中国科学 G 辑: 物理学 力学 天文学 2009 年 第 39 卷 第 11 期: 1606 ~ 1612
www.scichina.com phys.scichina.com
《中国科学》杂志社
SCIENCE IN CHINA PRESS

基于逆向协调的连续变量量子密钥分发数据协调

逯志欣[①*], 于丽[①], 李康[①], 刘炳灿[②], 林建桂[①], 焦荣珍[①], 杨伯君[①]

① 北京邮电大学理学院, 信息光子学与光通信教育部重点实验室, 北京 100876;
② 北京装甲兵工程学院基础部, 北京 100072
* E-mail: lzx_159@sohu.com

收稿日期: 2009-05-04; 接受日期: 2009-07-21
国家自然科学基金(批准号: 60578043)和北京市教委共建项目(编号: XK100130937)资助

摘要 采用低密度奇偶校验码(LDPC)实现了逆向协调的连续变量量子密钥分发的仿真研究. 采用多级编码/多级译码结构的协调校验方案, 充分利用矢量量化、迭代译码等优化技术, 并结合最逼近仙农极限的信道编码, 实现了高效率的逆向协调算法. 通过仿真计算, 最终能够实现 20 km 单模光纤中 2.2 kb/s 的密钥传输速率, 编码效率达到 0.89, 并且仍有很大的提高余地.

关键词
量子通信
密钥分发
逆向协调
低密度奇偶校验码

在密码学中, 通信双方可以通过共享密钥来保证通信安全. 通信双方共享一组密钥的过程就是密钥分发, 经典密钥分发只能做到有条件下的安全. 根据量子信息理论, 可以设计出具有无条件安全性的密钥分发方案. 以单光子为信息载体的量子密码分发系统, 尚无安全可靠的单光子源, 且探测效率比较低. 与之相反, 基于连续变量的量子密码通信不仅具有稳定可靠的光源, 探测效率高, 而且其系统与常规经典通信系统相容, 目前基于连续变量量子密钥分发已成为量子信息科学中研究热点之一.

在连续变量量子密钥分发安全性方面, 常见攻击方式包括个体攻击、集体攻击和相干攻击, 其中集体攻击是最佳的攻击方式[1], 其安全性已经得到证明[2,3]. 在连续变量密钥分发系统中, 可以采用二进制调制[4]或高斯调制. 前者突出的优点是易于操作, 密钥提取方便. 虽然后者噪声性能差、纠错复杂, 但是可以采用多进制提取密钥, 增大密钥速率, 因此只要找到纠错性能和处理效率优良的纠错码, 就可以克服高斯调制的缺点, 提高密钥传输率.

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, 由校验矩阵决定其特性, 它的校验矩阵是一种稀疏矩阵, 即矩阵中非零元素要远远少于零元素, 这种稀疏性能够保证构造出低复杂度、高性能的好码. 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、实用灵活、具有较低的错误平台等优点. 基于LDPC码的协调方案理论上能够达到最佳性能[5]. 但对于长距离密钥传输而言, 如文献[6]所述当传输距离很长(100 km)其密钥的提取难度很大, 为实现长距离密钥传输, 目前已有很多关于可信中继的研究[7~9], 在实际中可结合高效后处理技术和可信中继办法实现长距离高效密钥传输.

本文首先从理论上给出了影响量子密钥分发系统安全性的物理参数, 并结合实际情况给出了较为理想并且可行的参考数据, 根据这些数据提出了安全的协调方案需要满足的条件. 最后, 本文详细介绍

引用格式: 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. 中国科学 G 辑, 2009, 39(11): 1606—1612
Lu Z X, Yu L, Li K, et al. Reverse reconciliation for continuous variable quantum key distribution. Sci China Ser G, doi: 10.1007/s11433-010-0069-2

了基于LDPC码的逆向协调的设计过程, 并通过仿真计算出 20 km 单模光纤中 2.2 kb/s 的密钥传输速率, 编码效率达到 0.89.

