文章编号:1004-4213(2011)12-1809-6

采用纠缠辅助量子 LDPC 码和检错重传策略的量子直传通信方案

邵军虎,白宝明

(西安电子科技大学 ISN 国家重点实验室,西安 710071)

摘 要:针对现有量子信息直传协议在有噪音量子信道下传输效率低及可靠性差的问题,提出了一种有效利用纠缠资源的量子安全直传通信方案.通过收发双方共享纠缠粒子作为辅助比特,采用纠缠辅助量子低密度校验码对量子态信息进行前向纠错保护,以提高系统在噪音环境下的传输可靠性.同时采用自动请求重传策略对量子态信息进行检错编码保护,当因窃听或强噪音导致译码获得的信息不正确时,则请求发端对该组信息进行编码重传操作.文中对所选用纠缠辅助量子低密度校验码在量子退极化噪音信道下的迭代译码性能进行了仿真,最后对方案的安全性进行了分析论证.

关键词:量子通信;量子纠错码;量子信息直传;量子自动请求重传

中图分类号:O431;TN911.22 **文献标识码**:A **doi**:10.3788/gzxb20114012.1809

0 引言

在量子信息领域中,量子安全直传通信(Quantum Secure Direct Communication, QSDC)实现了信源与信宿之间信息的确定性传输,属于真正意义上的量子通信方案.对于通信双方在无法事先建立共享密钥的环境下,QSDC 方案可以实现安全的直接量子信息传输.2002 年 BieGe 等人首次提出基于非纠缠单光子光源的量子安全信息直传方案[1],同年 Bostrom 和 Felbinger 提出基于 EPR(Einstein-Podolsky-Rosen)纠缠态的量子直传 Ping-Pong 协议[2].将密集编码思想、量子纠错码、纠缠交换等技术引入 QSDC 系统,许多改进的量子信息直传方案相继被提出[3-7].QSDC 方案的安全性是其优于经典信息传输的重要特点,针对 QSDC 方案在各种窃听策略下的安全性分析已有研究结果被提出[8-10],并且关于直传 Ping-Pong 协议的实验可行性也已有相关的研究报道[11].

通信的目的是实现信息在信源与信宿之间的可靠有效传输,有效性是对信息传输速率的要求,可靠性是对信息传输准确性的要求.对于现有的各种多步传输 QSDC 协议方案[12-13],其携载信息的粒子均为双向传输机制,并随机检测 EPR 纠缠对以达到防止窃听的安全通信.因此对于具有双向传输特点的 QSDC 方案,自动请求重传(Automatic Repeat-Request, ARQ)策略将是一种简单适用的后向纠错方案.然而在信道环境较差时,单纯的后向 ARQ 纠错会导致频繁的重传操作,从而降低系统的传输效率.因此,在 QSDC 方案中加入前向纠错技术即量子纠错码,对信息进行前向纠错编码处理,可降低 ARQ 的重传频率,提高 ARQ 系统的信息传输速率.

量子纠错码技术是保护量子信息对抗环境消相干噪音等影响的重要手段,已经成为量子通信、量子容错计算、量子纠缠提纯等应用中必不可少的组成部分.将经典通信领域中可逼近 Shannon 容量限的低密度校验(Low-Density Parity-Check, LDPC)码技术推广至量子信息领域,近年来关于量子 LDPC 码的构造及其译码算法涌现出了许多的研究结果[14-16].由于量子态信号的不可复制及不可直接测量等特点,稳定子理论成为当前研究量子纠错码的一种有效方法,且与经典纠错码有着直接的联系.而纠缠辅助量子纠错码利用收发双方预先共享的纠缠粒子资源,降低了标准稳定子码矩阵的约束条件,从而可以取得更好的迭代译码纠错性能[17].

