量子高斯密钥分发中后处理的安全性分析

阎 金 王晓凯 郭大波 孙 艺

山西大学物理电子工程学院, 山西 太原 030006

摘要 在量子高斯密钥分发实验中,后处理是提升数据协调效率和保证安全密钥提取的关键技术之一。通过分层纠错协议给出一种具体后处理的数据协调方案,并采用准循环低密度奇偶校验码与传统低密度奇偶校验码相级联的方式对信息进行压缩编码。结合零拍探测下的连续变量量子密钥分发,分析了个体攻击和集体攻击下采用正向协调和逆向协调的实验方案中密钥提取的安全性。实验结果表明:在码长为 2×10^5,三、四级码率为 0.3/0.95 的数据协调方案中协调效率可达 91.2% 。采用最优攻击下可提取安全密钥量为 3.98 kbit/s ,而传输距离达 30 km 左右,证明了所提协调方案的安全性,能够满足城域网络的通信要求。

关键词 量子光学;量子密钥分发;数据协调;低密度奇偶校验码;零拍探测;安全性

中图分类号 O431 **文献标识码** A

doi: 10.3788/AOS201636.0327003

Security Analysis of Post-Processing in Quantum Gaussian Key Distributed

Yan Jin Wang Xiaokai Guo Dabo Sun Yi

College of Physics and Electronic Engineering, Shanxi University, Taiyuan, Shanxi 030006, *China*

Abstract In quantum Gaussian key distribution experiment, post-processing is one of key technologies to improve data reconciliation efficiency and guarantee the security of the extracted secret key. A specific data reconciliation of post-processing is proposed through the slice error correction which uses the quasi-cyclic low density parity check code and traditional low density parity check code to cascade to compress and code. To analyze the security of secret key extracted, direct reconciliation and reverse reconciliation scheme are proposed in individual attack and collective attack on the continuous variable quantum key distribution with homodyne detection. The result indicates that the data reconciliation efficiency can achieve 91.2% when code length is 2×10^5 and the third and fourth level code rate is 0.3/0.95. The amount of the extracted secret key can reach 3.98 kbit/s using the optimal attack and transmission distance can reach about 30 km, which proves the safety of the data reconciliation scheme and can satisfy the requirement of the metropolitan area network communication.

Key words quantum optics; quantum key distribution; data reconciliation; low density parity check code; homodyne detection; security

OCIS codes 270.5585; 270.5565; 270.5568

1 引 言

近几年随着信息技术的发展,量子保密通信成为信息安全技术的一个新兴分支,它涉及到量子力学,光学,信息论以及电子和通信技术。为了提高量子通信过程中的稳定性和安全性,研究人员提出量子密钥分发(QKD)技术。这一理论是量子理论和经典信息理论的结合产物,它利用了通信系统的量子特性,使密钥分

收稿日期: 2015-09-14; **收到修改稿日期**: 2015-10-24

基金项目: 山西省国际科技合作计划项目(2014081027-1)、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)

作者简介: 阎 金(1989—),男,硕士研究生,主要从事量子密钥分发方面的研究。E-mail: yanjinco@163.com

导师简介: 王晓凯(1963—),男,博士,教授,主要从事通信网络管理、控制与优化等方面的研究。

E-mail: wxk2000@263.net (通信联系人)

配的安全性得到不可破译的安全保障[1]。量子密钥分发能够使相距较远的合法通信双方Alice端和Bob端，在传输系统有噪声干扰以及第三方Eve对信道实施窃听行为的情况下，实现安全的信息密钥传输。

经典量子密钥分发实验中，通过量子信道的密钥信息并不能作为通信双方的密钥直接使用。这是由于信道存在噪声信号以及窃听者Eve的影响，导致密钥信息出现错误和泄露等现象，因此需要引入相关的处理算法来获得一致且安全的密钥信息。研究人员在传统BB84量子密码通信协议框架内，进一步提出采用数据协调和私密放大两个过程对量子密钥分发进行后处理[2]。其中数据协调是一个对密钥串纠错的过程：通信的接收方对接受量子态进行测量，通过数据筛选得到相互关联的密钥量，然后通信双方Alice和Bob利用经典信道编码对数据进行纠错，从而得到完全一致的数据序列。

早期离散量子密钥分发(Discrete-Variable-QKD)研究中，采用单光子以及微弱光脉冲作为载体实现信号的离散调制。随着连续变量量子密钥分发(Continuous-Variable-QKD)的发展，采用相干态，双模纠缠态等连续量子变量作为载波技术的应运而生。但是量子信号为微弱信号，容易受到环境因素影响[3]，因而如何提高量子密钥分发协调效率，以及延长信息传输距离成为研究的热点。2011年上海交通大学实现了27.2km的CV-QKD的高斯相干态调制[4]，2013年山西大学实现了CV-QKD的光纤四态分离调制[5]，另外清华大学、中国科学技术大学等研究单位在量子密钥分发的研究上也取得了丰硕的成果。Leverrier等[6]提出多维密钥协调算法，该协议利用虚拟诱骗技术，能够抵御大规模攻击行为，成为近几年来CV-QKD的主要密钥协调方案。法国的Jouguet等[7]在同年实现了标准高斯调制的CV-QKD方案，采用低密度奇偶校验码(LDPC)进行数据协调，获得的安全密钥量在25km可达到10kbit/s。Furrer等[8]证明了在有限码长下基于高斯相干态调制CV-QKD协议的无条件安全性，使CV-QKD协议理论完善有了质的飞跃。但是由于现代技术设备的有限，实际CV-QKD方案的光源信号制备，探测器，以及后处理器件性能的不足都制约了CV-QKD的技术应用。