1 仿真系统参数设定

在连续变量的量子密钥分发系统中, 一般通过光场的正则位置和动量加载信息. 压缩态、纠缠态对各种损耗极为敏感, 难于实现长距离传输, 而相干态则易于保持. 本方案以相干态为信息载体实现量子密钥分发. 密钥分发过程可分为两个阶段, 量子通信阶段和经典通信阶段, 前者用于密钥的传输, 后者用于经典信息的处理, 系统如图 1 所示.

该仿真模型由发射方Alice、接收方Bob、量子信道和经典信道四部分组成. 计算中, 光源是重复频率 500 kHz、工作波长 1550 nm的激光器, 量子信道为 20 km长的单模光纤. 首先, 发射方Alice随机地对处于真空态光场的振幅分量x和相位分量p进行调制, 产生的信号光通过量子信道发送给Bob, 其中x和p是均值为零、方差为$V_A N_0$满足高斯分布的随机变量, N_0是作高斯分布的真空噪声功率, 我们取V_A=12. 接收方Bob对收到的信号进行探测, 随机地测量x或p分量, 并通过经典信道公布测量基给Alice进行数据筛选. 然后通信双方再利用经典信道交换部分数据, 判断通信是否安全有效. 若通信有效, 则继续进行密钥提取.

理论分析表明[10,11], 在个体攻击下逆向协调和集体攻击下逆向协调, 相应的安全判据分别为

$$\Delta I_{RR}^{\text{indi}} = I_{AB} - I_{BE} = \frac{1}{2}\log_2\left(\frac{1/\left[T\left(\chi_L + \frac{1}{V}\right)\right] + \chi_H T}{T(1+\chi_T)}\right), \quad (1)$$

$$\Delta I_{RR}^{\text{coll}} = I_{AB} - \chi_{BE},$$

且

$$\chi_{BE} = S(\rho_E) - \int P(B) S(\rho_{E|B}) \mathrm{d}B, \quad (2)$$

其中$V = 1 + V_A$为Alice端发送信号的等效功率; T 为光纤信道传输率; χ_L, χ_H 和 χ_T 分别为量子信道、平衡零拍探测系统和整个系统在Alice输出端的等效噪声; ρ_E, $\rho_{E|B}$ 分别为Eve的密度矩阵和相对于接收者Bob的条件密度矩阵, $S(\rho)$为Von Neumann熵, 满足 $S(\rho) = -Tr(\rho \log_2 \rho)$, $P(B)$是Bob测量结果的概率分布.

研究表明采用直接协调方案存在一个 3 dB 极限, 即只有在信道传输率 $T > 0.5$ (信道衰减小于 3dB)时, 密钥分发是安全的. 对于逆向协调方案, 则突破了这个限制. 若采用长距离的标准单模光纤作为量子信道时, 信道损耗往往会大于 3 dB, 故在我们以下的分析中采取逆向协调方案.

量子信道噪声包括信道损耗和额外噪声两部分, 其中额外噪声ε对密钥分发的限制比较大. 理论上与窃听者的克隆攻击、调制技术不完善和光源的相位噪声等问题紧密联系, 实验中很难精确计算, 但实际操作时可以通过增加一定的额外通信开销, 利用数据处理软件实现估算. 若暂不考虑探测损耗, 根据(1)和(2)式可以得到密钥分发速率(互信息ΔI)与线路额外噪声ε的关系, 如图 2 所示.

