连续变量量子密钥分发多维数据协调算法优化

窦 磊 郭大波 王晓凯
山西大学物理电子工程学院, 山西 太原 030006

摘要 针对连续变量量子密钥分发(CVQKD)通信距离较短的问题,在多维数据协调方案的基础上,利用连续密度进化和差分进化方法,设计出优质度数分布的低密度奇偶校验(LDPC)码,并提出 LDPC 码码字重复方法,进一步提高多维数据协调的效率,有效地降低了收敛信噪比,延长了信息传输距离。实验仿真结果表明:在分组码长为 10^6 时,收敛信噪比能够降低至 −6 dB 以下,协调效率可达 90.27%,提取到的安全密钥量为 0.22 kb/s,信息传输距离超过 80 km,该方法可有效延长 CVQKD 系统的通信距离。

关键词 量子光学; 连续变量量子密钥分发; 多维数据协调算法; 连续密度进化; 差分进化; 重复码字
中图分类号 O431.2 **文献标识码** A
doi: 10.3788/AOS201636.0927001

Optimizing Multidimensional Reconciliation Algorithm for Continuous-Variable Quantum Key Distribution

Dou Lei Guo Dabo Wang Xiaokai
College of Physics and Electronic Engineering, Shanxi University, Taiyuan, Shanxi 030006, *China*

Abstract For the problem of short communication distance in continuous-variable quantum key distribution (CVQKD) protocol and on the basis of multidimensional reconciliation scheme, the low-density parity-check (LDPC) codes with good degree distribution are designed using a continuous density evolution and differential evolution method. The method of repeating LDPC codes is proposed as well, which further improves the efficiency of multidimensional data coordination, effectively reduces the convergence signal-to-noise ratio threshold and extends the secure range of communication distance. The simulation results indicate that when the block length is 10^6, the convergence signal-to-noise ratio can be less than −6 dB, and the data reconciliation efficiency can achieve 90.27%. The amount of the extracted secure secret key is about 0.22 kb/s, and the secure range of communication distance exceeds to 80 km, which means the distance can be effectively extended in CVQKD system.

Key words quantum optics; continuous-variable quantum key distribution; multidimensional reconciliation algorithm; continuous density evolution; differential evolution; repetition codes
OCIS codes 270.5565; 270.5568; 270.5585

1 引 言

量子保密通信作为信息安全的一个新兴领域,受到了人们的广泛关注。为了保证量子保密通信的稳定性和安全性,研究人员提出了量子密钥分发(QKD)的方法。20 世纪 80 年代,Bennett[1] 首先提出了无条件绝对安全的 QKD 方案,被称为 BB84 协议。在此协议基础上,学者们利用离散变量(即单光子)开发了离散变量量子密钥分发(DVQKD)系统,但是这种技术受到单光子探测器探测效率的限制。2002 年,学者们又提出了基于连续变量的量子密钥分发方案,称为连续变量量子密钥分发(CVQKD)协议[2],该协议不仅摆脱了之前探测效率低的限制,而且具有信道容量大的优势,因此具有更高的密钥传输速率,已得到学界的广泛

收稿日期: 2016-03-29; **收到修改稿日期**: 2016-04-28
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)、山西省国际科技合作项目(2014081027-1)
作者简介: 窦 磊(1990—),男,硕士研究生,主要从事量子密钥分发方面的研究。E-mail: doulei1722@126.com
导师简介: 郭大波(1963—),男,博士,副教授,硕士生导师,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)

认可。

然而 CVQKD 在后期信息处理中也存在数据协调的问题。在两种 QKD 方案中，由于量子信道噪声和可能的窃听者 Eve 的干扰，Alice 和 Bob 在通信中会得到不一致但相关的离散变量或者连续变量序列。双方从相关的序列中，提取完全一致的信息过程称为数据协调[2]，提取出信息后再通过私密放大，即可提取出密钥。相对于 DVQKD，CVQKD 的数据协调需要较大的信道信噪比才能收敛，因此其通信距离大大低于 DVQKD 方案。

2003 年，Assche 首先提出了基于分层纠错协议(SEC)的逆向数据协调算法，由于在低信噪比下误码平台很大，收敛信噪比仅在 4.9 dB 左右[3]，导致安全传输距离被限制在 25 km[4-5]。之后提出的符号协调算法因为在低信噪比时不能有效地区分信息，协调过程得不到收敛，限制了 CVQKD 的安全传输距离。2008 年，Leverrier 等[6]提出了多维数据协调方法，其安全传输距离超过了 50 km。2011 年，Jouguet 等[7-8]提出的非高斯调制多维数据协调方案，从理论上证明了其安全传输距离可达到 150 km 以上。2013 年，Jouguet 等[7,9]实验研究得到在 80 km 安全传输距离下，传输密钥量达到每秒几百比特。自此以后，多维数据协调算法一直被认为是 CVQKD 协议中最优的数据协调算法。