目前CV-QKD还处于发展阶段，其系统的安全码率以及传输的距离等性能指标有待提高，其中数据的后处理中协调技术最终影响整个CV-QKD的密钥生成率和传输效率。数据协调方案的优化有助于提升CV-QKD协议的速率和效率，而且其密钥的安全性能是整个系统可靠运行的保障。本文结合分层纠错协议给出后处理中具体的数据协调方案，并在纠错码中将具有优良性能的准循环LDPC码与传统LDPC码相结合，以降低编码复杂度，提升解码速率，并实验证明了本方案在最优攻击——高斯集体攻击下的安全性，同时给出此种攻击下所能提取的最大密钥量和传输距离。

2 基于分层纠错协议的逆向数据协调方法

分层(Slice)纠错协议是Assche等[9]为解决CV-QKD的密钥协商问题提出的一种算法方案。Slice纠错方案的主要思想是将连续变量量化为离散的二进制比特，然后Alice端和Bob端通过二进制纠错，将传输过程中不一致的比特信息纠正，并且尽可能减少泄露其中的密钥信息。通信双方通过交换信息共享同一组密钥，这个过程等效为传统通信中的分布式信源编码。

2.1 信源联合边信息编码

双方通信的最终目标是得到互信息 $I(X;Y)$：

$$I(X;Y)=H(X)-H(X|Y)=H(Y)-H(Y|X)\,, \tag{1}$$

根据信息论理论，经典的公共信道的容量有限，因此通信双方在交换信息时需要将连续信号量化为离散信号。假设Alice端和Bob端拥有的信息分别表示为 $\{x_i\}_{1\cdots n}\in\mathbb{R}^n$ 和 $\{y_i\}_{1\cdots n}\in\mathbb{R}^n$ 并假设独立随机变量 $X,Y\in\mathbb{R}^n$。Alice经过量化处理后信息 $\hat{X}$ 有 $\hat{X}=Q(X)\left[Q(X)\text{为量化函数}\right]$，Bob量化后的信息为 $\hat{Y}$。在CV-QKD协议下，通过最优量化方式得到的共享互信息量应满足 $I(X;\hat{Y})\leqslant I(X;Y)$。

Bob端将接受到的信息量化为离散值，并通过一个经典的理想信道将冗余信息传送给Alice端。设 $I_{\mathrm{rec}}^{\min}$ 为数据协调过程中每信息比特交换所需要的最小信息量。则根据Slepian Wolf (SW)编码定理[10]，Bob只需通过经典信道传输压缩信息：

$$I_{\mathrm{rec}}^{\min}=H(\hat{Y}|X)\,, \tag{2}$$

Alice端将Bob发送来的冗余信息结合已有信息，采用SW译码器得到量化信息 $\hat{Y}$ 的估计值，完成整个数据协调。

图1为基于分布式信源编码的等效编译码框图，当Alice端从激光器中产生的相干态光脉冲信号 X 通过量子信道到达Bob端，Bob通过平衡零拍探测器接受到的光脉冲信号为 $\hat{Y}$ 。此时信号通过的量子信道可以等效为一种信源 C_1，而信号通过离散调制等效为另一种独立信源 C_2 。根据分布式信源编码理论，纠错信息可以独立进行信源编码，并结合Alice端已有的辅助边信息在接受端进行联合译码。

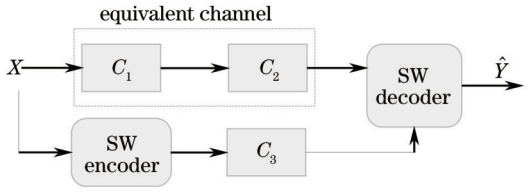

图1 等效经典分布式信源编码框图

Fig.1 Equivalent classical distributed source coding diagram

2.2 多级编译码协调方式

CV-QKD通信中安全提取Alice和Bob两端的密钥串，并且能够纠正其中的错误是保证安全通信的前提。设Alice端的 l 个信息比特 $(x_1\cdots x_l)$ 对Bob端的 l 个信息比特 $(y_1\cdots y_l)$ 进行协调。协商开始时，双方需要约定其协商的量化层数 m ，而Alice端要选择量化函数 $S(x)$，Bob端设定其估计函数 $E(x)$ 。在正向的协调过程中，Alice首先利用量化函数 $S(x)$ 将 l 个信息位映射为比特串 $\left[L_1(\hat{X})\cdots L_l(\hat{X})\right]$ 并作为第 i 层的密钥，Bob端则利用估计函数 $E(x)$ 和信息比特 Y ，并结合前面 $i-1$ 层中协调信息 $S_1(x)\cdots S_{i-1}(x)$ ，对密钥串进行估计。Bob端对每一层比特串进行判决时，如果计算得到的误码率超过期望值，则舍弃纠错，随后Alice公开这一层的比特串。如果误码率在设定范围内，Bob端进行纠错并将纠正后的密钥传送给下一层。最后双方根据量化信息的全部层或者部分层的协调信息作为共享密钥。