为确保密钥分发的安全性, 同时考虑到实际可操作性, 理论分析时选择 $\varepsilon = 0.05$. 接收方 Bob 采用平衡零拍探测系统测量光信号, 探测器的探测效率 $\eta \geqslant 0.6$, 探测系统引入的额外噪声 $\upsilon \leqslant 0.05$, 至此可以得到 Bob 端接收信号的信噪比 SNR 为 3.32 dB,

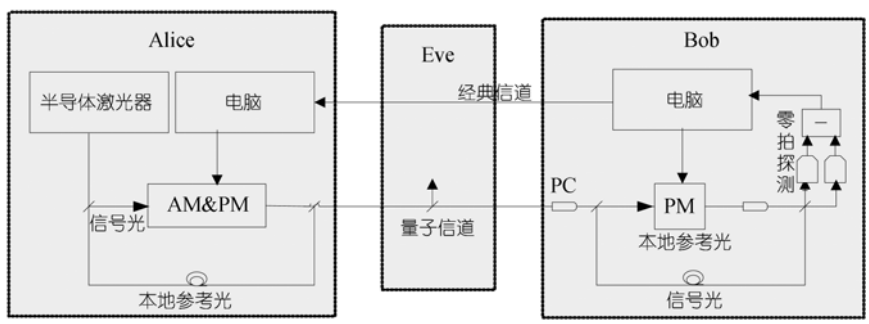

图 1 基于连续变量的量子密钥分发系统

AM 为幅度调制, PM 为相位调制, PC 为偏振控制器

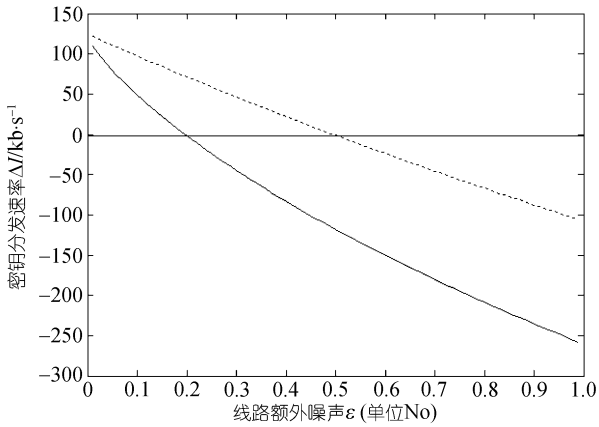

图 2　密钥分发速率(互信息ΔI)与线路额外噪声ε的关系

虚线为 ΔI_{RR}^{indi}，实线为 ΔI_{RR}^{coll}

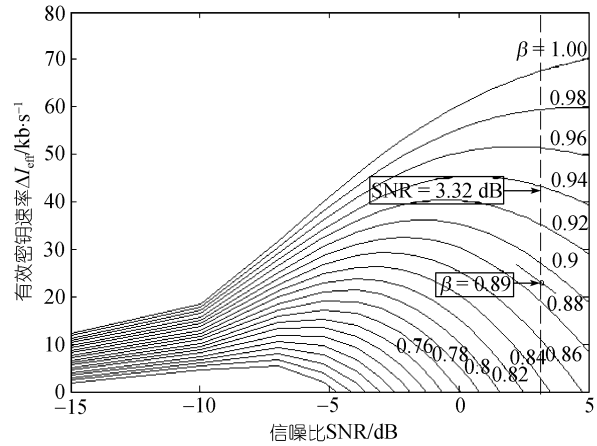

图 3　协调效率β、信噪比 SNR 和有效密钥速率之间的关系

同时有 $\Delta I_{RR}^{\text{indi}} = 67.8$ kb/s, $\Delta I_{RR}^{\text{coll}} = 50.4$ kb/s. 但是这些数据含有大量的冗余信息，如窃听者所窃取的信息，噪声误码等，需要经过协调纠错和密性放大进行蒸馏处理，以提取最终密钥. 密性放大[12]作为目前非常成熟的技术，本文就不做讨论. 本文主要通过数值仿真分析逆向协调过程.

2　计算仿真

协调部分包括信源编码和信道编码两部分，根据信息理论，它们都会带来一定的密钥损失，损失程度决定了最终密钥的安全性，这就引入了一个协调效率的概念，用来表示协调系统的密钥损失率.