在国内，2014 年，王云艳等[10]在 60 km 安全距离下实现了 8 kb/s 的密钥传输率。本文在此基础上继续探索降低多维数据协调算法收敛信噪比的方法，使收敛信噪比低于－6.0 dB，延长安全传输距离至80 km。算法实施过程中，1)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；2)通过参考连续密度进化[11]和差分进化方法[12]，经过大量实验数据对比，设计出在一系列低码率、优质度数分布的非规则低密度奇偶校验(LDPC)码，并将其运用到多维数据协调算法中，使得收敛信噪比达到－4 dB 左右，延长安全传输距离至 70 km 左右；3)根据二进制输入高斯白噪声信道(BIAWGNC)的特点，提出 LDPC 码重复码字的优化方法，重复 k 倍码字，使得收敛信噪比与 LDPC 码率呈比例下降到－6 dB，提取到安全密钥量为 0.22 kb/s，从而将连续变量量子密钥(CVQK)的安全传输距离提高至 80 km 以上，实现了 CVQKD 的远程化。

2　多维 CVQKD 数据协调方案

2.1　数据协调的安全性分析

在 CVQKD 中，一个非常重要的过程就是数据协调(校验)。只有通过数据校验过程，才能提取安全密钥。Alice 和 Bob 通过经典信道从双方相关的密钥信息中提取一致的安全密钥，并且保证将尽可能少的信息泄露给 Eve。定义理论上的密钥速率(密钥量)为(以正向协调举例)

$$K_{\mathrm{th}}=I(x,y)-\chi(x,E),\tag{1}$$

式中 $I(x,y)$为 Alice 端所发序列 x 与 Bob 端所接收的序列 y 的互信息量，$\chi(x,E)$为窃听者 Eve 所接收的序列 E 与 Alice 端所发序列 x 的 Holevo 信息量。在 CVQKD 中，实际提出的数据协调过程的效率达不到 100%，因此实际数据协调方案中的密钥速率通常可表示为

$$K_{\mathrm{real}}=\beta I(x,y)-\chi(x,E),\tag{2}$$

式中 β 为数据协调的效率。$K_{\mathrm{real}}>0$ 表示通信过程是安全的，因此较高协调效率对于保证安全密钥速率 K_{real}是十分重要的。在传统的一维协调方案中，要获得一个好的数据协调效率 β 必须使收敛信噪比 S_{NR}满足 $S_{\mathrm{NR}}\geqslant 1$[3,13-14]，因此限制了 CVQKD 的安全传输距离。为了解决这一问题，Leverrier 等[6]提出了多维数据协调方案。

2.2　多维数据协调方案

图 1 为多维协调算法示意图，左边为量子传输信道。

1) Alice 首先将 d 个连续高斯变量构成 d 维向量 $\boldsymbol{X}$，Bob 作为接收者接收 d 维向量 $\boldsymbol{Y}$，信道传输模型为 $\boldsymbol{Y}=t\boldsymbol{X}+\boldsymbol{Z}$，$t$ 表示传输中的损耗。为简化分析，可假定量子信道传输没有损失，即 $t=1$，则有

$$\boldsymbol{Y}=\boldsymbol{X}+\boldsymbol{Z},\ \boldsymbol{X}\sim N(0,\Sigma^2)^d,\ \boldsymbol{Z}\sim N(0,\sigma^2)^d,\tag{3}$$

式中～$N(0,*)$表示服从高斯分布，Σ 为 Alice 端信号调制方差，通常设为 1，σ 为信道噪声方差。

2) 将发送向量和接收向量球面化，与算法示意图中的第二列对应：

$$\begin{cases} \boldsymbol{x}=\boldsymbol{X}/\|\boldsymbol{X}\| \\ \boldsymbol{y}=\boldsymbol{Y}/\|\boldsymbol{Y}\| \end{cases}, \tag{4}$$

式中 $\|\boldsymbol{X}\|=\sqrt{\langle \boldsymbol{X},\boldsymbol{X}\rangle}$，$\|\boldsymbol{Y}\|=\sqrt{\langle \boldsymbol{Y},\boldsymbol{Y}\rangle}$。

通过归一化操作将欧氏空间$\mathbb{R}^d$向量映射到黎曼空间中的球面空间$\mathbb{S}^{d-1}$向量，这一过程将某些近原点的信号点拉到等距的球面上，减少了解码过程中近零点带来的误码概率。

3）将球面上信号点之间距离最大化，与算法示意图中的最后两列对应。Alice 在单位球面$\mathbb{S}^{d-1}$上随机选取 d 维向量 $\boldsymbol{u}\in\left\{\frac{-1}{\sqrt{d}},\frac{1}{\sqrt{d}}\right\}^d$，计算旋转矩阵 $\boldsymbol{r}=\boldsymbol{u}\cdot\boldsymbol{x}^{-1}$，并通过公开信道发送给 Bob，Bob 端同样利用这个矩阵计算出 $\boldsymbol{v}=\boldsymbol{r}\cdot\boldsymbol{y}$。这一过程可以看作一个输入为 $\boldsymbol{u}$，输出为 $\boldsymbol{v}$ 的虚拟 BIAWGNC 产生过程，这意味着在物理信道中 d 个连续变量被映射为虚拟的 BIAWGNC 中的 d 个近似副本，并且在虚拟的 BIAWGNC 中进行纠错，最后得到实际密钥。