传统的分层纠错(SEC)协议的基本原则是通过不同层的信息传递进行数据协调，这种通信方式非常类似于传统信息技术中的多电平编码调制(MLC)和多级译码技术(MSD)[11]。因此采用MLC的编码调制方案优势是不同信息层可以等效为独立的通信信道，使各级码率能够自适应，而且对不同优先级的信息能够采取不同的保护措施。

2.3 基于准循环LDPC码的MLC/MSD过程

Bob端采用零拍探测得到连续的高斯变量后，对其离散量化得到二进制信息比特串。通过对信息比特串进行多电平编码，Bob将编码后的校验信息通过经典信道发送回Alice端。其中采用性能优良的校验矩阵 H ，以及选取不同信息层的码率是影响最终编码效率的重要因素。根据信道容量准则，编码分级级数的增加并不能有效地提高编码效率，而且级数增加反而增加了系统的运算的开销，因此采用4bit、16V电平的编码压缩方案。

图2为采用MLD/MSD设计的CV-QKD数据协调方案。由于各级信息受到不同程度的噪声干扰，因此需要采用不同的校验矩阵对应各级编码。二进制数据串通过二元映射，编码生成四级码流，表示为 $L_1/L_2/L_3/L_4$ 。由MSD理论计算可知在通信信噪比(SNR)较低的情况下，第一、二级的量化有效性比较小，对协调过程中互信息的贡献可以忽略不计，因此通信中编码不完全公开这两级信息，对整个方案的安全性影响甚微[12]。第三、四级码率的设计将是本方案重点所考虑的。

准循环LDPC作为一类重要的LDPC码的子类，其校验矩阵形式更具有结构化特征。采用经过优化处理的准循环LDPC，在高码率上性能优势明显，能够取得接近香农极限的纠错能力[13]。准循环LDPC校验矩阵构造灵活，非常适用于码率自适应的协调方案，由于矩阵具有准循环结构，其编码、译码便于并行化设计。但准循环LDPC码在较长码长下，性能优势并不明显，因此MSD的方案中采用准循环LDPC和传统LDPC相结合的方式。根据经典信息论，上述方案中每一级所含的密钥量可以表示为：

$$I(X;L_i|L_1\cdots L_4)=H(L_i|L_1,\cdots,L_{i-1})-H(L_i|X,\cdots,L_{i-1})\,. \tag{3}$$

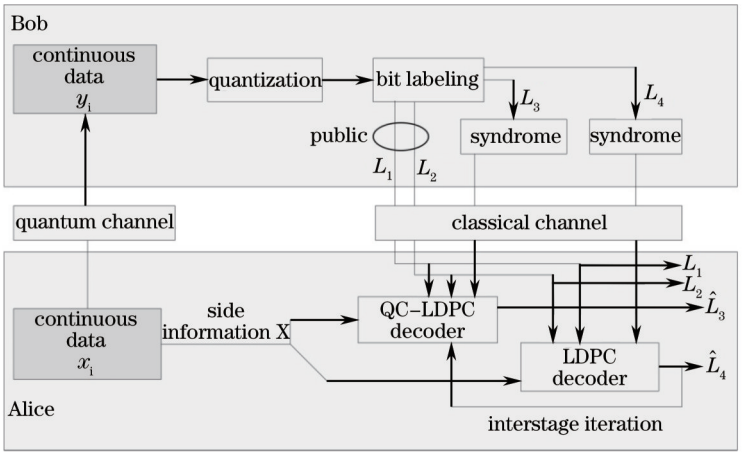

图2 连续变量量子密钥分发协调框图

Fig.2 Continuous variable quantum key distribution diagram

图3表示为每一级所携带的信息量与信噪比的关系示意图。从图中可以看出，当信噪比 $f_{\mathrm{SNR}}<1$ dB 的情况下，前两级的信息量基本为0。由(3)式结合多级译码的过程可以得到不同信噪比下每层中携带的密钥量 $I(X|L_i)$。比如当 $f_{\mathrm{SNR}}=3$ dB 时，各信息最佳码率为0.002、0.016、0.259、0.921。可以看出当选择公开前两级，带来的信息损失仅为 $\Delta I=0.018$ bit/s，因而有助于在数据协调中提高密钥传输速率。编码时Bob将量化后的二进制信息串 Y 通过编码生成校验子：