2.1　估算协调效率β

可令β($\beta<1$)代表整个协调过程的效率，此时个体攻击和集体攻击下逆向协调的安全判据则变为

$$\begin{aligned}\Delta I_{\text{eff}}^{\text{indi}} &= \beta I_{AB} - I_{BE},\\ \Delta I_{\text{eff}}^{\text{coll}} &= \beta I_{AB} - \chi_{BE}.\end{aligned} \tag{3}$$

由于β主要是作用于I_{AB}，对窃听者影响不大，所以个体攻击与集体攻击的分析十分类似，本文以考虑个体攻击为例，探讨最大协调效率β和计算出密钥传输速率. 根据(3)式协调效率β和Bob端信噪比SNR对密钥分发的影响如图 3 所示.

如图 3 中虚线所示，在 SNR 为 3.32 dB 处，为保证安全密钥的生成，要求总协调效率β不得低于 0.84. 在下面的分析中，我们最终会给出β高达 0.89 的协调方案设计，足以满足要求.

2.2　设计协调方案并仿真

已有的协调方案包括 Bennett 方法, CasCade 方案等. Bennett 的方法效率不高，而且每一步还要丢弃比特; CasCade 采用二分查找算法，它是 Alice 和 Bob 通过交互式讨论查找错误的一种方法，这种双向通信会导致 Alice 和 Bob 的信息同时泄露给 Eve. 由于我们采用连续变量调制信号，无论是在速率还是误码率上都要求更高，同时也希望信息泄露尽可能少，故本仿真方案采用 MultiLevel Coding/MultiStage Decoding (MLC/MSD)结构的协调系统，如图 4 所示，它是单向通信，即只需 Bob 发送纠错信息给 Alice，有效控制了 Alice 的信息泄露.

多级编码(MLC)又被称为“带宽有效性编码”，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的核心思想是要用不同级上的不同码率对不同权重的信息位进行最有效的保护. 对于MLC系统来说，分量码的纠错性能越好，MLC系统的抗干扰性能就越优良. 这里分量码选择性能优良的LDPC码，它强大的纠错能力非常适合噪声性能极不理想的连续变量量子密钥分发系统.

无论对分组码还是卷积码，最佳的译码方案都是建立在最大似然译码(MLD)准则基础之上的，但是当方案中码字信息位较大时，译码过程就变得异常

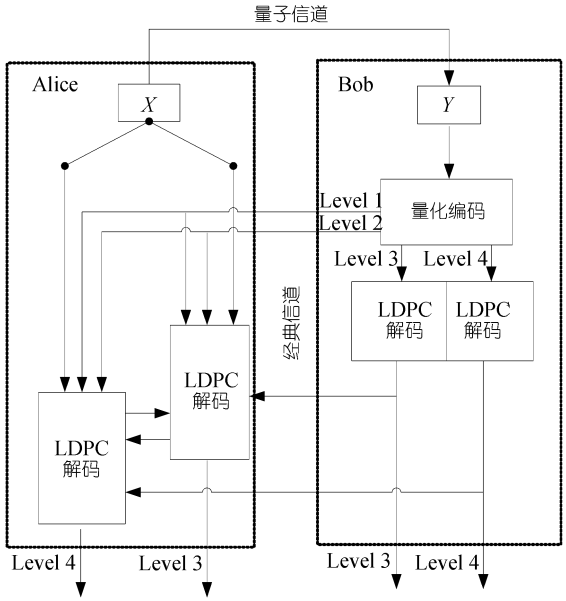

图 4 基于 LDPC 码的多级协调框图

复杂而不切实际, 此时在 MLC 方案中, 一般采用准最佳或改进的译码方案, 以求在性能和复杂度之间折中. 研究表明, 多级译码(MSD)是适合 MLC 的准最佳译码方法.