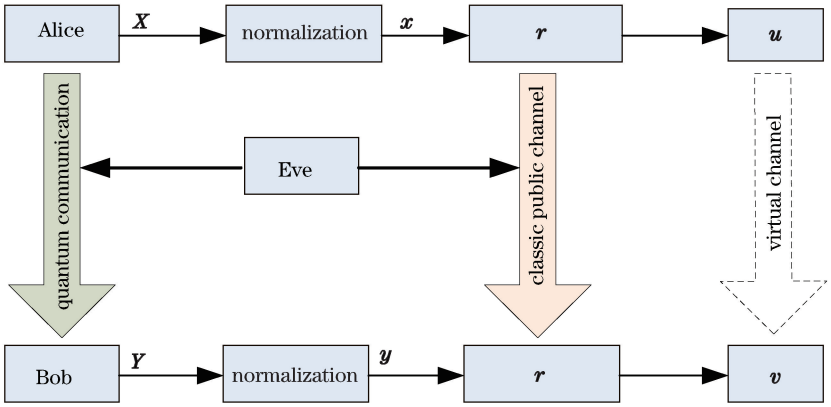

图 1　多维协调算法整体示意图

Fig. 1　Schematic diagram of multidimensional reconciliation algorithm

2.3　多维数据协调的噪声分析

系统中存在的噪声 $\boldsymbol{w}$ 为

$$\boldsymbol{w}=\boldsymbol{v}-\boldsymbol{u}=\boldsymbol{r}\cdot\boldsymbol{y}-\boldsymbol{r}\cdot\boldsymbol{x}=\boldsymbol{u}\cdot\boldsymbol{x}^{-1}\cdot(\boldsymbol{x}+\boldsymbol{z})-\boldsymbol{u}=\boldsymbol{u}\cdot\boldsymbol{x}^{-1}\cdot\boldsymbol{z}=\boldsymbol{r}\cdot\boldsymbol{z}, \tag{5}$$

式中 $\boldsymbol{u}$，$\boldsymbol{v}$，$\boldsymbol{w}$ 分别为 d 维欧式空间的向量 $\boldsymbol{X}$，$\boldsymbol{Y}$，$\boldsymbol{Z}$ 映射到 d-1 维球面空间的向量。由于 $\boldsymbol{r}$ 仅表示在单位圆上的一个旋转操作，所以 $\boldsymbol{w}$ 的各个分量和 $\boldsymbol{z}$ 的各个分量满足相同的概率分布，即 $\boldsymbol{w}\sim N(0,\sigma^2)^d$。当 Alice 将 $\boldsymbol{x}$ 的范数 $\|\boldsymbol{X}\|$ 传送给 Bob 时，这个信道被认为是携带边信息的衰减信道[15]，衰减系数为 $\|\boldsymbol{X}\|$，$\|\boldsymbol{X}\|$ 服从 $\chi(d)$分布。当 d 趋于无穷大时，$\chi(d)$分布近似于 Dirac 分布，因此应尽可能获得最高的欧氏空间 $\mathbb{R}^d$ 以获得退化的衰减信道（其衰减系数为 1），即 BIAWGNC。但是，算法所需的除法运算符只存在于 $d=1,2,4,8$ 维的欧氏空间[7]，因此，不能在任意维数的欧氏空间使用上述算法，8 维数据协调算法是目前所能达到的最高维数据协调算法。在 $d=1,2,4,8$ 时，$\boldsymbol{r}$ 可表示为

$$\boldsymbol{r}=\sum_1^d a_i(x,u)\boldsymbol{A}_i, \tag{6}$$

式中$[a_1(x,u),a_2(x,u),\cdots,a_d(x,u)]$为 $\boldsymbol{u}$ 在正交基$(\boldsymbol{A}_1x,\boldsymbol{A}_2x,\cdots,\boldsymbol{A}_dx)$上的坐标。$(\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_d)$在实际协调过程中是确定的。

3　非规则 LDPC 码参数的优化

LDPC 码是通过校验矩阵定义的线性分组码，所以构造 LDPC 码即对应构造一个稀疏校验矩阵 $\boldsymbol{H}$。LDPC 码可以用 Tanner 图表示，Tanner 图是一种双向图，可以用 $\boldsymbol{G}=\{(\boldsymbol{V},\boldsymbol{E})\}$表示，其中 $\boldsymbol{V}$ 是节点的集合，$\boldsymbol{V}=\boldsymbol{V}_b\cup\boldsymbol{V}_c$ 对应维数为 $m\times n$ 的校验矩阵；$\boldsymbol{V}_b=(b_1,b_2,\cdots,b_n)$称为变量节点，对应校验矩阵的列；$\boldsymbol{V}_c=(c_1,c_2,\cdots,c_m)$称为校验节点，对应校验矩阵的行。$\boldsymbol{E}$ 是节点之间相连的边的集合[16]。一个 LDPC 码的集合 $\boldsymbol{D}^n(\lambda,\rho)$可以用度数分布表示，其中

$$\begin{cases}\lambda(x)=\sum_{i=2}^{d_v}\lambda_i x^{i-1}\\ \rho(x)=\sum_{i=2}^{d_c}\rho_i x^{i-1}\end{cases},\tag{7}$$