本文基于现有 Ping-Pong 协议方案原理,提出一种采用纠缠辅助量子 LDPC 纠错码和 ARQ 策略的量子信息直传方案.采用纠缠辅助量子 LDPC 码

基金项目:国家自然科学基金(No. 60972046)资助

第一作者:邵军虎(1980—),男,博士研究生,主要研究方向为信道编码和量子信息纠错码.Email: jhshao@mail.xidian.edu.cn

导师(通讯作者):白宝明(1966—),男,教授,主要研究方向为信道编码、无线通信和量子通信.Email: bmbai@mail.xidian.edu.cn

收稿日期:2011-09-07;**修回日期**:2011-10-13

为前向纠错码，对一定噪音范围内可被纠正的编码量子态序列，进行实时纠错处理；同时当检错码检测到 Bob 的接收信息不正确时，则自动请求 Alice 对该组量子态信息序列编码重传，即后向纠错的量子 ARQ 策略. 对所选用的纠缠辅助量子 LDPC 码在量子退极化噪音信道下的迭代译码性能进行了 Monte Carlo 仿真，将退极化强度为 0.01 时的 10^{-2} 初始出错率降低到了 10^{-6} 以下. 量子通信的优势在于其由量子力学原理所保障的安全性，文中最后对该方案各环节的安全性进行了分析.

1 采用纠缠辅助量子 LDPC 码和 ARQ 策略的 QSDC 方案

1.1 系统原理框图

现有 QSDC 方案多为基于双向传输的 Ping-Pong 协议原理，该类方案在有噪音量子信道环境下，Alice 将携载信息的粒子回传给 Bob 所经过的量子信道非理想时，则必然会受到噪音的影响. 由于环境噪音和信道退极化噪音等引起的携载信息量子态出错或丢失，将导致大量纠缠粒子的无效利用，从而降低了 QSDC 的通信效率. 本文所提出的 QSDC 方案，引入纠缠辅助量子 LDPC 纠错码对回传量子态信息进行编码保护，同时采用检错 ARQ 策略对译码输出信息的正确性进行判断. 这种混合式的纠错机制（Hybrid-ARQ，HARQ）保障了 QSDC 通信系统的可靠性和有效性.

具体 QSDC 方案原理见图 1 中所示，主要包括建立安全纠缠信道、前向纠错（Forward Error Correction，FEC）、后向 ARQ 策略等三部分. 首先是安全纠缠信道的建立，这主要依赖于在纠缠共享过程中 Alice 和 Bob 随机选择 EPR 纠缠对进行相关性测量的结果. 如果两者对纠缠粒子对的测量结果为不相同，则表明无窃听；反之若两粒子测量结果为相同，则表明存在窃听，放弃该组纠缠粒子对. 收到 Bob 发送的纠缠粒子之后，Alice 和 Bob 便共享了一对纠缠粒子，其中每个粒子称为一个 ebit. 对于信息的编码过程，Alice 首先对欲传输给 Bob 的经典信息进行密集编码得到携载信息的量子态序列.

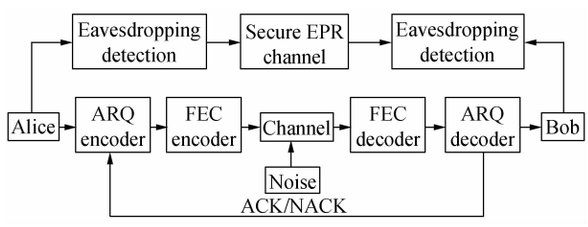

图 1 方案原理

Fig. 1 Scheme of the proposed QSDC system

接着对信息量子态序列进行检错编码，编码所得序列再进行纠缠辅助量子 LDPC 码的 FEC 前向纠错编码，最后将编码量子态序列传输给接收端 Bob. 接收端 Bob 收到编码序列之后，首先进行纠缠辅助量子 LDPC 码的 FEC 前向纠错迭代译码，译码得到的序列再送入 ARQ 检错译码器进行检错译码操作，并判断接收端得到的信息是否正确. 若错误伴随式为零则认为接收到正确的信息，返回一个正确接收（Positive Acknowledgment，ACK）信号；否则返回一个错误接收（Negative Acknowledgment，NACK）信号，并请求发端 Alice 对该组信息进行重新编码传输.

采用这种前后向混合纠错的思想，可以保障在信道条件较好（弱噪音干扰）时可靠的信息传输，以及在信道条件不好（强噪音干扰）时对出错信息序列进行检错重传，从而保证 QSDC 系统的整体通信有效性和可靠性. 本文将分别对该 QSDC 系统中的信息传输流程、纠缠辅助量子 LDPC 码的编译码步骤，以及检错 ARQ 策略进行详细描述.