仿真中采用 16 进制量化、4 bit编码, 如图 4 所示. Bob先对接收到的大量连续信号量化, 每个信号脉冲对应一个 4 比特码本, 所有码本相同信息位(Level)的比特组成一组比特流, 即共 4 组比特流, 然后对这些比特流分别进行编码[14].

在 Alice 端采用的是迭代译码方法, 即前一级的译码结果作为后级译码的输入, 如此循环反复, 以使解码效果达到最好, 如图 4 所示, 同时可以通过 EXIT 曲线来分析译码器的收敛性[15]. 本文用 Y 和 $\hat{Y}$ 分别表示Bob接收到的高斯型信号和量化后的离散信号, X 表示Alice发送的连续高斯型信号. 此时信息位 i ($1 \leqslant i \leqslant 4$, 1 代表最低位, 4 为最高位)所携带的密钥可以表示为 $I_{Li} = I\left(X; L_i \mid L_1, ..., L_{i-1}\right)$.

协调原理采用的是边信息(side information)纠错方法[14], 具体过程如图 5 所示. Bob对零差探测接收到的离散的、连续取值的高斯分布信号先进行量化编码, 转化为二进制数据流, 接着与LDPC码的校验矩阵H相乘, 得到校验S(syndrome), 校验子的大小由码率决定: 码率越小, 校验子越长; 然后Bob通过理想经典信道将S传输给Alice; 最后Alice将自己已有的原始数据结合接收到的校验子S, 联合译码, 并猜测出Bob的值. 在这个过程中, 通信公开的信息压缩至S, 对有用信息没有过多透露, 从而最大程度保护了最终密钥量.

2.2.1 信源编码

由图 5 所示, 信源编码就是Bob对接收到的连续信号进行量化并映射为二进制数据的过程, 其关键是量化空间和码本的选择. 研究表明[16], 如果能够满足 X 和 Y 的联合概率分布具有对称性, 理论上可以找到最好的LDPC码, 也即可以最大程度提高信道编码的效率. 仿真中码本选取具有对称性的自然码. 量化空间的选择则参考了Lloyd和Max提出的最佳量化器及矢量量化的思想. 理论上, 量化必然会带来一定的信息损失, 即 $I(X;\hat{Y}) < I(X;Y)$, 但是这种差距是可以减小至可容忍范围里的[17], 为了达到这种效

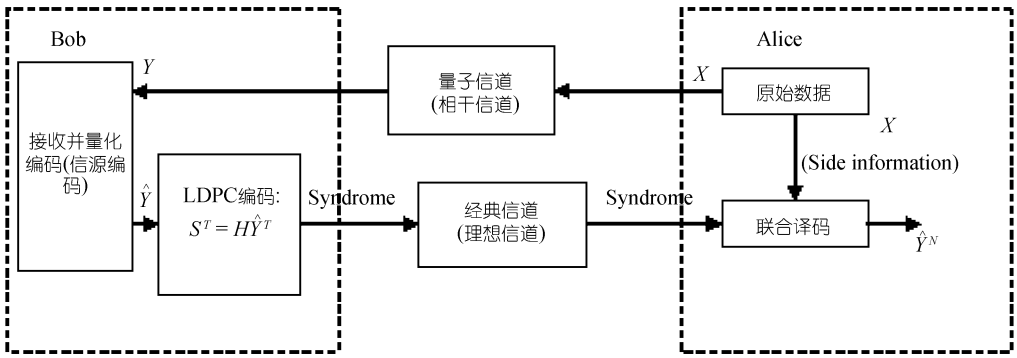

图 5 基于 LDPC 码的边信息纠错原理

果, 可以将最大化有效密钥速率(互信息 $I(X;\hat{Y})$)作为设计量化空间的判断条件, 其中

$$I\left(X;\hat{Y}\right)=I\left(X;L_1,L_2,L_3,L_4\right)=\sum_{i=1}^{4}I\left(X;L_i\mid L_1,...,L_{i-1}\right),\tag{4}$$

量化空间同时还要满足对称性. 通过计算推演, 并以不高于 2%的量化损失作为阈值, 最后选择的量化空间见表 1.