$$S_i=L_i\times H_i,\quad i=3,4\quad ,\tag{4}$$

之后将校验信息 S_3,S_4 连同前两级信息 L_1,L_2 一同传给Alice端，完成整个多级编码过程。

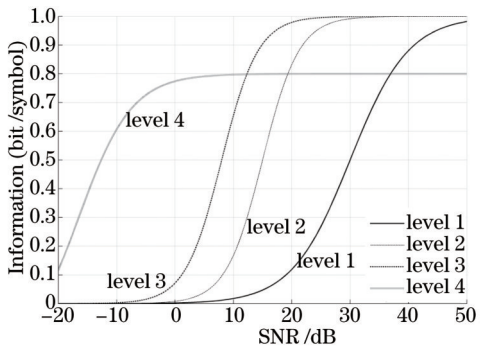

图3 各级互信息量与信噪比关系示意图

Fig.3 Relationship between mutual information and SNR

实际的迭代译码中，信息传递并不仅限于变量节点到校验节点之间，还包括节点内部的信息流动[14]。设连续变量量化映射为多级的变量节点集 $N(j)=\{i:H_{ij}=1\}$，与之对应的校验节点集为 $C(i)=\{j:H_{ji}=1\}$。信息传递包含了变量节点集 $N(j)$ 接受的外信息 o_{ij}，变量节点提供给校验节点的外信息 v_{ij}，校验节点提供给变量节点集的外信息 u_{ij}，以及变量节点通过加和运算得到的内信息 e_{ij}，以上信息都提供给相邻节点做译码处理。设Alice端提供的辅助校验边信息为 S_j。

基于消息概率似然比译码(LLR-BP)的具体流程为：

1) 初始化信息：

根据具体信道的条件计算每个变量消息的后验概率：

$$o_{ij}=\log\frac{\sum\limits_{\hat{y}:\hat{y}_j=1}P(x_i,\hat{y})}{\sum\limits_{\hat{y}:\hat{y}_j=0}P(x_i,\hat{y})}=\log\frac{\sum\limits_{\hat{y}:\hat{y}_j=1}\int_{y_1}^{y_2}\frac{1}{\sqrt{2\pi\sigma}}\exp\left(-\frac{(y-x)^2}{2\sigma^2}\right)\mathrm{d}y}{\sum\limits_{\hat{y}:\hat{y}_j=0}\int_{y_1}^{y_2}\frac{1}{\sqrt{2\pi\sigma}}\exp\left(-\frac{(y-x)^2}{2\sigma^2}\right)\mathrm{d}y}\quad ,\tag{5}$$

2) 变量节点信息更新：

$$v_{ij}=o_{ij}+\sum_{j\in N(i)\backslash j}u_{ij}\ , \tag{6}$$

3) 校验节点信息更新：

$$\tanh(u_{ij})=(1-2S_j)\prod_{i\in C(j)\backslash i}\tanh(\frac{v_{ij}}{2})\ , \tag{7}$$

4) 变量节点的内信息更新：

$$e_{ij}=\sum_{k\in N(ij)}u_{ij}\ , \tag{8}$$

5) 译码判决：

对 $\forall i\in\{1,\cdots,n\}$ 所有变量节点集硬判决译码

$$v_{ij}=-\frac{1}{2}\left[\mathrm{sign}(e_{ij}+o_{ij})-1\right],\qquad \mathrm{sign}(x)=\begin{cases}+1, & x>0\\ -1, & x\leqslant 0\end{cases}, \tag{9}$$

通过不断的级间迭代，满足收敛或到达最大迭代次数时译码结束。

3 零拍探测下CV-QKD的安全性

安全密钥量是量子密钥分发实验中很重要的一个指标。当通信双方在经过数据协调以及密性放大等后处理步骤后，只有安全密钥量达到一定的值时，双方才能建立安全的通信[15]。设Alice与Bob之间的互信息为 I_{AB}，Alice与窃听者Eve之间的互信息为 I_{AE}，Bob与Eve之间的互信息为 I_{BE}。根据信息论的理论双方能够安全通信的准则为 $I_{AB}>I_{AE}$ 或者 $I_{AB}>I_{BE}$。

根据信号源制备的不同可以分为基于零拍探测和相干态高斯调制的CV-QKD协议，以及采用异差探测和压缩态调制的CV-QKD协议[16]。针对基于零拍探测的CV-QKD协议进行主要讨论，其中图4表示相干态连续变量量子密钥分发的通信模型。

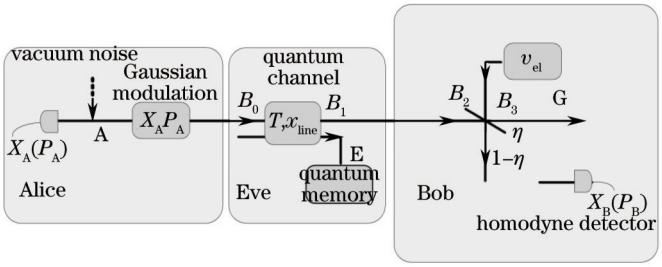

图4 基于零拍探测的CV-QKD通信模型

Fig.4 CV-QKD communication model based on homodyne detection

Alice端将相干态 $\left|x_A+\mathrm{i}p_A\right\rangle$ 通过量子信道发送给Bob端，其中正则分量 x_A 和 p_A 服从 $N(0,V_AN_0)$ 均值为0，方差为 V_AN_0 的高斯分布。设量子信道的透射系数为 $T\leqslant 1$，信息传输过程中引入额外噪声 ε，忽略Alice端耦合器的衰减因素，则Bob端输入的噪声功率为 $(1+T\varepsilon)N_0$，此时信道输入的噪声表示：