式中 d_v 为最大变量节点的度数，d_c 为最大校验节点的度数，λ_i，ρ_i 分别表示与度数为 $i\geqslant 2$ 的变量节点或校验节点相连的边数在总边数中所占的比例。

3.1　非规则 LDPC 码的连续密度进化与门限值确定

用随机构造法构造非规则 LDPC 码，就是将变量节点的边和校验节点的边进行随机排列。在置信传播(BP)译码中，校验消息与变量消息的迭代过程表示为

$$\tanh\frac{q_j^{(l)}}{2}=\prod_{i=1}^{d_c-1}\tanh\frac{p_i^{(l-1)}}{2},\tag{8}$$

$$p_i^{(l)}=p_i^{(0)}+\sum_{j=1}^{d_v-1}q_j^{(l)},\tag{9}$$

式中 $p_i^{(0)}$ 为第 0 次迭代时变量节点接收到的信息的初始消息，$q_j^{(l)}$，$p_i^{(l)}$ 分别为第 l 次迭代时校验节点和变量节点接收到的信息。在译码过程中，p 和 q 是服从一定概率分布的随机变量，$P^{(l)}(p)$ 表示每一个 $p_i^{(l)}$ 的密度函数，$Q^{(l)}(q)$ 表示每一个 $q_j^{(l)}$ 的概率分布函数。于是得到校验密度到变量密度的进化[17]

$$P^{(l)}=P^{(0)}*\bigotimes_{j=1}^{d_v-1}Q^{(l)}=P^{(0)}*(Q^{(l)})^{\otimes(d_v-1)},\tag{10}$$

以及变量密度到校验密度的进化

$$Q^{(l)}=R\{P^{(l-1)},R\{\cdots R[P^{(l-1)},P^{(l-1)}]\cdots\}\},\tag{11}$$

式中⊗表示卷积，$R\{P_x,P_y\}=\sum_{(x,y):z=\gamma(x,y)}P_x(x)P_y(y)$，其中 $\gamma(x,y)=2\mathrm{artanh}[\tanh(x/2)\times\tanh(y/2)]$。

在消息迭代时，度数不同的节点输出消息的密度也不同，而总的消息密度是消息密度的数学期望[11]。由(7)式可得到平均变量密度和平均校验密度为

$$\begin{cases}P^{(l)}=\sum_{i=2}^{d_v}\lambda_i P_i^{(l)}\\ Q^{(l)}=\sum_{i=2}^{d_c}\rho_i Q_i^{(l)}\end{cases},\tag{12}$$

则非规则 LDPC 码消息的密度进化过程为

$$P^{(l)}=P^{(0)}*\sum_{i=2}\lambda_i\cdot[Q^{(l)}]^{\otimes(d_v-1)},\tag{13}$$

$$Q^{(l)}=\Delta^{-1}\left\{\sum_{i=2}\rho_i\{\Delta[P^{(l-1)}]\}^{\otimes(i-1)}\right\},\tag{14}$$

式中 $\Delta[\cdot]$ 为拉普拉斯算子，则错误概率

$$P_e^{(l)}=\int_{-\infty}^{0}P^{(l)}(p)\mathrm{d}p。\tag{15}$$

参数为 $\boldsymbol{D}^n(\lambda,\rho)$ 的非规则 LDPC 码，通过参数为 δ 的信道，使用 BP 译码算法解码。信道参数具有一个门限值 δ^*，称为码容量[11]，表示 LDPC 码可以容忍的信道环境的恶劣程度。根据上述的连续密度进化，当信道参数 δ 和 LDPC 码的参数 $\lambda(x)$、$\rho(x)$ 确定时，通过一定迭代次数 l，可以计算出 BP 译码的错误概率 $P_e^{(l)}$。当 $\lambda(x)$，$\rho(x)$ 和 l 确定后，$P_e^{(l)}$ 是关于 δ 的单调增函数。在一定的错误概率 P_e 的约束下，δ 存在门限值 δ^*，表达式为[16]

$$\delta^*=\sup\{\delta>0\,|\,P_e^{(l)}(\delta,\lambda,\rho)<P_e\},\tag{16}$$

式中 sup() 表示取最大值。

3.2　差分进化对非规则 LDPC 码参数的优化

由非规则 LDPC 码连续密度分析可知，在码率 S、预期要达到的错误概率 $P_e^{(l)}$、迭代次数 l_{max} 确定时，不

同的码参数通过密度进化分析所得到的信道参数极限是不同的，其中对应最大信道参数门限值的码参数称为最优码参数[18]，这个过程称为 LDPC 码的优化设计。码参数的优化可以利用差分进化技术实现。差分技术是一种并行直接搜索技术[12]。通过设定一个初始序列，在迭代过程中不断改变序列，直到找到使代价函数最佳的序列。码参数的优化差分进化具体步骤为：