2.2.2 信道编码

信道编码就是对二进制数据进行纠错编码和译码. 仿真方案中LDPC编码部分较为简单, 直接由比特串与校验矩阵相乘得到校验子, 如图 5 所示, 所以信道编码的关键是Alice的译码. 译码算法的优劣决定了码本身的纠错潜力能否被最大程度地发挥出来, 同时算法复杂度也决定了实现的可行性. 基于概率的BP算法属于逐符号软判决译码, 它由校验矩阵决定, 在码长较长时性能可逼近Shannon极限, 但实现复杂度较高. 我们采用改良的基于对数域译码的对数似然比(LLR) BP算法[14], 它把大量乘法运算变换成了加法运算, 极大地减少了运算时间, 但具体算法的实现仍然取决于校验矩阵. 因此, 关键是要设定每个信息位所对应的码率, 然后根据码率和码长由计算机搜索得到具体的校验矩阵. 根据经典信息论, 每个信息位所含密钥信息还可以表示为

$$I_{Li}=I\left(X;L_i\mid L_1,...,L_{i-1}\right)=H\left(L_i\mid L_1,...,L_{i-1}\right)-H\left(L_i\mid X,L_1,...,L_{i-1}\right).\tag{5}$$

由上式及结合对信源编码和多级译码过程的联合分析, 仿真得到每个信息位所携带的密钥信息 I_{Li} 与量化前 Bob 端接收信号的信噪比 SNR 的关系, 如图 6 所示.

从图中可以看到, 当 SNR<10 时, 信息位越低所携带的密钥信息就越少. 本方案中 SNR=3.32 dB, 据图 6 可以计算各信息位所携带的密钥信息分别为

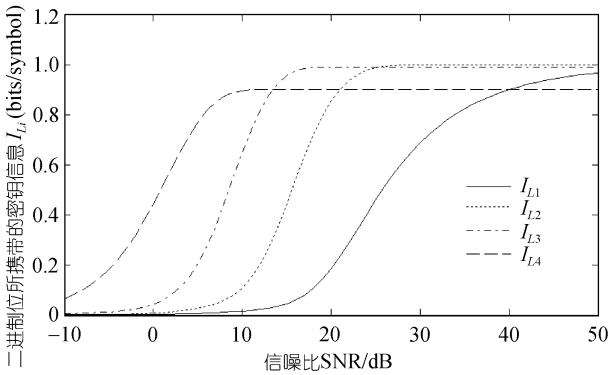

图 6 I_{Li}与信噪比SNR的关系

$I_{L1}=0.0040$ bits/symbol, $I_{L2}=0.0165$ bits/symbol, $I_{L3}=0.1201$ bits/symbol, $I_{L4}=0.6706$ bits/symbol.

此时 Bob 端的量化损失为 $\Delta=I_{AB}-\sum I_{Li}=0.0159$ bits/symbol, 对系统影响很小(约为 I_{AB} 的 1.9%), 可以容忍, 其中 $\sum I_{Li}=I(X;\hat{Y})$. 同时, 如果完全公开传输低两位, 见图 4, 此时带来的额外损失只有 0.0205 bits/symbol, 对协调效率的影响可以接受, 而实际上, 这样处理后减少了耗时, 反而有利于提高密钥传输速率, 所以我们选择不对其编码, 直接公开传输, 这里充分利用了 MLC 系统码率可调的优点来重点保护信息量大的信息位.