1.2 窃听检测和信息传输流程

根据图 1 中 QSDC 的原理图，该方案中的信息传输流程见图 2. 首先，Bob 制备纠缠源 $|\psi^-\rangle_{AB}=\frac{1}{\sqrt{2}}(|0_A1_B\rangle-|1_A0_B\rangle)$，将每组纠缠对中的粒子 A 发送给 Alice，而粒子 B 自己保留. 为了保障 QSDC 信息传输过程的安全性，对于每一对纠缠粒子，Alice 以概率 $1-p$ 选择对其进行窃听检测，以概率 p 选择

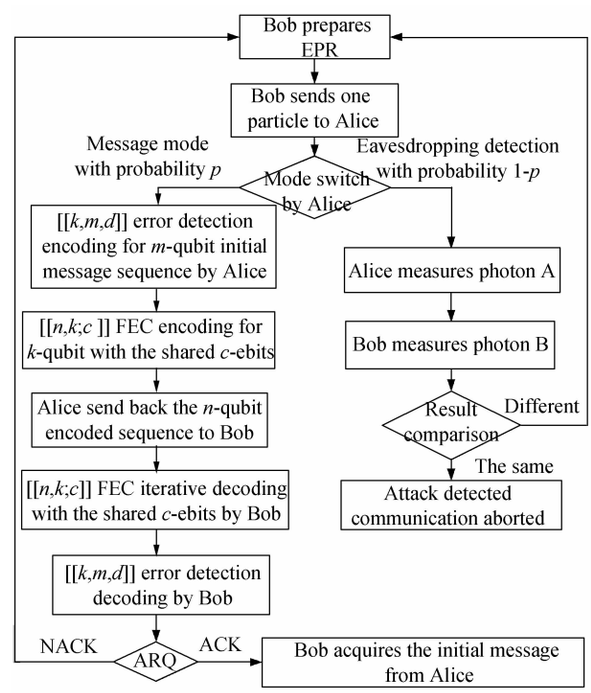

图 2 信息传输流程图

Fig. 2 The flow chart of information transmission

将其用作信息传输的纠缠共享粒子. 对于用于窃听检测的纠缠粒子组，Alice 和 Bob 分别对其进行局部测量，依据纠缠粒子对之间的相关性，判断当前是否存在窃听[2]. 通过这一过程，Alice 和 Bob 建立起安全的纠缠信道，双方共享到一串纠缠粒子序列，这里称所共享的纠缠粒子为 ebit 信息.

QSDC 方案的目的是传输经典信息，Alice 和 Bob 首先需要在经典比特信息和纠缠粒子量子态之间建立起一一对应的关系，如表 1 中的密集编码过程. Alice 将欲发送给 Bob 的 $2m$-bit 经典信息序列，通过表 1 中所示的密集编码思想，每两 bit 对应一个局部操作算符 $U\in\{I,X,Y,Z\}$ 对其拥有的粒子进行局部操作，得到一个 m-qubit 量子态序列. 当从量子信息恢复经典信息时，Bob 对接收到 m-qubit 量子态和其拥有的粒子，进行 Bell 基 X_1X_2，Z_1Z_2 联合测量，则可得到 Alice 发送的 $2m$-bit 经典信息序列.

表 1　密集编码过程

Table 1　Superdense coding process

Message sequence with Alice	00	01	10	11
Corresponding Pauli operators	I_A	X_A	Z_A	Y_A
Local operation by Alice	$I_AI_B\|\psi^-\rangle_{AB}$	$X_AI_B\|\psi^-\rangle_{AB}$	$Z_AI_B\|\psi^-\rangle_{AB}$	$Y_AI_B\|\psi^-\rangle_{AB}$
Entanglement state received by Bob	$\|\psi^-\rangle_{AB}$	$\|\varphi^-\rangle_{AB}$	$\|\psi^+\rangle_{AB}$	$\|\varphi^+\rangle_{AB}$
Message sequence received by Bob	00	01	10	11