1）初始化：设定期望错误概率 P_e，最大迭代次数 l_{max}，并给定一个信道参数 δ。随机选取 N 个 l 维的分量 $\boldsymbol{k}_{i,G}$，$i=0,1,2,\cdots,N-1$，G 为进化代数，当进化代数 $G=0$ 时，对每一个 $\boldsymbol{k}_{i,G}$ 进行密度进化，得到错误概率 $P_{e_{i,G}}$，比较得到最小的错误概率 $P_{e_{best,G}}$ 对应的最佳分量 $\boldsymbol{k}_{best,G}$。

2）变异：根据一定的组合改变分量。在 $i=0,1,2,\cdots,N-1$ 中，随机选取 4 个分量 $\boldsymbol{k}_{r_1,G}$，$\boldsymbol{k}_{r_2,G}$，$\boldsymbol{k}_{r_3,G}$，$\boldsymbol{k}_{r_4,G}$ 形成新的分量，即

$$\boldsymbol{k}_{i,G+1}=\boldsymbol{k}_{best,G}+c\cdot(\boldsymbol{k}_{r_1,G}-\boldsymbol{k}_{r_2,G}+\boldsymbol{k}_{r_3,G}+\boldsymbol{k}_{r_4,G}),\tag{17}$$

式中 c 为常数，用来控制分量变化。取 $c=0.5$，对每一个 $\boldsymbol{k}_{i,G+1}$ 进行密度进化，可得到错误概率 $P_{e_{i,G+1}}$。

3）选择：比较 $P_{e_{i,G}}$ 和 $P_{e_{i,G+1}}$，选取 $G+1$ 代进化中最小的错误概率 $P_{e_{best,G+1}}$ 对应的最佳分量 $\boldsymbol{k}_{best,G+1}$。

4）结束标准：当最佳矢量 $\boldsymbol{k}_{best,G+1}$ 所对应的错误概率 $P_{e_{best,G+1}}>P_e$ 时，说明没有达到目标，则返回第 2）步，继续寻找；当 $P_{e_{best,G+1}}<P_e$ 时，返回第 1）步，微弱增加信道参数 $\delta=\delta+\Delta\delta$，继续寻找。如果 δ 增加到某一值，错误概率达不到期望错误概率，进化过程结束，得到信道参数极限值 δ^*。

利用连续密度进化和差分进化方法，并且经过大量的实验数据对比，设计出了在 BIAWGNC 下，码率分别为 0.2，0.3，0.4，0.5 且距香农极限很近的非规则 LDPC 码。以码率为 0.5 为例：设计非规则 LDPC 码的最大变量节点度数为 50，错误概率为 10^{-6} 时，距离香农极限仅 0.1 dB，其门限值距离香农极限仅 0.06 dB。码率为 0.5 的优化的码参数如表 1 所示，其中最大变量节点度数 $d_{max}=7,8,9,10,11,12$，信道门限值为 δ^*，对应的信噪比为 R_{SN}^*，λ_{2max} 为错误概率收敛时 λ_2 的最大值。

表 1　BIAWGNC 条件下码率为 0.5 时优化的码参数

Table 1　Optimized code parameters for BIAWGNC under 0.5 coding rate

d_{max}	10	11	12	15	20	30	50
λ_{2max}	0.27165	0.26269	0.25522	0.244446	0.23261	0.21306	0.18379
λ_2	0.25105	0.23882	0.24426	0.23802	0.21991	0.19606	0.17120
λ_3	0.30938	0.29515	0.25907	0.20997	0.23328	0.24039	0.21053
λ_4	0.00104	0.03261	0.01054	0.03492	0.02058	0	0.00273
λ_5	0	0	0.05510	0.12015	0	0	0
λ_6	0	0	0	0	0.08543	0.00228	0
λ_7	0	0	0	0.01587	0.06540	0.05516	0.00009
λ_8	0	0	0.01455	0	0	0.16602	0.15269
λ_9	0	0	0	0	0	0.04088	0.09227
λ_{10}	0.43853	0	0.01275	0	0	0.01064	0.02802
λ_{11}	0	0.43342	0	0	0	0	0
λ_{12}	0	0	0.40373	0	0	0	0
λ_{14}	0	0	0	0.00480	0	0	0
λ_{15}	0	0	0	0.37627	0	0	0
λ_{19}	0	0	0	0	0.08064	0	0
λ_{20}	0	0	0	0	0.22798	0	0
λ_{28}	0	0	0	0	0	0.00221	0
λ_{30}	0	0	0	0	0	0.28636	0.07212
λ_{50}	0	0	0	0	0	0	0.25830
ρ_7	0.63676	0.43011	0.25475	0	0	0	0
ρ_8	0.36324	0.56999	0.73478	0.98013	0.64854	0.00749	0
ρ_9	0	0	0.01087	0.01987	0.34747	0.99101	0.33620
ρ_{10}	0	0	0	0	0.00399	0.00150	0.08883
ρ_{11}	0	0	0	0	0	0	0.27497
δ^*	0.9558	0.9572	0.9580	0.9622	0.9649	0.9690	0.9718
R_{SN}^*	0.3927	0.3799	0.3727	0.3347	0.3104	0.2735	0.2485

