学报, 2013, 19(1): 32－38.

18 Guo Dabo, Liu Gang, Zhang Ning, *et al*.. Reverse reconciliationa of quantum Gaussian distributed key [J]. Acta Sinica Quantum Optica, 2013, 19(3): 219－226.
郭大波，刘 纲，张 宁，等. 量子高斯密钥分发的逆向数据协调[J]. 量子光学学报, 2013, 19(3): 219－226.

19 Robert Gallager. Low-density parity-check codes [J]. Information Theory, IRE Transactionon, 1962, 8(1): 21－28.

20 Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, *et al*.. Quantum key distribution over 25 km with an all-fiber continuous-variable system [J]. Phys Rev A, 2007, 76(4): 042305.

21 Guo Dabo, Zhang Yanhuang, Wang Yunyan. Performance optimization for the reconciliation of Gaussian quantum key distribution [J]. Acta Optica Sinica, 2014, 34(1): 0127001.
郭大波，张彦煌，王云艳. 高斯量子密钥分发数据协调的性能优化[J]. 光学学报, 2014, 34(1): 0127001.

22 Anthony Leverrier, Romain Alléaume, Joseph Boutros, *et al*.. Multidimensional reconciliation for a continuous-variable quantum key distribution [J]. Phys Rev A, 2008, 77(4): 042325.

23 Lin Yi, He Guangqiang, Zeng Guihua. The application of LDPC codes in the mulitidimensional reconciliation of quantum key distribution [J]. Acta Sinica Quantum Optica, 2013, 19(2): 116－121.
林 毅，何广强，曾贵华. LDPC码在量子密钥分配多维协商算法中的应用[J]. 量子光学学报, 2013, 19(2): 116－121.

24 Yuan Dongfeng, Zhang Haigang. The Theory and Application of LDPC Code [M]. Beijing: Posts & Telecom Perss, 2008. 75－79.
袁东风，张海刚. LDPC码理论与应用[M]. 北京：人民邮电出版社, 2008. 75－79.

25 Li Kang. Study on Continuous Variable Quantum Key Distribution [D]. Beijing: Beijing University of Post and Telecommunications, 2009. 32－43.
李 康. 基于连续变量的量子密钥分发研究[D]. 北京：北京邮电大学, 2009. 32－43.

26 Miguel Navascués, Antonio Acín. Security bounds for continuous variables quantum key distribution [J]. Phys Rev Lett, 2005, 94(2): 020505.

27 Anthony Leverrier, Philippe Grangier. Continuous-variable quantum key distribution protocols with a discrete modulation [J]. arXiv: 1002.4083, 2010.

28 Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier. Long-distance continuous variable quantum key distribution with a Gaussian modulation [J]. Phys Rev A, 2011, 84(6): 062317.

栏目编辑：史 敏