本文将对收发两端的 FEC 前向纠错及后向 ARQ 策略中的信息操作流程进行逐步说明. 如图 2 所示第一步：Alice 将携载有经典信息序列的 m-qubit 量子信息序列，以检错码$[[k,m,d]]$进行检错编码操作，得到 k-qubit 检错码字序列；第二步，Alice 从共享得到的纠缠粒子中选取 c 组用作 ebit 序列(即 c-ebit)，以纠缠辅助量子 LDPC 码$[[n,k;c]]$对检错编码输出的 k-qubit 序列进行前向纠错编码操作，得到一个 n-qubit 编码量子态序列；第三步：Alice 将该 n-qubit 编码序列通过量子信道(实际信道中存在噪音)回传给 Bob，后者根据其相应的 c 组 ebit，对$[[n,k;c]]$纠缠辅助量子 LDPC 码进行 FEC 迭代译码，得到 k-qubit 信息序列. 第四步，Bob 对 FEC 译码得到的 k-qubit 信息序列进行$[[k,m,d]]$的检错译码操作，即计算其错误伴随式是否为 0(译码输出的信道错误算子与稳定子生成元是否对易)，如果伴随式为 0，则认为得到正确的 m-qubit 序列并返回一个正确接收 ACK 信号；如果错误伴随式不为 0，则返回一个非正确接收 NACK 信号，进行该组序列的编码重传操作.

1.3　纠缠辅助量子 LDPC 码

对量子信息增加冗余保护的量子纠错码技术，是各种量子信息应用方案中对抗信道噪音影响的重要手段. 将 k 量子比特信息编码为 n 量子比特的$[[n,k]]$稳定子码 $C(S)$，可以由 n 阶 Pauli 算子群 G_n 的一个 2^{n-k} 维可换子群 S(称为该码的稳定子群)来确定，该码空间为 Hilbert 空间$(C^2)^{\otimes n}$的一个 2^k 维子空间. 稳定子群 S 的所有元素可由 $n-k$ 个独立且对易的生成元相乘得到. $n-k$ 个稳定子生成元所对应的矩阵称为该量子码的校验矩阵 $\boldsymbol{A}=(\boldsymbol{A}_1|\boldsymbol{A}_2)$，其中 $\boldsymbol{A}_1$、$\boldsymbol{A}_2$ 是大小为$(n-k)\times n$ 的二进制矩阵. 此时，稳定子生成元之间的对易约束条件转化为子矩阵之间的约束条件 $\boldsymbol{A}_1\boldsymbol{A}_2^{\mathrm{T}}+\boldsymbol{A}_2\boldsymbol{A}_1^{\mathrm{T}}=0$. 式(1)中矩阵 $\boldsymbol{A}$ 对应的稳定子码称为 CSS(Calderbank-Shor-Steane)码，当 $\boldsymbol{H}=\boldsymbol{G}$ 时则该量子码为对偶包含 CSS 结构的稳定子码[13].

$$\boldsymbol{A}=(\boldsymbol{A}_1|\boldsymbol{A}_2)=\begin{pmatrix}\boldsymbol{H} & 0\\ 0 & \boldsymbol{G}\end{pmatrix},\boldsymbol{H}\boldsymbol{G}^{\mathrm{T}}=0 \tag{1}$$

从 Alice 和 Bob 共享的纠缠粒子中选取 c 组纠缠粒子(ebit)，采用纠缠辅助量子 LDPC 码$[[n,k;c]]$，将 k-qubit 信息编码为 n-qubit 长的量子态码字序列，其净码率为$(k-c)/n$. 对偶包含 CSS 结构的纠缠辅助量子 LDPC 码，其所需的 ebit 数目 $c=\mathrm{rank}(\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}})$，其中 $\boldsymbol{H}$ 为经典 LDPC 码的稀疏校验矩阵[18]. 纠缠辅助量子 LDPC 码，降低了构造中稳定子矩阵的自对偶约束条件，从而扩大了矩阵构造的选择范围. 同时该类纠缠辅助 LDPC 码可避免其校验矩阵中的短环(4 环)对迭代译码性能的影响，具有更好的纠错性能[17-18].