$$\chi_{line}=1/T-1+\varepsilon\ , \tag{10}$$

在Bob采用零拍探测相干光信号，引入的信道噪声为：

$$\chi_{hom}=(1+\nu_{el})/\eta-1\ \ , \tag{11}$$

式中 ν_{el} 为探测的系统的热噪声，η 为探测效率，以上噪声都以散粒噪声 N_0 为单位。

这些噪声存在于Alice和Bob的通信之间，因而可以等效为系统信道的总输入噪声 χ_{tot}，此时有：

$$\chi_{tot}=\chi_{line}+\chi_{hom}/T\ , \tag{12}$$

Alice端进行分离调制时，相干态强度较弱，具有高斯分布方差 $V_AN_0=(V-1)N_0$。此时Bob端对正交分量测量的功率值 $V_B=\eta T(V+\chi_{tot})$，而对Alice测量的条件方差 $V_{B|A}=\eta T(1+\chi_{tot})$。根据香农信道容量公式可知Alice端与Bob端之间的互信息为：

$$I_{AB}=\frac{1}{2}\log_2\frac{V_B}{V_{B|A}}=\frac{1}{2}\log_2\frac{V+\chi_{tot}}{1+\chi_{tot}}\ , \tag{13}$$

根据前面给出的数据协调方案，如果纠错信息与原始密钥信息传递的方向一致时，称这种协议为正向协调，反之协调方向不一致时，此时的协议称为逆向协调[17]。

假设第三方采用个体攻击去测量Bob端的基矢量，并对每一个量子态独立测量。此时窃听者Eve为了到达隐蔽，需要将干扰信号混杂在信道的额外噪声中，最终Eve从信道中获得的密钥量取决于信道噪声[18]。当数据协调选择正向协调方案时，Eve与Alice端的互信息表示为：

$$I_{AE}=\frac{1}{2}\log_2\frac{V_E}{V_{E|A}}=\frac{1}{2}\log_2\left[1+\frac{V_A}{(1+\chi_{tot})/\chi_{line}}\right]\ , \tag{14}$$

因此后处理采用直接协调时提取的安全密钥量为：

$$\Delta I_{dR}^{in}=\beta I_{AB}-I_{AE}\ , \tag{15}$$

式中 β 为Alice与Bob之间的协调效率，取 $\beta=1$ 代入(14)式、(15)式可得：

$$\Delta I_{dR}^{in}=\frac{1}{2}\log_2\frac{\chi_{tot}+V}{1+V\chi_{line}+\chi_{hom}}\ , \tag{16}$$

当数据协调选择逆向协调时，Alice根据Bob发送的纠错信息估计密钥串，并结合已有的边信息作为辅助协调。由于信息传递方向的改变，因而不能像正向协调直接计算密钥量，需要在一定条件下对Bob端信息熵进行估算。Eve获得的信息量可以通过测量Bob端的方差 V_B 和条件方差 $V_{B|E}$ 计算得出：

$$I_{BE}=\frac{1}{2}\log_2\frac{V_B}{V_{B|E}}\ , \tag{17}$$

式中条件方差 $V_{B|E}=\eta\left[\frac{1}{T(1/V+\chi_{line})}+\chi_{hom}\right]$，结合(16)式可以得到逆向协调情况下的安全密钥量：

$$\Delta I_{rR}^{in}=\beta I_{AB}-I_{BE}\ . \tag{18}$$

假设实验中采用理想条件，即不考虑信道中的额外噪声和零拍探测损耗时，在个体攻击中直接协调与逆向协调方案中，Alice与Bob端所取得的安全密钥量与信道透射系数 T 的关系如图5所示。

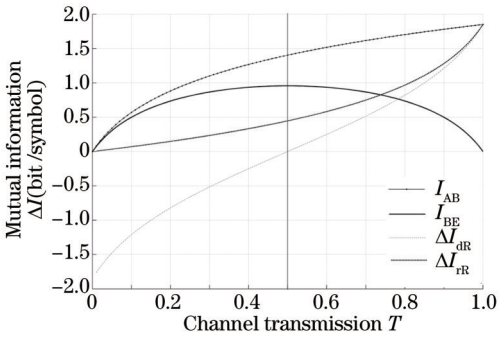

图5 互信息量与信道透射率关系曲线

Fig.5 Relationship between mutual information and the channel transmission

由图5可知，当信道透射系数 $T\leqslant 0.5$ 时，采用直接协调方案得到的密钥量 $\Delta I_{dR}^{in}<0$，即存在3dB的极限。只有当 $T>0$ 时，Alice与Bob之间才能有效提取安全密钥。而逆向协调方案突破了这个极限，无论信道的衰减量有多少，通信双方总能取得安全密钥。例如若在1550 nm波段工作的光纤按衰减常数 $\alpha=0.21$dB/km，实验系统采用 $L=25$ km长的标准单模光纤，计算得到的信道透射率 $T=10^{(-\alpha L/10)}=0.299<0.5$，因此直接协调下不能安全提取密钥。在下面的实验方案讨论中只采用逆向协调方案。

如果第三方采用集体攻击窃取信息，则窃听者Eve对Alice端与Bob端在完成数据协调纠错后，对获得的信息进行相干态测量。此时Eve所获得的互信息上界 χ_{BE}，不再由香农信息熵给出，而是由Holevo限[19]给出：

$$\chi_{BE}=S(\boldsymbol{\rho}_E)-\int p(x_B)S(\boldsymbol{\rho}_E^{x_B})\mathrm{d}x_B\ , \tag{19}$$