由表 1 可以得到，信道门限值 δ^* 所对应的信噪比门限值 $R_{\mathrm{SN}}^*=(E_{\mathrm{b}}/N_0)^*=1/(2R\delta^{*2})$。将该参数的非规则 LDPC 码用于 CVQKD 的多维数据协调，得到一个较好的协调效率 $\beta=95.98\%$，完全可以保证信息的安全传输。

4　提高协调效率方法分析

利用连续密度进化和差分进化算法，设计了一系列低码率梯度上高效率的 LDPC 码。将其应用到多维数据协调算法中，降低了收敛信噪比，提高了安全传输距离。在已有的低收敛信噪比情况下，根据 BIAWGNC 的特点，应用重复码字的方法继续降低收敛信噪比。

对于码率为 S 的 LDPC 码，在信噪比为 R_{SN} 的 BIAWGNC 中可以获得的协调效率为 β。通过重复 k 倍码字构造一种新的 LDPC 码，使得新的 LDPC 码的码率为 $S'=S/k$，收敛信噪比为 $R'_{\mathrm{SN}}=R_{\mathrm{SN}}/k$，从而得到协调效率 $\beta'(R'_{\mathrm{SN}})=\beta(R_{\mathrm{SN}})\dfrac{\mathrm{lb}\,(1+R_{\mathrm{SN}})}{k\,\mathrm{lb}\,(1+R_{\mathrm{SN}}/k)}$。这一方法仅适用于信噪比很低的情况，并且以牺牲小部分的协调效率为代价从而获得更小的信噪比。

以下对该方法的可行性进行证明。令高斯信道(AWGNC)的信道容量 C_{AWGNC} 为

$$C_{\mathrm{AWGNC}}=\frac{1}{2}\mathrm{lb}\,(1+R_{\mathrm{SN}})。\tag{18}$$

在多维协调方案中，离散高斯调制限制信道为 BIAWGNC，达不到高斯信道的容量。将 Alice 端和 Bob 端在 BIAWGNC 信道上的最大互信息量定义为 BIAWGNC 的信道容量[8]：

$$C_{\mathrm{BIAWGNC}}(R_{\mathrm{SN}})=-\int\phi_{R_{\mathrm{SN}}}(x)\mathrm{lb}\,[\phi_{R_{\mathrm{SN}}}(x)]\mathrm{d}x-\frac{1}{2}\mathrm{lb}\,(2\pi e)+\frac{1}{2}\mathrm{lb}\,R_{\mathrm{SN}},\tag{19}$$

式中

$$\phi_{R_{\mathrm{SN}}}(x)=\sqrt{\frac{R_{\mathrm{SN}}}{8\pi}}\{\exp[-R_{\mathrm{SN}}(x+1)^2/2]+\exp[-R_{\mathrm{SN}}(x-1)^2/2]\}。\tag{20}$$

在低信噪比的条件下，BIAWGNC 的信道容量 C_{BIAWGNC} 与 AWGNC 的信道容量 C_{AWGNC} 非常接近。然而在信噪比较大时，C_{BIAWGNC} 与 C_{AWGNC} 有明显的不同。随着信噪比增大，C_{AWGNC} 的值趋于无穷大，而 C_{BIAWGNC} 的值无限趋近于 1。因此在低信噪比条件下，可认为 $C_{\mathrm{BIAWGNC}}\approx C_{\mathrm{AWGNC}}$。AWGNC 的信道容量 C_{AWGNC} 与 BIAWGNC 的信道容量 C_{BIAWGNC} 随信噪比 R_{SN} 的变化曲线如图 2 所示。

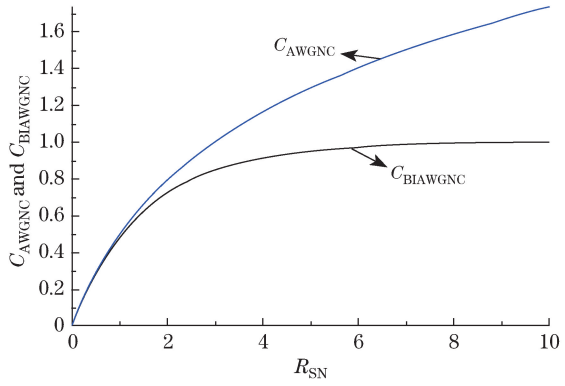

图 2　二进制高斯调制下 C_{AWGNC} 与 C_{BIAWGNC} 随信噪比 R_{SN} 的变化曲线

Fig. 2　Curves of C_{AWGNC} and C_{BIAWGNC} as functions of R_{SN} with binary-Gaussian modulation

利用离散高斯调制，可在每一个信道中发送小于 1 bit 的信息。记离散高斯调制下的协调效率 β_{dis} 为

$$\beta_{\mathrm{dis}}=\beta_{\mathrm{modulation}}\frac{S}{C_{\mathrm{BIAWGNC}}},\tag{21}$$

式中 $\beta_{\mathrm{modulation}}$ 为调制效率，即

$$\beta_{\mathrm{modulation}}=\frac{C_{\mathrm{AWGNC}}}{C_{\mathrm{BIAWGNC}}}。\tag{22}$$