这里采用代数有限域的构造方法，将准循环结构的纠缠辅助量子 LDPC 纠错码$[[961,480;163]]$，作为纠缠源量子信息直传中的前向纠错码，在 163 个 ebit 辅助下实现将 480-qubit 信息编码为 961-qubit 序列，其净码率为 0.33. 在退极化量子噪音信道模型下对该码的迭代译码纠错性能进行了 Monte Carlo 仿真.

图 3 给出了纠缠辅助量子 LDPC 码$[[961,480;163]]$在量子退极化信道下的迭代译码纠错性能，其中横坐标表示退极化强度 ε，纵坐标表示误帧率(Frame Error Rate，FER)和误量子比特率(Qubit

Error Rate, QBER). 由图 3 中曲线可以看出,在信道退极化强度 $\varepsilon=0.01$ 时未编码量子态粒子序列的出错概率 QBER 为 10^{-2},而采用纠缠辅助量子 LDPC 纠错码之后的 QBER 则可降到 10^{-6} 以下,即在信道噪音造成 10^{-2} 的原始出错概率下,采用该纠错码之后的粒子出错率降低到了 10^{-6} 以下,大大提高了 QSDC 系统在噪音信道下的通信可靠性.

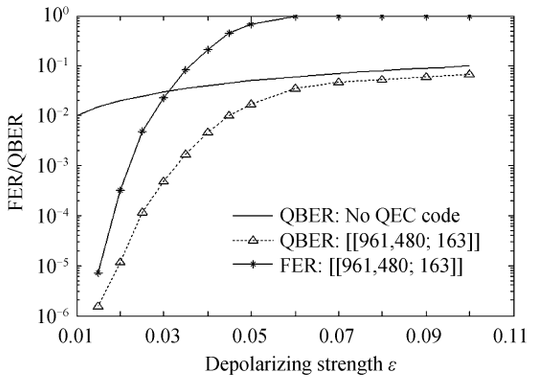

图 3 纠缠辅助量子 LDPC 纠错码[[961,480;163]]在量子退极化信道下的迭代译码性能

Fig. 3 Iterative decoding performance of the entanglement-assisted quantum LDPC FEC code [[961,480;163]] over quantum depolarizing channel

本文方案中收发两端采用纠缠辅助量子 LDPC 码的具体编译码操作过程作以描述. 采用纠缠辅助的前向量子 LDPC 纠错码方案,Alice 将 k-qubit 量子态 $|\varphi\rangle_k$ 编码为 n-qubit 序列的编码操作为

$$|\Psi\rangle_n=U_E|\psi\rangle_c^{\mathrm{A}}|\varphi\rangle_k|0\rangle_{n-c-k} \tag{2}$$

这里编码操作算符 U_E 可以由稳定子生成元矩阵 $\boldsymbol{A}$ 变换得到,$|\psi\rangle_c^{\mathrm{A}}$ 为 Alice 共享所得到的 c 组 ebit 粒子,$|0\rangle_{n-c-k}$是初始态为 0 的编码辅助粒子. 经由噪音量子信道,Bob 接收到携载有 Alice 发送信息的信道输出量子态序列 $|\psi'\rangle_n$,联合其拥有的 c 组 ebit 粒子进行量子纠错码的错误伴随式测量 s,接着进行 LDPC 码的迭代译码过程,最终对接收序列进行错误恢复操作为

$$\begin{aligned}|\varphi'\rangle_k&=D_E^{\wedge}|\psi'\rangle_n|\psi\rangle_c^{\mathrm{B}}=D_E^{\wedge}E|\psi\rangle_n|\psi\rangle_c^{\mathrm{B}}=\\&D_E^{\wedge}EU_E|\varphi\rangle_k|0\rangle_{n-c-k}|\psi\rangle_c^{\mathrm{A}}|\psi\rangle_c^{\mathrm{B}}=\\&D_E^{\wedge}EU_E|\varphi\rangle_k\end{aligned} \tag{3}$$

这里的错误伴随式测量,是对噪音信道输出的量子态码字序列进行稳定子生成元算子的本征值测量. 根据错误伴随式 s 对纠缠辅助量子 LDPC 纠错码进行迭代译码,得到最可能的信道错误算子 $\hat{E}$,当 $D_E^{\wedge}EU_E=I$时即可通过算符 $D_E^{\wedge}$ 的操作恢复出正确的量子态序列,如式(3).