式中 $\boldsymbol{\rho}_E$ 为Eve测量的量子态由密度矩阵来表示，$\boldsymbol{\rho}_E^{x_B}$ 表示Eve以Bob测量结果 x_B 为条件的密度矩阵，$p(x_B)$

为Bob测量结果的概率分布，S函数为量子态ρ的冯·诺依曼熵，当ρ满足高斯形态时S函数为：

$$S(\rho)=\sum_i G\left(\frac{\lambda_i-1}{2}\right), \tag{20}$$

式中$G(x)=(x+1)\log_2(x+1)-x\log_2 x$，$\lambda_i$是高斯态协方差矩阵$\boldsymbol{\gamma}_{\mathrm{AB}}$的特征值，而在高斯协议中$p(x_{\mathrm{B}})$与测量结果$x_{\mathrm{B}}$相互独立，熵$S(\rho_{\mathrm{B}})$可以由协方差矩阵$\boldsymbol{\gamma}_{\mathrm{AB}}$特征值给定：

$$\boldsymbol{\gamma}_{\mathrm{AB}}=\begin{bmatrix} V\cdot E & \sqrt{T(V^2-1)}\cdot\boldsymbol{\sigma}_Z \\ \sqrt{T(V^2-1)}\cdot\boldsymbol{\sigma}_Z & T(V+\chi_{\mathrm{line}})\cdot E \end{bmatrix}, \tag{21}$$

式中E为单位矩阵，$\boldsymbol{\sigma}_Z$为Pauli矩阵表示为$\boldsymbol{\sigma}_Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$，则矩阵$\boldsymbol{\gamma}_{\mathrm{AB}}$特征值$\lambda_1,\lambda_2$的表达式是：

$$\lambda_{1,2}^2=\frac{1}{2}(A\pm\sqrt{A^2-4B}), \tag{22}$$

式中$A=V^2(1-2T)+2T+T^2(V+\chi_{\mathrm{line}})$，$B=T^2(V\chi_{\mathrm{line}}+1)^2$，(20)式第二部分同样可以由特征值$\lambda_3,\lambda_4,\lambda_5$得出有：

$$\begin{cases}\lambda_{3,4}^2=\dfrac{1}{2}(C\pm\sqrt{C^2-4D})\\ \lambda_5=1\end{cases}, \tag{23}$$

式中$C=\dfrac{V\sqrt{B}+T(V+\chi_{\mathrm{line}})+A\chi_{\mathrm{hom}}}{T(V+\chi_{\mathrm{tot}})}$，$D=\dfrac{V\sqrt{B}+B\chi_{\mathrm{hom}}}{T(V+\chi_{\mathrm{tot}})}$，则Holevo限可以改写为：

$$\chi_{\mathrm{BE}}=\sum_{i=1}^{2}G\left(\frac{\lambda_i-1}{2}\right)-\sum_{i=3}^{5}G\left(\frac{\lambda_i-1}{2}\right), \tag{24}$$

因而当高斯集体攻击下采用逆向协调方案时，能提取的安全密钥量的表达式为：

$$\Delta I_{\mathrm{rR}}^{\mathrm{co}}=\beta I_{\mathrm{AB}}-\chi_{\mathrm{BE}}. \tag{25}$$

4 实验仿真结果与分析

在数据协调过程中，由于受到香农极限的限制，协调效率β的值不可能达到100%，因此需要选择合适的码率以及校验矩阵来提高纠错效率，增加密钥提取的安全性。对协调效率进行估算：

$$\beta=\frac{H(\hat{Y})-m+\sum_{i=1}^{m}R_s^i}{I_{\mathrm{AB}}}, \tag{26}$$

式中$H(\hat{Y})$为信息量化后的信息熵，m表示映射层数，R_s^i表示各级码率，I_{AB}表示Alice与Bob之间的互信息，可以看出协调效率与各级码率密切相关。所使用硬件平台是CPU为Inter Xeon E5620 2.4GHz、内存为32G的双核服务器，选择分组码长为2×10^5，概率译码的最大迭代次数设为100，共分为10组进行统计实验仿真。根据前面给出的分层纠错协调，采用$m=4$层的映射方案，前两级不作编码处理，直接公开通过经典信道传输。第三级码采用Mackay所提出的随机搜索[20]的构造的非规则LDPC码，第四级码采用林舒所提出的代数方法构造LDPC码[21]。根据收敛信噪比结合理论分析各级最佳码率，通过实验仿真时的实际译码收敛情况选择第三级码率R_3为0.1、0.2、0.3、0.45分别与第四级码率R_4为0.8、0.9、0.95、0.98的组合方案。而校验矩阵H_3、H_4采用稀疏矩阵的结构，在计算机中以双向循环链表形式进行数据存储[22]，这样有效节约了内存空间，提高运算的效率。表1是三、四级校验矩阵采用上述4种不同的码率组合方案，得到的实验结果。