最佳码率公式为

$$R_{Li}^{opt}=1-(I_{L\inf}-I_{Li}),\tag{6}$$

式中 $I_{L\inf}$ 是 $SNR\to\infty$ 时, 信息位 i 所携带的理想密钥信息, $(I_{L\inf}-I_{Li})$ 就是实际中需要排除的冗余信息. 根据图 6 可以计算各信息位的最佳码率分别为

$$R_{L1}^{opt}=0.004,\quad R_{L2}^{opt}=0.016,$$

$$R_{L3}^{opt}=0.127,\quad R_{L4}^{opt}=0.768.$$

可见高信息位的抗噪性能最好, 可以采用高码率传输, 低信息位则相反, 必须降低码率以换取纠错性能. 以上分析都是在理想情况下, 此时 Bob 只需传输冗余比特 $H(\hat{Y}\mid X)$ 就能实现理想纠错, 最佳效率

表 1 量化空间(量化区间为[–inf,b1], [b1,b2], ..., [b14,b15], [b15,inf])[a)]

–b1=b15=2.4603	–b2=b14=1.8952	–b3=b13=1.4791	–b4=b12=1.1332
–b5=b11=0.8051	–b6=b10=0.5388	–b7=b9=0.2663	b8=0

a) 设信号功率为 1, 单位No, SNR = 3.32 dB

$\beta^{opt} = I(X;\hat{Y})/I(X;Y) = 0.98$. 但是实际通信中, 信道编码受Shannon极限限制, 为了保证码的纠错性能, 只能降低编码效率. 此时通过增加传输的冗余比特即降低码率来实现, 结果导致协调系统的效率降低, 即 $\beta < \beta^{opt}$. 实际码率的选取需要评估与Shannon极限的差距, 这里有两种方法, 即Monte-Carlo仿真和高斯密度进化理论[11], 但是鉴于后者实用性太差, 而且复杂度也很高, 我们直接采用Monte-Carlo仿真法.

本方案选择不规则LDPC码作为信道码, 码长为200000. 校验矩阵H是LDPC码的核心, 直接影响到编码的性能. 但是由于H矩阵的选取具有很强的随机性, 实际中是很难找到最佳性能的矩阵. 由于随机LDPC码适合码长很长的码, 它参数设计灵活, 而且长的随机LDPC码具有逼近Shannon极限的能力. 我们采用Mackay随机构造法寻找比较理想的LDPC码. 设定码长为200000、码率和度的上下限(3~300)后, 由计算机搜索而得到. 仿真中选取的实际可操作码率为 $R_{L1}/R_{L2}/R_{L3}/R_{L4} = 0/0/0.11/0.73$. 为了达到更好的纠错性能, 还可以在LDPC编码器之后级联其他的信道编码, 如BCH码[11], 不过这同时也会引入一定系统开销, 如延时等. 译码仿真时, 可以根据EXIT曲线[15]分析迭代译码的收敛性, 从而选择最佳的迭代次数.

2.2.3 仿真结果

仿真选取的实际可操作码率为 $R_{L1}/R_{L2}/R_{L3}/R_{L4} = 0/0/0.11/0.73$, 又因 $I_{L\inf}$ 不变, 根据(6)式可以算出各信息位相对应的密钥信息 I_{Li}, 再结合式 $I(X;\hat{Y}) = \sum I_{Li}$ 和 $\beta = I(X;\hat{Y})/I(X;Y)$, 此时最终得到协调系统的效率 $\beta = 0.89$.

最终仿真结果是, 经过密性放大后, 密钥分发系统理论上可获得的安全密钥速率为: $\Delta I_{\text{eff}}^{\text{indi}} = \beta I_{AB} - I_{BE} = 22.3$ kb/s. 考虑到平均延时近 10 s, 仿真结果实际上能达到的最大密钥速率为: $\Delta I_{\text{eff}}^{\text{indi}} = 2.2$ kb/s.

3 结论

本文首先分析了连续变量量子密钥分发系统设计时的有关参数和基于现有实验条件的具体方案, 详细介绍了基于LDPC码的逆向协调方案的设计. 仿真结果表明, 该协调方案的效率能够达到 0.89, 并最终实现 2.2 kb/s 的理论密钥传输速率, 为以后的实验实现提供了很好的指导作用.