$\beta_{\text{modulation}}$使得离散调制协调效率$\beta_{\text{dis}}$在信噪比$R_{\text{SN}}$趋近于0时迅速地趋近于1，而$S/C_{\text{BIAWGNC}}$直接反映所选LDPC码在BIAWGNC上的性能。在低信噪比条件下，近似得到$\beta_{\text{modulation}}\approx1$，这意味着所选LDPC码的码率近似为关于信噪比$R_{\text{SN}}$的函数，即

$$S(R_{\text{SN}})\approx\frac{\beta}{2}\text{lb}\,(1+R_{\text{SN}})\approx\frac{\text{lb e}}{2}\beta R_{\text{SN}}。\tag{23}$$

固定协调效率β不变，可见LDPC码的码率S与信噪比R_{SN}近似成正比。因此，可构造一种加工过程。当已知LDPC码的码率为S，在收敛信噪比为R_{SN}时，数据协调效率为β。通过重复k($k\geqslant2$，且为整数)倍码字的操作，可以获得一种新的LDPC码，码率为$S'=S/k$，在信噪比为$R'_{\text{SN}}=R_{\text{SN}}/k$下得到协调效率$\beta'$。

重复码字时，不再随机发送$x_i=\pm1$给信道，而是重复发送k次相同的值，即：$x_{i1}=x_{i2}=\cdots=x_{ik}\equiv X_i$，则Bob端可获得$k$种关于$X_i$的不同的噪声，即

$$\begin{cases}y_{i1}=x_{i1}+z_{i1}\\y_{i2}=x_{i2}+z_{i2}\\\vdots\\y_{ik}=x_{ik}+z_{ik}\end{cases},\tag{24}$$

式中$z_{i1},z_{i2},\cdots,z_{ik}$为$k$个独立同分布的随机变量，$z_{ij}\sim N(0,\sigma^2)$，$j\in\{1,\cdots,k\}$。定义新的随机变量

$$\begin{cases}X_i\equiv\dfrac{1}{k}\displaystyle\sum_{j=1}^{k}x_{ij}\\Y_i\equiv\dfrac{1}{k}\displaystyle\sum_{j=1}^{k}y_{ij}\\Z_i\equiv\dfrac{1}{k}\displaystyle\sum_{j=1}^{k}z_{ij}\end{cases},\tag{25}$$

则有

$$Y_i=X_i+Z_i,\tag{26}$$

式中$X_i=\pm1$，$Z_i\sim N\left(0,\dfrac{\sigma^2}{k}\right)$，由此得到一个新的信道，新信道输入为$X_i$，输出为$Y_i$，此时该信道仍是一个BIAWGNC，且信噪比是原来信道信噪比的k倍。但该方法仅适合于正向协调，因为在逆向协调中，该信道的输入为Y_i，输出为X_i，此时不能确定该信道仍为BIAWGNC。把重复k倍码字操作后得到新的LDPC码用于数据协调中，在信噪比$R'_{\text{SN}}=R_{\text{SN}}/k$下，数据协调效率$\beta'$为

$$\beta'(R'_{\text{SN}})=\beta(R_{\text{SN}})\frac{\text{lb}\,(1+R_{\text{SN}})}{k\,\text{lb}\,(1+R_{\text{SN}}/k)}。\tag{27}$$

在信噪比很低时，$\beta'(R'_{\text{SN}})\approx\beta$。

5　仿真结果及分析

使用CPU为Inter Xeon E5620，2.4 GHz和32 G内存的双核服务器作为硬件平台，在8维数据协调算法下，利用LDPC码作为纠错码，译码最大迭代次数设为100。利用随机构造法构造码长为2×10^5，不同码率的LDPC码在8维数据协调算法中的实验结果如表2所示[10]。

表2　码率不同时8维数据协调算法实验结果

Table 2　Experimental results of eight dimensional reconciliation algorithm at different rates

Rate	R_{SN} /dB	β /%	Rate bit /(kb/s)	Distance /km
0.2	−3.979	82.4	−21.83	69.90
0.25	−3.010	85.48	−14.34	65.05
0.3	−2.596	94.89	8.61	62.98
0.35	−1.549	91.44	0.19	57.75
0.4	−0.969	94.34	7.26	54.85

利用连续密度进化和差分进化方法对 LDPC 码进行优化设计后，码长为 10^6，不同码率的 LDPC 码在 8 维数据协调算法中的收敛情况如表 3 所示。

表 3　优化设计后不同码率 8 维数据协调算法实验结果

Table 3　Experimental results of eight dimensional reconciliation algorithm at different rates after optimized design

Rate	R_{SN} /dB	β /%	Rate bit /(kb/s)	Distance /km
0.2	−4.789	96.21	4.74	73.81
0.25	−3.605	95.59	3.88	68.02
0.3	−2.612	95.18	3.30	63.06
0.35	−1.746	94.76	2.70	58.73
0.4	−0.980	94.52	2.36	55.06

对比表 2 与表 3 可见，利用连续密度进化和差分进化方法进行 LDPC 码的优化设计后，在不同码率下，收敛信噪比明显降低，协调效率明显提高，从而可获得较远的安全传输距离。当继续降低码率，在码率为 0.15的条件下，得到收敛信噪比为 −2.874，协调效率为 49.98%，此时得到的安全密钥量为负值，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。