通过表1可得，收敛信噪比R_{SN}从3.2 dB增加到了6.5 dB，这是由于方案中三、四级码率的增加使得非规则LDPC码携带的校验信息减少，在级间译码迭代过程中一些置信信息错误不能得到更正，导致其收敛性能降低。随着码率增加，平均译码迭代次数(Average_L)从72.5降低到了60以下，而译码时间(Per_time)同样从55 s降低到30 s以下，说明码率的增加能带来一定程度上译码速率的提升，这与文献[14]中的变化是一致的。通过设计不同的码率组合，采用三、四级码率为0.3、0.95的协调方案，协调效率$\beta_{\max}$可以达到91.2%，相比文献[15]中效率有所提高。根据(26)式可知当三、四级码率越大时，协调效率越高，但此时收敛信噪比较高，影响了密钥的传输距离。当码率减小时，收敛信噪比降低，由香农信息理论可知Alice与Bob之间的互信

息减小，而协调效率相应增大，但此时额外增加了时间的开销，从而影响了整个系统的密钥分发效率。因此实际的协调方案选择需要综合考虑。

表1 不同方案下的有关参数

Table 1 Parameters at the different schemes

Scheme	R_3/R_4	R_{SN} /dB	Average_L	Per_time /s	β_{max}
1	0/0/0.1/0.8	3.2	72.5/36.8	55.04	89.3%
2	0/0/0.2/0.9	4.1	65.8/41.7	38.37	86.5%
3	0/0/0.3/0.95	5.0	42.6/24.7	35.26	91.2%
4	0/0/0.45/0.98	6.5	51.9/38.4	27.13	85.1%

图6为集体攻击的方式下，不同协调效率的有效密钥量随着信噪比的变化曲线。实验仿真中，选择接近理想高斯信源的调制方差值 $V_A = 18.9N_0$，系统热噪声 $\nu_{el} = 0.0436N_0$。由于Bob端采用零差探测方法，其光分束器的损耗，以及放大器和光电检测管灵敏度会影响系统的检测效率，探测效率取 $\eta = 0.6$。为了提高密钥分发安全性同时考虑实际可操作性，信道的额外噪声取 $\varepsilon = 0.005N_0$，信道透射率采用25 km下的标准单模光纤参数 $T = 0.302$。图6中协调效率从0.7变化到1.0,在一定信噪比下，Alice端发送的密钥信息经过后处理技术使得Bob端得到的信息误码率降低，随之有效密钥量曲线不断上升。当在较高的信噪比情况下，信道噪声较低，结合密钥分发的安全性理论可知Eve能够获得Bob端较多的密钥信息，导致合法通信双方的密钥信息减小，有效密钥量曲线随之降低。因而在一定信噪比下，协调效率必须大于一定值，通信双方才能进行安全的密钥交换。由图6可得在信噪比 $f_{SNR} > 4.0$ dB 情况下，当协调效率低于87%时，由集体攻击下的安全密钥量表达式可知，泄露给窃听者Eve的信息量 χ_{BE} 大于Alice和Bob之间传输的密钥 βI_{AB}，即不满足安全通信准则，此时密钥分配失败。同样在信噪比 $f_{SNR} > 5.0$ dB 时，协调效率不能低于88%。通过比较上述实验方案，只有方案一和三能够在集体攻击下提取到安全密钥。根据逆向协调下的安全密钥计算公式可得，个体攻击下 $I_{AB} = 361.67$ kbit/s，$I_{BE} = 320.38$ kbit/s，集体攻击下 $\chi_{BE} = 325.86$ kbit/s，采用方案三，个体攻击下最终获得的安全密钥为 $\Delta I_{rR}^{in} = 9.46$ kbit/s，集体攻击下的安全密钥量 $\Delta I_{rR}^{co} = 3.98$ kbit/s。因此即使在信道衰减程度较大的情况下，方案三也能保证其密钥分发的安全性。

图7是采用方案一时正向协调与逆向协调下的密钥量随距离的变化曲线。当通信双方的距离增加时，Bob端所接受的量子态信息幅度减弱，误码率增加，导致安全密钥量快速下降。根据CVQKD的安全理论可知，在正向协调时当信道衰减大于3 dB即 T<0.5时，Eve采用分束攻击就能得到比Bob更多的密钥信息，此时密钥分发是不安全的。由图7可知，正向协调受到3 dB约束下密钥只能安全传输不到10 km，而采用逆向协调，安全距离可以达到30 km左右，相比正向协调提高了安全通信距离。

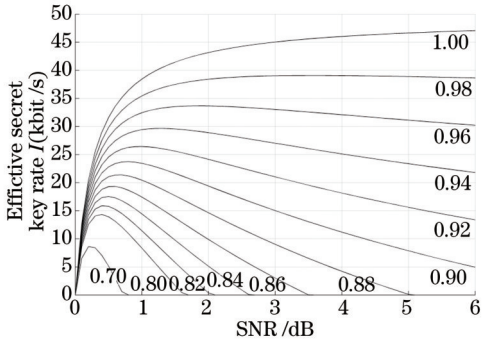

图6 不同协调效率下密钥量与信噪比的关系曲线

Fig.6 Relationship between secret key and SNR at different efficiency

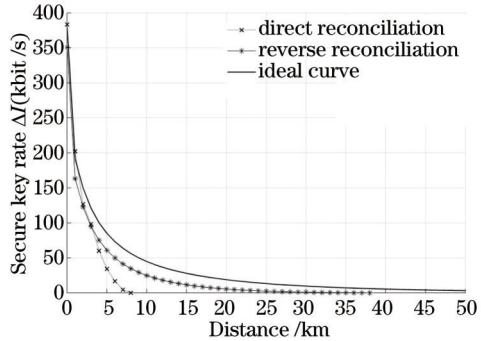

图7 不同协调方案下密钥量与传输距离关系曲线

Fig.7 Relationship between secret key and transmission distance

5 结 论

采用了基于分层纠错协议下准循环LDPC码与传统LDPC相级联的数据协调方案，并采用逆向高斯CV-QKD方案进行数据仿真，在连续变量为 2×10^5 的分组实验中，协调效率可达91.2%。通过CV-QKD的实验