1.4 量子 ARQ 策略

由于量子信息比特具有不同于经典比特的性质,使得对于量子纠错码,在测量结果属于码字空间的条件下(即错误伴随式为 0 时),定义量子 ARQ 协议的保真度为接收量子态的测量结果与传输量子态共线的概率[19]. 对于量子 ARQ 协议,其漏检错误定义为当伴随式 s 为 0 而译码结果 w 不等于发送码字 c 的概率

$$P_{\mathrm{ue}}(C,\varepsilon)=\Pr(s=0,w\neq c) \tag{4}$$

这里 C 代表整个码字空间,ε 为信道的转移概率. 同时,这一事件的条件概率可以定义为,在伴随式为 0 的条件下,译码结果等于发送信息序列的条件概率即

$$P_{\mathrm{con}}(C,\varepsilon)=\Pr(w=c|s=0) \tag{5}$$

条件概率表示当伴随式为 0 时此次传输无错误的可靠性程度. 现已证明存在一系列码率在[0,1]之间的量子纠错码,其漏检概率随着码长增加以指数形式减小[19]. ARQ 协议大致分为停止等待式 ARQ、回退式 ARQ、选择重传式三种,现已有数据链路层上的选择自动重传量子 ARQ 协议方案提出[20].

在本文方案中,如图 2,采用了一个[[k,m,d]]检错量子码对 Alice 的 m-qubit 量子信息进行检错编码,以作为量子 ARQ 协议是否需要重传的标准. 纠缠辅助量子 LDPC 前向纠错码译码输出的 k-qubit 序列作为检错码译码器[[k,m,d]]的输入,接收端 Bob 对其进行检错译码. 当伴随式 s 为 0 时,则返回一个正确接收的 ACK 信号;否则当伴随式 s 不为 0 则返回一个重传的 NACK 信号. 该检错码的最小距离为 d,可以检测出 $d-1$ 个 qubit 错误. 通常 ARQ 协议中的检错码选择冗余度较少的高码率长码(例如单检码),其操作简单且实现复杂度低.

在前向量子纠错码的基础上,添加自动请求重传 ARQ 协议,构成量子信息传输的混合式 HARQ 纠错系统. 在量子信息直传过程中, FEC 的作用是纠正因信道噪音导致的一些量子态错误,提高通信的可靠性,减少 ARQ 的重传频度提高 QSDC 系统的纠缠资源利用率. 而当出现强噪音或窃听干扰带来的错误无法被 FEC 纠错码纠正时,通过检错码[[k,m,d]]的错误检测机制,使接收端可以请求发端进行 ARQ 重传操作,而不是将不可靠的数据直接送给信宿. 该方案既增加了信息传输的可靠性,同时又兼顾 QSDC 系统的通信传输效率.

2 安全性分析

与传统基于纠缠源 Ping-Pong 协议的 QSDC 方案相比,本文所提方案采用了前向 FEC 纠错码技术和后向 ARQ 策略,以提高系统在噪音环境下的通信传输效率以及可靠性. 其中,前向 FEC 纠错码采用具有较强纠错性能的纠缠辅助量子 LDPC 码,后

向 ARQ 策略则可选用冗余度较低的量子检错码来实现. 本文将对该 QSDC 方案从纠缠信道的建立到 Alice 信息编码以及 Bob 端译码等各个阶段的安全性，分别做以分析论证.

首先，在建立纠缠信道过程中仍然采用了传统方案中的窃听检测方法. Alice 和 Bob 对每组纠缠粒子，以概率 p 将该组粒子用于信息传输，以概率 $1-p$ 将该组粒子用于探测当前是否存在窃听，最终达到建立安全纠缠信道的目的. 这里参量 p 的大小是协调 QSDC 系统纠缠资源利用率和窃听探测频度的参量，p 值越大则纠缠粒子的利用率越高，p 值越小则表示用于监测纠缠信道安全的纠缠粒子数目越多，能够更实时地监测纠缠信道以及共享粒子的安全性[4-5].