在上述的仿真计算中, 采用的传输距离为 20 km. 对于长距离密钥传输而言, 文献[6]指出逆向协调连续变量量子密钥分发的最小计算复杂度随着长度的增加指数增长, 若传输距离按 100 km 计算, 最终几乎提取不出安全密钥. 密钥率对传输距离很敏感, 在本文利用LDPC码作为协调方案的仿真中, 将传输距离设为100 km时, 同样也得不到安全密钥, 跟文献[6]的结论一致. 因此, 在实际中可结合高效后处理技术和可信中继办法实现长距离高效密钥传输.

我们注意到, 协调方案设计中, 量化编码还可以更加有效, 如采取多维矢量量化, 码本选择也可以不等长; LDPC 码校验矩阵生成时参数设定比较简单随机性太强, 需要更加有效的构造方法, 如比特填充法甚至代数构造法. 协调方案的改进是非常重要也比较困难的工作, 这正是接下来需要进一步努力的方向.

参考文献

1 Garcia-Patron P, Cerf N J. Unconditional optimality of gaussian attacks against continuous－variable quantum key distribution. Phys Rev Lett, 2006, 97: 190503[DOI]

2 Renner R, Cirac J I. A de Finetti representation theorem for infinite dimensional quantum systems and applications to quantum cryptography, arXiv: 0809.2243, 2008

3 Zhao Y B, Han Z F, Guo G C. Apply current exponential de Finetti theorem to realistic quantum key distribution. arXiv: 0809.2683, 2008

4 Zhao Y B, Heid M, Rigas J, et al. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. Phys Rev A, 2009, 79: 012307[DOI]

5 Shannon C. A mathematical theory of communication. Bell Syst Tech J, 1948, 27: 623—656
6 Zhao Y B, Gui Y Z, Chen J J, et al. Computational complexity of continuous variable quantum key distribution. IEEE Trans Inform Theor, 2008, 54: 2803－2807[DOI]
7 Elliott C. Building the quantum network. New J Phys, 2002, 4: 46-1—12
8 Wang W Y, Wang C, Zhang G Y, et al. Arbitrarily long distance quantum communication using inspection and power insertion. Chin Sci Bull, 2009, 54(1): 158—162[DOI]
9 Wen H, Han Z F, Zhao Y B, et al. Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network. Sci China Ser F-Inf Sci, 2009, 52(1): 18—22[DOI]
10 Grosshans F, Assche G V, Wenger J, et al. Quantum key distribution using Gaussian-modulated coherent states. Lett Nat, 2003, 421: 238—241[DOI]
11 Londewyck J, Block M, García-Patrón R, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. Phys Rev A, 2007, 76: 042305[DOI]
12 Bennett C H, Brassard G, Crépeau C, et al. Generalized privacy amplification. IEEE Trans Inform Theor, 1995, 41: 1915—1923[DOI]
13 Wachsmann U, Fischer R F H, Huber J B. Multilevel codes: theoretical concepts and practical design rules. IEEE Trans IT, 1999, July: 1361—1391[DOI]
14 Liveris A D, Xiong Z, Georghiades C N. Compression of binary sources with side information at the decoder using LDPC codes. IEEE Commun Lett, 2002, 6: 440—442[DOI]
15 Bloch M, Thangaraj A, McLaughlin S W, et al. LDPC-based Gaussian key reconciliation. In: Proc IEEE Inform Theor Workshop (Punta del Este, Uruguay), 2006. 116—120
16 Richardson T J, Shokrollahi M A, Urbanke R L. Design of capacity-cpproaching irregular low-density parity-check codes. IEEE Trans Inform Theor, 2001, 47: 619—637[DOI]
17 Assche G V, Cardinal J, Cerf N J. Reconciliation of a quantum-distributed Gaussian key. IEEE Trans Inform Theor, 2004, 50: 394—400[DOI]