在 LDPC 码的优化设计基础上，利用重复 2 倍码字，得到码长为 2×10^6 的 LDPC 码在 8 维数据协调中的实验结果如表 4 所示。

表 4　使用重复码子优化后的 LDPC 码在 8 维数据协调算法中的实验结果

Table 4　Experimental results of eight dimensional reconciliation algorithm with repetition of LDPC codes

Rate	R_{SN} /dB	β /%	Rate bit /(kb/s)	Distance /km
0.2	−4.789	96.21	4.74	73.81
0.1	−7.798	90.27	0.22	88.99

为了进一步降低收敛信噪比，在码率为 0.2 时，利用重复码字的方法，取 $k=2$ 得到新码，其码率为 0.1，收敛信噪比约为 −7.798 dB，得到协调效率为 90.27%，提取到的安全密钥量为 0.22 kb/s，使得安全距离大于80 km。

6　结　　论

基于 CVQKD 的多维数据协调方案，利用连续密度进化和差分进化方法，设计出优质度数分布的 LDPC 码，同时结合 LDPC 码码字重复方法，对 CVQKD 进行数据仿真。分组码长为 10^6 的实验仿真结果表明：当码率降低至 0.1 时，收敛信噪比能够降低至 −7.798 dB，协调效率可达 90.27%，提取到的安全密钥量为 0.22 kb/s，信息传输距离超过 80 km，延长了 CVQKD 系统的通信距离。

参　考　文　献

1　Bennett C H. Quantum cryptography: public key distribution and coin tossing[C]. International Conference on Computer System and Signal Processing, 1984: 175-179.

2　Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states[J]. Physical Review Letters, 2002, 88(5): 057902.

3　Lodewyck J, Bloch M, García-Patrón R, *et al*. Quantum key distribution over 25 km with an all-fiber continuous-variable system[J]. Physical Review A, 2007, 76(4): 042305.

4　Bloch M, Thangaraj A, McLaughlin S W, *et al*. LDPC-based secret key agreement over the Gaussian wiretap channel [C]. 2006 IEEE International Symposium on Information Theory, 2006: 1179-1183.

5　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.

6　Leverrier A, Alléaume R, Boutros J, *et al*. Multidimensional reconciliation for a continuous-variable quantum key distribution[J]. Physical Review A, 2008, 77(4): 042325.

7　Jouguet P, Kunz-Jacques S, Leverrier A. Long-distance continuous-variable quantum key distribution with a Gaussian

modulation[J]. Physical Review A, 2011, 84(6): 062317.

8 Leverrier A, Grangier P. Continuous-variable quantum key distribution protocols with a discrete modulation[Z/OL]. 2010[2015-03-21]. http://arxiv.org/abs/1002.4083.

9 Jouguet P, Kunz-Jacques S, Leverrier A, *et al*. Experimental demonstration of long-distance continuous-variable quantum key distribution[J]. Nature Photonics, 2013, 7(5): 378-381.

10 Wang Yunyan, Guo Dabo, Zhang Yanhuang, *et al*. Algorithm of multidimensional reconciliation for continuous-variable quantum key distribution[J]. Acta Optica Sinica, 2014, 34(8): 0827002.
王云艳, 郭大波, 张彦煌, 等. 连续变量量子密钥分发多维数据协调算法[J]. 光学学报, 2014, 34(8): 0827002.

11 Richardson T J, Urbanke R L. The capacity of low-density parity-check codes under message-passing decoding[J]. IEEE Transactions on Information Theory, 2001, 47(2): 599-618.

12 Shokrollahi A, Storn R. Design of efficient erasure codes with differential evolution[M]. Berlin: Springer, 2005: 413-427.

13 Bloch M, Thangaraj A, McLaughlin S W. Efficient reconciliation of correlated continuous random variables using LDPC codes[Z/OL]. 2005[2016-03-21]. http://arxiv.org/abs/cs/0509041.

14 van Assche G. Quantum cryptography and secret-key distillation[M]. Cambridge: Cambridge University Press, 2006.

15 Richardson T, Urbanke R. Modern coding theory[M]. Cambridge: Cambridge University Press, 2008.

16 Yuan Dongfeng, Zhang Haigang. The theory and application of LDPC code[M]. Beijing: Posts & Telecom Perss, 2008: 31-32, 122-123.
袁东风, 张海刚. LDPC 码理论与应用[M]. 北京: 人民邮电出版社, 2008: 31-32, 122-123.

17 Xiao Juan, Wang Lin, Deng Lizhao. Density evolution method and threshold decision for irregular LDPC codes[J]. Journal of Electronics & Information Technology, 2005, 27(4): 617-620.
肖　娟, 王　琳, 邓礼钊. 不规则 LDPC 码的密度进化方法及其门限值确定[J]. 电子与信息学报, 2005, 27(4): 617-620.

18 Hou J, Siegel P H, Milstein L B. Performance analysis and code optimization of low density parity-check codes on Rayleigh fading channels[J]. IEEE Journal on Selected Areas in Communications, 2001, 19(5): 924-934.