对本文方案中 Alice 信息编码过程以及编码信息回传过程的安全性进行分析. 在传输经典信息时采用密集编码思想，每两比特经典信息对应一组纠缠粒子得到对应携载有经典信息的量子态序列. 纠缠辅助量子 LDPC 码的主要作用，是纠正 Alice 将编码粒子序列回传给 Bob 时非理想信道中的噪音所带来的错误. 窃听者 Eve 的目的是获得发送者 Alice 发送的信息，由于只有接收端 Bob 持有和发端 Alice 共享的纠缠 ebit 序列，而对于纠缠辅助量子纠错码的译码而言，缺少了 ebit 的辅助 Eve 即使完全截获该组码字序列，仍然无法得到正确的译码结果[17].

检错码$[[k,m,d]]$的作用是判定 Bob 接收到的信息是否与 Alice 的发送消息一致，若不一致则放弃此组数据并请求发端重传. 检错码参量的选择，同时亦关系到编码粒子组传回给 Bob 过程中的安全性即第二次窃听检测问题. 在无噪音的理想信道条件下，检测码单纯用以判定 Bob 是否正确接收到 Alice 发送的信息. 而当信道存在噪音时，则可通过设定检错码最小距离 d 的大小（具有检测 $d-1$ 个 qubit 错误的能力），来检测除信道噪音之外 Eve 的窃听操作所带来的影响. 由于 Eve 只能窃听到纠缠粒子中的一个，而纠缠粒子中每个单一粒子的状态是无法区分的完全混合态 $\rho_A=\mathrm{Tr}_B\{\|\phi'^+\rangle\langle\phi'^+|\rangle\}=\frac{1}{2}I_A$，即窃听者 Eve 采取截获重传的窃听策略，不能获得关于编码量子态的任何信息[9-10].

3　结论

本文基于 EPR 纠缠态的 Ping-Pong 协议思想，提出了一种采用前向纠缠辅助量子 LDPC 纠错码和后向 ARQ 策略的 QSDC 方案. 其中，前向纠缠辅助量子 LDPC 纠错码的作用，是保障在噪音量子信道下 QSDC 系统的通信可靠性，同时提高 QSDC 系统的纠缠资源利用效率. 另外，本文方案在前向纠错的基础上引入后向 ARQ 策略，用以判断 Bob 是否正确接收到 Alice 的发送信息，正确则接收，不正确则请求发端进行编码重传. 对所选用纠缠辅助量子 LDPC 纠错码在退极化量子噪音信道下的迭代译码纠错性能进行了 Monte Carlo 仿真，获得了比采用编码时更好的性能. 最后，对本文方案中的纠缠信道建立过程以及信息回传过程中的安全性进行了分析论证.

受限于当前的量子态精密操控技术、量子信息存储技术，以及单光子探测器准确度等因素，量子信息直传通信方案的实际应用还存在一些困难，但其理论可行性已得到了论证，并且已有相关可行性实验的研究报道. 相信随着光量子器件技术的不断发展进步，量子信息安全直传通信将会成为量子信息领域的另一项重要应用.

参考文献

[1] BEIGE A, ENGLERT B G, KURTSIEFER C, *et al*. Secure communication with a publicly known key[J]. *Acta Physics Polonica A*, 2002, **101**(3): 357-368.

[2] BOSTROM K, FELBINGER T. Deterministic secure direct communication using entanglement [J]. *Physics Review Letter*, 2002, **89**(18): 7902-7905.

[3] CAI Qing-yu, LI Bai-wen. Improving the capacity of the Bostrom-Felbinger Protocol[J]. *Physics Review A*, 2004, **69**(5): 4301-4303.

[4] GUO Ying, ZENG Gui-hua. Deterministic quantum key distribution using stabilizer quantum code[J]. *International Journal of Quantum Information*, 2007, **5**(3): 319-334.

[5] LU Xin, MA Zhi, FENG Deng-guo. Quantum secure direct communication using quantum Calderbank-Shor-Steane error correcting codes[J]. *Journal of Software*, 2006, **17**(3): 509-515.

[6] DENG Fu-guo, LONG Gui-lu. Secure direct communication with a quantum one- time pad[J]. *Physics Review A*, 2004, **69**(5): 2319-2322.