计算得到,个体攻击下的安全密钥为 9.46 kbit/s ,而在最优高斯集体攻击下可以提取安全密钥为 3.98 kbit/s ,密钥的传输距离达到30 km,证明了方案中数据协调的安全性和可靠性。

信噪比影响着密钥的传输距离,因而想要对数据协调进一步的优化,必须实现在低信噪比SNR下协调效率的提升。此外高斯量化也影响着有效密钥的生成效率,下一步工作就是对非高斯调制的研究以及后处理技术GPU上的实现以提高数据吞吐量。

参 考 文 献

1 Hoi Kwong Lo, Hoi Fung Chau. Unconditional security of quantum key distribution over arbitrarily long distances[J]. Science, 1998, 283 (5410): 2050-2056.

2 Huang Chunhui, Wang Xuejin. Research and prospect on continuous variable quantum communication[J]. Journal of Electronic Measurement and Instrument, 2014, 28(1): 1-9.
黄春晖, 王雪津. 连续变量量子通信的研究与展望[J]. 电子测量与仪器学报, 2014, 28(1): 1-9.

3 Liu Youming, Wang Chao, Huang Duan, *et al*.. Study of synchronous technology in high-speed continuous variable quantum key distribution system[J]. Acta Optica Sinica, 2015, 35(1): 0106006.
刘友明, 汪 超, 黄 端, 等. 高速连续变量量子密钥分发系统同步技术研究[J]. 光学学报, 2015, 35(1): 0106006.

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

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

6 Anthony Leverrier, Philippe Grangier. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation[J]. Physical Review A, 2011, 83(4): 042312.

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

8 Fabian Furrer, Torsten Franz, Mario Berta, *et al*.. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks[J]. Physical Review Letters, 2012, 109(10): 100502.

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

10 Angelos D Liveris, Zixiang Xiong, Costas N Georghiades. Compression of binary sources with side information at the decoder using LDPC codes[J]. Communications Letters IEEE, 2002, 6 (10): 440-442.

11 Ahmed Attia Abotabl, Aria Nosratinia. Multi-level coding and multi-stage decoding in MAC, broadcast, and relay channel[C]. IEEE International Symposium on Information Theory, 2014, 2014: 96-100.

12 Guo Dabo, Liu Gang, Zhang Ning, *et al*.. Reverse reconciliation 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.

13 Juane Li, Keke Liu, Shu Lin, *et al*.. Algebraic quasi-cyclic LDPC codes: construction, low error-floor, large girth and a reduced-complexity decoding scheme[J]. IEEE Transactions on Communications, 2014, 62(8): 2626-2637.

14 Dabo Guo, Yanhuang Zhang, Yunyan Wang. 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.

15 Lu Zhixin, Yu Li, Li Kang, *et al*.. Reconciliation for continuous variable quantum key distribution based on reverse reconciliation[J]. Science China Physics, Mechanics and Astronomy, 2009, 39(11): 1606-1612.
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: 物理学, 力学, 天文学, 2009, 39(11): 1606-1612.

16 Song Hanchong, Gong Lihua, Zhou Nanrun. Continuous-variable quantum deterministic key distribution protocol based on quantum teleportation[J]. Acta Physics Sinica, 2012, 61(15): 154206.
宋汉冲, 龚黎华, 周南润. 基于量子远程通信的连续变量量子确定性密钥分配协议[J]. 物理学报, 2012, 61(15): 154206.

17 Xinlu Zhi, Yu Li, Kang Li, *et al*.. Reverse reconciliation for continuous variable quantum key distribution[J]. Science China Physics, Mechanics and Astronomy, 2010, 53(1): 100-105.

18 Chen Yan, Shen Yong, Zou Hongxin. An all-fiber continuous variable quantum key distribution based on multi-bits coding of single pulse[J]. Acta Optica Sinica, 2015, 35(7): 0727001.

陈 岩, 沈 咏, 邹宏新. 基于单脉冲多位编码的全光纤连续变量量子密钥分发[J]. 光学学报, 2015, 35(7): 0727001.

19 Xiangchun Ma, Shihai Sun, Musheng Jiang, *et al*.. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution[J]. Physical Review A, 2013, 89(4): 042335.

20 David J C MacKay. Good error-correcting codes based on very sparse matrices[J]. IEEE Transactions on Information Theory, 1999, 45 (2): 399-431.

21 Yingyu Tai, Lan Lan, Lingqi Zeng, *et al*.. Algebraic construction of quasi-cyclic LDPC codes for the AWGN and erasure channels[J]. IEEE Transactions on Communications, 2006, 54(10): 1765-1774.

22 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.

栏目编辑：刘丰瑞