[7] CAI Xin-hua, NIE Jian-jun, GUO Jie-rong. Entanglement translation and quantum teleportation of the single-photon entangled state[J]. *Acta Photonica Sinica*, 2006, **35**(5): 776-779.
蔡新华，聂建军，郭杰荣. 单光子纠缠态的纠缠转移和量子隐形传态[J]. 光子学报，2006，**35**(5): 776-779.

[8] CAI Qing-yu. The "Ping-Pong" protocol can be attacked without eavesdropping[J]. *Physics Review Letter*, 2003, **91**(10): 9801.

[9] WOJCIK A. Eavesdropping on the "ping-pong" quantum communication protocol[J]. *Physics Review Letter*, 2003, **90**(15): 7901-7904.

[10] BOSTROM K, FELBINGER T. On the security of the ping-pong protocol[J]. *Physics Letters A*, 2008, **372**(22): 3953-3956.

[11] OSTERMEYER M, WALENTA N. Experimental demonstration of quantum key distribution with entangled photons following the ping-pong coding protocol[DB/OL].

2007,arXiv:Quant-ph/0703242.

[12] DENG Fu-guo, LONG Gui-lu, LIU Xiao-Shu. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. *Physics Review A*, 2003, **68**(4): 2317-2322.

[13] WANG Chuan, DENG Fu-guo, LONG Gui-lu. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state [J]. *Optics Communications*, 2005, **253**(1-3): 15-20.

[14] MACKAY D, MITCHISON G, MCFADDEN P. Sparse-graph codes for quantum error correction [J]. *IEEE Transactions on Information Theory*, 2004, **50**(10): 2315-2330.

[15] SHAO Jun-hu, BAI Bao-ming, LIN Wei, *et al*. Jointly-check iterative decoding algorithm for quantum sparse graph codes [J]. *Chinese Physics B*, 2010, **19**(8): 307-313.

[16] SHAO Jun-hu, BAI Bao-ming, LIN Wei, *et al*. Construction and decoding of nonbinary quantum LDPC codes [J]. *Journal of Xidian University*, 2010, **37**(6): 1005-1010.
邵军虎, 白宝明, 林伟, 等. 多元量子 LDPC 码的构造与译码[J]. 西安电子科技大学学报, 2010, **37**(6): 1005-1010.

[17] BRUN T A, DEVETAK I, HSIEH M H. Correcting quantum errors with entanglement[J]. *Science*, 2006, **314**(5798): 436 - 439.

[18] HSIEH M H, BRUN T A, DEVETAK I. Entanglement-assisted quantum quasi-cyclic low-density parity-check codes [J]. *Physics Review A*, 2009, **79**(3): 2340-2346.

[19] ASHIKHMIN A. Fidelity of a quantum ARQ protocol[C]. IEEE Information Theory Workshop, 13-17 March 2006, Punta del Este, 2006: 42-46.

[20] ZHOU Nan-run, ZENG Bin-yang, GONG Li-hua. Selective automatic repeat quantum synchronous communication protocol based on quantum entanglement[J]. *Acta Physics Sinica*, 2010, **59**(4):2193-2199.
周南润,曾宾阳,龚黎华. 基于纠缠的选择自动重传量子同步通信协议[J]. 物理学报,2010,**59**(4):2193-2199.

Quantum Secure Direct Communication by Using Quantum Entanglement-assisted LDPC Codes and ARQ Strategy

SHAO Jun-hu, BAI Bao-ming

(*State Key Lab of Integrated Service Networks, Xidian University, Xi'an* 710071, *China*)

Abstract: To improve the performances of the present Ping-Pong protocol systems over noisy channels, an efficient quantum secure direct communication scheme is proposed. Entanglement-assisted quantum low-density parity-check code is used to protect the encoded quantum information sequences against the channel noises, which improves the reliability of the quantum secure direct communication system. Furthermore, quantum automatic repeat-request protocol with error detection code is used to detect the strong channel noise effect, which improves the communication efficiency. Two steps of eavesdropping detection are taken to ensure the system security, and the iterative decoding performance of entanglement-assisted quantum low-density parity-check code is simulated over quantum depolarizing channel.

Key words: Quantum communication; Quantum Secure Direct Communication(QSDC); Quantum error-correcting code; Quantum Automatic Repeat-Request(ARQ)